CYSP 2023

دومین کنفرانس فضای سایبر

مجموعه مقالات

02230-21686

دانشگاه تهران

University of Tehran

۹ تا ۱۱ آبان ۱۴۰۲

31 October, 1-2 November 2023

CYSP 2023

دومین کنفرانس

فضای سایر

مجموعه مقالات

02230-21686

دانشگاه تهران

۹ – ۱۱ آبان ۱۴۰۲

.

مجموعه مقالات
دومین کنفرانس ملی فضای سایبر (CYSP 2023)
برگزارکننده: دانشگاه تهران

تدوین: کاظم فولادی قلعه
با همکاری: حسین عظیمی، علیرضا زینی

ناشر: دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
چاپ و صحافی: ماتریس
سال انتشار: ۱۴۰۲

نشانی دبیرخانه: قم، بلوار دانشگاه، دانشکدگان فارابی دانشگاه تهران، دانشکده مهندسی
کد پستی: ۳۷۱۸۱۱۷۴۶۹
تلفن: ۰۲۵-۳۶۱۶۶۶۵۱
فکس: ۰۲۵-۳۶۱۶۶۶۵۲
ایمیل: cysp.conf@ut.ac.ir
وب‌سایت: http://cysp2023.ut.ac.ir
پیام‌رسان و شبکه‌های اجتماعی: @cysp_conf
همه‌ی پیوندها در یک جا: http://conf.cysp.ir/links

حامیان علمی
Scientific Sponsers

حامیان سازمانی
Organizational Sponsers

حامیان رسانه‌ای و نشر
Media & Publication Sponsers

اعضای کمیته اجرائی

۱. **دکتر حمید زارع**، دانشیار، رئیس دانشکدگان فارابی دانشگاه تهران: رئیس کنفرانس
۲. **دکتر کاظم فولادی قلعه**، استادیار، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: دبیر علمی
۳. **دکترامیرحسین کیهانی‌پور**، استادیار، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: دبیر اجرایی
۴. **دکتر احمد علی‌نژاد**، استادیار، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول نشست‌ها و کارگاه‌ها
۵. **مهندس محمدعلی شکوهیان‌راد**، پژوهشگر ارشد آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران و مدرس مدعو دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول ارتباطات

همکاران کمیته اجرائی

۱. **مهندس علیرضا زینی**، دستیار پژوهشی آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران: مسئول امور مقالات
۲. **علیرضا میرزایی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول هماهنگی
۳. **مهندس محمدجواد خدمتی**، دستیار پژوهشی آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران: مسئول امور رسانه و خبرگزاری
۴. **مهدی حسومی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول پخش زنده اینترنتی
۵. **مهدی امامی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور چندرسانه‌ای
۶. **محمدحسین فرهادیان**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول تدوین ویدئویی
۷. **امیرحسین نصراللهی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور گرافیک
۸. **سجاد شکوه مسقانی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور نمایشگاه جانبی
۹. **سید محمدمهدی حسینی رکن‌آبادی**، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور پذیرش و تشریفات

سایر همکاران: امیرحسین احسانی، هلیا احمدی، پویا اردهخانی، فاطمه ارفاقی، پرنیا اسدی، معین اسدیان پاک فر، محمد امین اسعدی، محمدمهدی اسکندری، علی اشعری، راحله افکاری، محمد عرفان امیرآبادی فرهانی، زهرا انصاری‌فرد، امیرحسین انفرادی، هانی انوری شعاع، حانیه ایرانی، علی ایزدی، علی ایومن، مهدیس آتشی، امیررضا آخوندی، محمد رضا آرمان‌پور، نیما آریان‌نژاد، محمد آزاد، محمد سجاد آشناگر، امیرمسعود آشوری، زهرا آقامحمدی، محمدجواد بافرانی، نوید باقریان، زهرا بصیری، سیدمسعود بکائی قمی، زهرا سادات بنی هاشمیان، سید حسین بهاالدینی، آیلین بهنیا، یاسین بیرامی، محمد متین بیگدلی، محمد مهدی پسندیده‌خو، روژین پناو، مهدی پناهی، امیرعلی پوررستمی، محسن پورصدقی آلانق، زهرا پورفرزین، محمد امین پورمند، محسن پیری، بنیامین تفرشی، نیما تهرانی فرشید، امیرحسین جالیان، سید محمد جعفری، مهسا جلالی، علی جمشیدی، محمد عرفان جهان‌بخشی، مهدی جهانگیری، محسن چسباوی، محمد حسین حاجی اسفندیاری، محمدامین حاجیان نژاد، محسن حبیبی پناه، محسن حسن‌زاده، علی حسنی، پارسا حسین‌زاده یزدی، رقیه سادات حسینی، یحیی حسینی، محمدحسن حق‌شناس، محمد مهدی حکیمی، محمدرضا خدامرادی، مسعود خدایاری، امیرمحمد خسروی، علی رادمرد، حدیثه رجب‌زاده، امیر رجبی هشین، محمد رحیمی، سعید رزاقی، عارفه رشیدی، نرگس رضاییان، حسین رضائیان، هلیا رنجبر، محمد متین زارعی محمودآبادی، فاطمه سبحانی، سید محمدمهدی سبحانی‌پور، سورن سلطان‌زاده، فاطمه سلمانی، محمد جواد سمیعی زفرقندی، علیرضا شاکر اردکانی، محمد مهدی شجاعی، صدرا شریعت مهدوی، ریحانه شریفی اسدی، علی شفیعی سروستانی، یونس شمشیری، زینب شوندی، آوا شهاب‌الدین، امیرحسین صابری، عرفان صابری، مهرداد صادق‌پور، صبا صادقی بی‌غم، مبین صارمی، زهرا صالحی‌فر، پیام صائمی، مریم طاهری، سیده زینب طباطبائی لطفی، رژینا طلوع کیان، امیرعلی عابدی، محمد عباسی راد، ملیکا عرب‌زاده، علی عرفانی‌فر، ابوالفضل عزت‌پور، امیر محمد عزیزی، محسن علی احمدی، علی علی‌شیر، علی عمادی نظری، محمد غلامی، محمدرضا غلامی، محمدرضا فاضلی، الهه فردوسی، محمد فرزانه، سید علی فقیه موسوی گلپایگانی، سید یزدان قاسمی، زینب قدوسی‌زاده، ماهان قدیم‌خانی، سیدمحمدصالح قطبانی، محمد قلاوند، محمد امین قلی‌زاده، فاطمه کاشی، فاطمه کبیری اصل، حسام‌الدین کدخدا، ایمان کربلایی، عرفان کربلایی، علی کریمی، علی کشوری پسندیده، معین کفاش‌زاده، زهرا کمالیان، مصطفی کوتی، نیما کوه خضری، فاطمه کوهی، محمدمهدی گل محمدی، محمدرضا گنجی، علی لک‌زائی، عباس متقیان نژاد، سعید متولی، سجاد مجدی، فاطمه محمد گنجی، محمدرضا محمدی، امیرمهدی محمدی، سحر محمدی شرکانلو، حسین محمدیان، آرمان محمدیان، امیررضا مختاری راد، آریا مرادی، سید محمد ضیاء مصطفوی، سید یونس مطهری، محمدعلی مظاهری فرد، سید محمدجواد مقدس‌نژاد، محمد پارسا مقصودی، محمد ملانوروزی، آریامهر ملکی، سید مهدی منجم، سید ابوالفضل موسوی، یاسین مهدوی مقدم، امیر میرزائی موحد، سام ناجی، سیده فرگل ناظم‌زاده، محمدمهدی نصراللهی، محمد مهدی نظری، عرشیا نقوی، ابوالفضل نوروزی، سجاد واحدتی نیا، امیر واحدی، رادمهر وثوقی، آرش وجدانی، سبحان ولی‌زاده درخشان، سید علی هدایتی، امیررضا یوسفی.

دبیران نشست‌ها و کارگاه‌ها: مهندس یاشار ابری، مهندس علیرضا ابوالقاسمی، مهندس فهیمه احمدی، مهندس جلال استاد هادی دهکردی، مهندس محمدامین جوادی مقدم، مهندس محمدعلی حسین بیگی، مهندس فائزه خادم، مهندس حانیه رخشانی، مهندس فاطمه سلمانی، مهندس اسمعیل شاهسوند بغدادی، خانم فاطمه صفائی مهر، مهندس محدثه عباسی، مهندس علیرضا علی‌زاده، مهندس احمد فرید اصیل، مهندس عباس قدیم‌پور شبلو، مهندس حمیدرضا کریمی، مهندس عبدالحمید ناظرپناهی، حجت‌الاسلام اسماعیل نجاتی، مهندس محمدمهدی نظری، خانم رضوان هامانی.

دستیاران ویراستاری مجموعه مقالات (دانشجویان مهندسی کامپیوتر دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران): مهدیس آتشی، محمدسجاد آشناگر، علی احمدی رق‌آبادی، فاطمه ارفاقی، نیما آریان‌نژاد، محمد آزاد، علی افتخاری، محمدصالح آل اسحق، محمدعرفان امیرآبادی فراهانی، سیدمحمدحسین امیرحسینی، محمدجواد بافرانی، محسن بزازان، سیدحسین بهاالدینی، نوید تراش کاشانی، امیرحسین جالیان، سیدمحمد جعفری، مهسا جلالی، محمدامین حاجیان نژاد، سیدمحمدمهدی حسینی رکن‌آبادی، علی دانیالی، میلاد زند، فاطمه سبحانی نجف‌آبادی، امیرمحمد سلگی، محمدمهدی شجاعی، علی شفیعی سروستانی، پیام صائمی، عرفان صابری، مهرداد صادق‌پور، سیدمبین صارمی حصاری، سیده زینب طباطبائی لطفی، محمدامین عارفی نیا، محمد عباسی راد، احسان عبداللهی بیرون، علی عرفانی فر، علی علی شیر، محمدرضا غلامی، سیدعلی فقیه موسوی گلپایگانی، زینب قدوسی زاده، مصطفی کوتی، عباس متقیان نژاد، سعید متولی، سحر محمدی شرکانلو، آرمان محمدیان، حسین محمدیان بهنامی، سیدرضا مسلمی، سیدیونس مطهری، یاسین مهدوی مقدم، امیر میرزائی موحد، نیما میری، عرشیا نقوی.

اعضای کمیته علمی

۱. **دکتر حسین آقابابا**، دانشیار، دانشگاه تهران
۲. **دکتر مهرنوش ابوذری**، استادیار، دانشگاه تهران
۳. **دکتر مهشید التماسی**، استادیار، دانشگاه تهران
۴. **دکتر سروناز تربتی**، استادیار، دانشگاه آزاد اسلامی
۵. **دکتر فاطمه ثقفی**، دانشیار، دانشگاه تهران
۶. **دکتر سید محمدباقر جعفری**، دانشیار، دانشگاه تهران
۷. **دکتر امیر جلالی بیدگلی**، استادیار، دانشگاه قم
۸. **دکتر حامد جلالی بیدگلی**، استادیار، دانشگاه صنعتی اصفهان
۹. **دکتر مهدی چم‌پور**، استادیار، دانشگاه صنعتی قوچان
۱۰. **دکتر محسن حاجی زین‌العابدینی**، استادیار، دانشگاه شهید بهشتی
۱۱. **دکتر سید احمد حبیب‌نژاد**، دانشیار، دانشگاه تهران
۱۲. **دکتر رحیم خانی‌زاد**، استادیار، دانشگاه علم و صنعت ایران
۱۳. **دکتر سید نصیب‌اله دوستی مطلق**، استادیار، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی
۱۴. **دکتر مهدی ذاکری**، دانشیار، دانشگاه تهران
۱۵. **دکتر سعید روحانی**، دانشیار، دانشگاه تهران
۱۶. **دکتر محمدجواد شایگان‌فرد**، دانشیار، دانشگاه علم و فرهنگ
۱۷. **دکتر محمدحسن شیرعلی شهرضا**، استادیار، دانشگاه صنعتی امیرکبیر
۱۸. **دکتر سجاد شیرعلی شهرضا**، استادیار، دانشگاه صنعتی امیرکبیر
۱۹. **دکترمحمدحسین ظریفیان یگانه**، استادیار، دانشگاه تهران
۲۰. **دکتر سید سعیدرضا عاملی رنانی**، استاد، دانشگاه تهران
۲۱. **دکتر محمدعلی عبداللهی**، دانشیار، دانشگاه تهران
۲۲. **دکتر سید امید فاطمی**، دانشیار، دانشگاه تهران
۲۳. **دکتر کاظم فولادی قلعه**، استادیار، دانشگاه تهران
۲۴. **دکتر محمد کاشانی‌پور**، دانشیار، دانشگاه تهران
۲۵. **دکتر مسعود کوثری**، دانشیار، دانشگاه تهران
۲۶. **دکتر مهدی کارگهی**، استاد، دانشگاه تهران
۲۷. **دکتر محمدرضا کریمی قهرودی**، استادیار، دانشگاه صنعتی مالک اشتر
۲۸. **دکتر علی‌اصغر کیا**، استاد، دانشگاه علامه طباطبائی
۲۹. **دکتر امیرحسین کیهانی‌پور**، استادیار، دانشگاه تهران
۳۰. **دکتر احمد محمودی ازناوه**، استادیار، دانشگاه شهید بهشتی
۳۱. **دکتر محمود مختاری**، استادیار، دانشگاه شهید بهشتی
۳۲. **دکتر زهرا موحدی**، استادیار، دانشگاه تهران
۳۳. **دکتر عبدالرضا نوروزی چاکلی**، استاد، دانشگاه شاهد
۳۴. **دکتر خداداد هلیلی**، استادیار، دانشگاه علوم و فنون هوایی شهید ستاری
۳۵. **Dr. Christoph Stückelberger**، Professor، University of Basel

پیام وزیر علوم، تحقیقات و فناوری
به‌مناسبت برگزاری نخستین «کنفرانس فضای سایبر»

دکتر محمدعلی زلفی‌گل

۹ آبان ۱۴۰۱

بسم الله الرحمن الرحیم

محضر همه‌ی مدعوین نخستین کنفرانس فضای سایبر، به ویژه میهمانان بین الملل این رویداد علمی سلام عرض می‌کنم و آرزومندم که تحقیقات ارزنده‌ی ارائه شده در این همایش، به موفقیت روزافزون پژوهشگران پیوند بخورد.

در جایگاه وزیر علوم، تحقیقات و فناوری و به نمایندگی از جامعه‌ی علمی و دانشگاهی کشور، از اهتمام دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران و آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران در برگزاری این همایش مهم و ضروری تشکر و قدردانی می‌کنم.

موضوع «فضای سایبر» یکی از مهم‌ترین دغدغه‌های امروز ماست که همه سطوح جامعه را به خود وابسته و مشغول کرده است و به تعبیر مقام معظم رهبری «حفظه الله» به اندازه‌ی انقلاب اسلامی اهمیت دارد. بر خلاف دیدگاه گذشته، امروزه کمتر کسی منکر نقش راهبردی این پدیده می‌باشد. استقلال کشور، وابسته به استقلال و اشراف ما در فضای سایبر است و برای ارتقاء پایگاه سایبری، لازم است برتری علمی ایران اسلامی در علوم و فناوری‌های مرتبط با این حوزه بالا-خص دانش سایبرنتیک رقم بخورد و این مهم اتفاق نمی‌افتد مگر با همت پژوهشگران، فرهیختگان و نخبگان علمی دغدغه‌مند که ضرورت و اهمیت این موضوع را درک کرده‌اند.

این همایش می‌تواند در تسهیل روند پیشرفت معرفتی، علمی و فناوری در راستای بیانیه‌ی گام دوم انقلاب با همراهی آگاهانه‌ی دولت،اثرگذار و ثمربخش باشد. از دیگر سو، مشخصه‌ی «بین رشته‌ای» بودن موضوع این همایش حائز اهمیت است و فرصت مناسبی‌ست تا استادان و پژوهشگران محترم حوزه‌های مختلف، مطالعات، دستاوردها و آخرین یافته‌های علمی خود را با یکدیگر به اشتراک گذارند.

لازم می‌دانم مراتب سپاس و قدردانی خود را از همه‌ی استادان، پژوهشگران، دبیران علمی و اجرایی و عوامل برگزاری رویداد، اعلام دارم و امیدوارم دوره‌های بعدی این کنفرانس نیز با شکوه هر چه بیشتر برگزار شده و آثار آن سال به سال در نظام تصمیم‌سازی و حکمرانی کشور و سایر امور به‌طور فزاینده ملاحظه گردد.

بسمه تعالی

جمهوری اسلامی ایران
وزارت علوم تحقیقات و فناوری

تاریخ : ۱۴۰۱/۰۸/۰۹
شماره : ۲۲۸۰۳۳/و
پیوست :

شماره پیگیری
۹۸۰۲۹۲۷

پیام وزیر علوم، تحقیقات و فنّاوری به مناسبت برگزاری نخستین «کنفرانس فضای سایبر»

بسم‌الله الرحمن الرحیم

محضر همه‌ی مدعوینِ نخستینِ کنفرانس فضای سایبر، به ویژه میهمانان بین‌الملل این رویداد علمی سلام و عرض می‌کنم و آرزومندم که تحقیقات ارزنده‌ی ارائه شده در این همایش، به موفقیت روزافزون پژوهشگران پیوند بخورد.

در جایگاه وزیر علوم، تحقیقات و فناوری و به نمایندگی از جامعه‌ی علمی و دانشگاهی کشور، از اهتمام دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران و آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران در برگزاری این همایش مهم و ضروری تشکر و قدردانی می‌کنم.

موضوع «فضای سایبر» یکی از مهم‌ترین دغدغه‌های امروز ماست که همه‌ی سطوح جامعه را به خود وابسته و مشغول کرده است و به‌تعبیر مقام معظم رهبری (حفظه‌الله) به‌اندازه‌ی انقلاب اسلامی اهمیت دارد. بر خلاف دیدگاه گذشته، امروزه کمتر کسی منکر نقش راهبردی این پدیده می‌باشد. استقلال کشور، وابسته به استقلال و اشراف ما در فضای سایبر است و برای ارتقاء پایگاه سایبری، لازم است برتری علمی ایران اسلامی در علوم و فناوری‌های مرتبط با این حوزه بالاخص دانش سایبرنتیک رقم بخورد و این مهم اتفاق نمی‌افتد مگر با همت پژوهشگران، فرهیختگان و نخبگان علمی دغدغه‌مند که ضرورت و اهمیت این موضوع را درک کرده‌اند.

این همایش می‌تواند در تسهیل روند پیشرفت معرفتی، علمی و فناوری در راستای بیانیه‌ی گام دوم انقلاب با همراهی آگاهانه‌ی دولت، اثرگذار و ثمربخش باشد. از دیگر سو، مشخصه‌ی «بین‌رشته‌ای» بودن موضوع این همایش حائز اهمیت است و فرصت مناسبی‌ست تا استادان و پژوهشگران محترم حوزه‌های مختلف، مطالعات، دستاوردها و آخرین یافته‌های علمی خود را با یکدیگر به اشتراک گذارند.

لازم می‌دانم مراتب سپاس و قدردانی خود را از همه‌ی استادان، پژوهشگران، دبیران علمی و اجرایی و عوامل برگزاری رویداد، اعلام دارم و امیدوارم دوره‌های بعدی این کنفرانس نیز با شکوه هر چه بیشتر برگزار شده و آثار آن سال به سال در نظام تصمیم‌سازی و حکمرانی کشور و سایر امور به‌طور فزاینده ملاحظه گردد.

محمدعلی زلفی گل
وزیر علوم،تحقیقات و فناوری

نشانی :
تهران شهرک قدس
میدان صنعت ، خیابان
خوردین، خیابان هرمزان
نبش خیابان پیروزان جنوبی
کد پستی : ۱۴۶۶۶-۶۴۸۹۱
شماره تلفن : ۸۲۲۳۱۰۰۰
صندوق پستی :
تهران ۱۵۱۳-۱۴۶۶۵
Website:www.msrt.ir
Email:info@msrt.ir

سخن دبیر علمی

دکتر کاظم فولادی قلعه

عضو هیئت علمی دانشگاه تهران

سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران

قرن جدید هجری شمسی را در شرایطی آغاز کردیم که دنیا موقعیت‌های بسیار متفاوتی را تجربه می‌کند و بدون شک بخش مهمی از این تفاوت‌ها متأثر از گسترش نفوذ فضای سایبر در جهان و اثرگذاری عمیق آن بر بیشتر جنبه‌های زندگی فردی و اجتماعی بشر است. اکنون می‌توانیم ادعا کنیم که «نظم جدید جهان» بدون شک وابسته به مقوله‌ی «فضای سایبر» است.

فضای سایبر، فضایی است که اطلاعات در آن به گردش در می‌آید؛ اما این گردش اطلاعات به‌صورت هدفمند و جهت‌مند انجام می‌گیرد و این تعبیر، همان چیزی است که در اصطلاح علمی به آن «کنترل» گفته می‌شود. بر این اساس، فضای سایبر، به‌عنوان فضایی که در آن نوعی کنترل رقم می‌خورد، درک می‌شود. این مهم‌ترین و ذاتی‌ترین ویژگی این فضاست که البته در ادبیات عمومی و علمی ما کمتر بدان توجه شده است و باعث شده است جنبه‌ی «مجازی» بودن این فضا در افکار عمومی برجسته‌تر جلوه کند. البته توجه به این نکته نیز مهم است که در اینجا مجازی (virtual) در مقابل واقعی نیست و مجازی بودن به نوعی واقعیت ناملموس اشاره دارد که در برابر واقعیت ملموس (actual) تعریف می‌شود.

فضای سایبر، مبتنی بر دانش «سایبرنتیک» شکل گرفته است. به‌طور ساده، دانش سایبرنتیک، دانش سلطه و حاکمیت است و این حاکمیت از طریق روش «کنترل» محقق می‌شود. بر این اساس، فضای سایبر را می‌توان یک قلمروی حاکمیتی دانست که هر پدیده‌ای که به آن وارد می‌شود، تحت نوعی سلطه از جنس کنترل قرار می‌گیرد. برای شکل‌گیری کنترل، باید متغیر کنترل در اختیار کنترل‌کننده قرار گیرد و بدیهی است که هر نوع متغیر نیازمند دانش اختصاصی خود برای شیوه‌ی کنترل آن خواهد بود. شاخه‌های کاربردی دانش سایبرنتیک بر اساس انواع مختلف متغیرهای کنترل به جزئیات این موضوع می‌پردازند و آنها را به‌طور عمومی با عنوان X-cybernetics نامگذاری می‌کنیم که در آن X متغیر کنترل (کنترل‌کننده یا کنترل‌شونده) است. البته دانش‌های سایبری که با قالب کلی Cyber-X از آنها یاد می‌کنیم، شناخته‌شده‌تر هستند، چرا که این هدف دانش‌ها موضوع X است که در طبقه‌بندی متداول علوم به آن پرداخته شده است و صرفاً از ظرفیت «سایبر» برای هدف X استفاده می‌شود.

تنوع متغیرهای کنترل باعث می‌شود که طیف وسیعی از دانش‌ها در دامنه‌ی دانش سایبرنتیک واقع شوند یا به آن مرتبط شوند و به‌همین دلیل مطالعات بین رشته‌ای به‌صورت یک خصلت ذاتی در پژوهش‌های مرتبط با موضوع فضای سایبر و دانش پایه‌ی آن، یعنی دانش سایبرنتیک، شمرده می‌شود.

این کنفرانس قصد دارد زمینه‌ای را فراهم کند که مطالعات بین‌رشته‌ای بلکه فرارشته‌ای فضای سایبر به‌صورت منسجم شکل بگیرد و در قالب یک جریان علمی مؤثر و مفید به حرکت خود ادامه بدهد. برگزاری موفق نخستین دوره‌ی این کنفرانس در آبان ۱۴۰۱ و دستاوردهای آن انگیزه‌بخش پژوهشگران و دغدغه‌مندان موضوع این کنفرانس شد و به لطف الهی توفیق داریم دومین دوره‌ی این کنفرانس را در تاریخ ۹ الی ۱۱ آبان ۱۴۰۲ برگزار کنیم و امیدواریم برگزاری سالانه‌ی این کنفرانس هر چه بیشتر ما را به اهداف مشخص شده‌ی این رویداد نزدیک و نزدیک‌تر کند.

به‌علاوه، با توجه به رشد اهمیت فضای سایبر و کاربردهای آن، وسعت فراگیری و چالش‌های نوظهور حاکمیتی آن، ضرورت بررسی علمی ابعاد مختلف این پدیده در محیط دانشگاهی و هم‌اندیشی اندیشمندان مرتبط، بیش از پیش حس می‌شود. به‌همین منظور، دومین کنفرانس ملی فضای سایبر توسط دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران با محوریت «آزمایشگاه پژوهشی فضای سایبر» برگزار می‌شود. این کنفرانس محلی برای ارائه‌ی آخرین یافته‌های پژوهشگران و مباحثه پیرامون ایده‌های آنها در حوزه‌ی فضای سایبر، دانش سایبرنتیک و سیستم‌های سایبرنتیکی و مسائل مرتبط با آنها می‌باشد. متخصصان و پژوهشگران برای ارائه‌ی ایده‌های جدید و آخرین دستاوردهای خود به این کنفرانس دعوت شده‌اند و تمامی موضوعات مرتبط با حوزه‌ی فضای سایبر و دانش سایبرنتیک در سطوح استراتژیکی، تاکتیکی و تکنیکی در محدوده‌ی موضوعات مورد نظر این کنفرانس قرار می‌گیرد.

در برنامه‌ی دومین کنفرانس ملی فضای سایبر علاوه بر ۱۵ نشست ارائه‌ی مقالات شفاهی و نشست ارائه‌ی مقالات پوستری برای ارائه‌ی ۷۵ مقاله پذیرفته شده، بیش از ۲۰ نشست تخصصی/ میزگرد و کارگاه آموزشی پیش‌بینی شده است که شامل موضوعات پرکاربرد و پرمخاطب مرتبط با موضوع کنفرانس است. در اینجا جا دارد علاوه بر اعضای محترم کمیته‌های علمی و اجرایی، همکاران کمیته‌ها، پژوهشگران و نویسندگان مقالات، از سازمان‌ها، نهادها و شرکت‌های حمایت‌کننده از کنفرانس نیز تشکر ویژه داشته باشیم که غنای برنامه‌های تنظیم‌شده محصول همکاری این مجموعه‌ها با دبیرخانه‌ی کنفرانس می‌باشد.

امیدواریم توفیق پیدا کنیم دوره‌های بعدی این کنفرانس را با کیفیت هر چه بهتر در سال‌های پیش رو داشته باشیم و آثار مفید این جریان پژوهشی در نظامات معرفتی، علمی، تصمیم‌سازی و اجرایی کشور بلکه جهان دیده شود، ان‌شاءالله. ۱ آبان ۱۴۰۲

محورهای مقالات

- چارچوب نظری و مفهومی زیرساخت فضای سایبر:
  - اطلاعات: محتوا، فلسفه‌ی اطلاعات و نظریه‌ی اطلاعات
  - کنترل: تغذیه‌ی اطلاعات، کنترل مهندسی و کنترل اجتماعی
  - ارتباطات: انتقال اطلاعات، ارتباطات مهندسی و ارتباطات اجتماعی
  - محاسبات: پردازش اطلاعات، ذخیره و بازیابی اطلاعات
- تئوری سیستم‌ها و سیستم‌های سایبرنتیکی
- دانش سایبرنتیک و شاخه‌های دانش سایبرنتیک
- فلسفه‌ی فضای سایبر، دیدگاه‌های فلسفی به فضای سایبر
- سیستم‌های مدیریت اطلاعات و سیستم‌های اطلاعاتی مدیریت
- جامعه‌ی اطلاعاتی
- روابط میان فضای ویرچوآل و فضای اکچوآل
- فضای سایبر و انسان
- حکمرانی فضای سایبر، حکمرانی بر فضای سایبر، حکمرانی با فضای سایبر، حکمرانی در فضای سایبر
- جنگ سایبری، جنگ در فضای سایبر، جنگ به‌وسیله‌ی فضای سایبر
- قدرت سایبری، فضای سایبر و حاکمیت
- فرهنگ سایبری، فضای سایبر و فرهنگ، فضای سایبر و رسانه
- اقتصاد سایبری، فضای سایبر و اقتصاد
- جرائم سایبری، فضای سایبر و قانون
- روان‌شناسی سایبری
- فضای سایبر و هوش مصنوعی، کلان‌داده‌ها و یادگیری ماشینی
- فضای سایبر و اهداف توسعه پایدار سازمان ملل متحد (SDGs)
- سیستم‌های سایبر-فیزیکی و اینترنت اشیاء، انقلاب صنعتی چهارم
- سایبرنتیک کوانتومی، فضای سایبر کوانتومی، محاسبات و ارتباطات کوانتومی
- کاربردهای سایبری
- فضای سایبر و اینترنت
- فضای سایبر و شبکه‌های اجتماعی
- امنیت سایبری، فضای سایبر و امنیت
- بلاک‌چین (زنجیره‌بلوکی)، رمزارزها، ارز دیجیتال بانک مرکزی (CBDC)
- واقعیت ویرچوآل و واقعیت افزوده، متاورس و زندگی دوم
- سایر موضوعات مرتبط

نشست‌های تخصصی و کارگاه‌های آموزشی (قم)

سه‌شنبه ۹ آبان ۱۴۰۲ – ساعت ۱۳:۳۰ تا ۱۵:۱۵ – نشست‌های تخصصی و کارگاه‌های آموزشی (۱) – قم

کد نشست	زمان	نوع نشست	عنوان	سخنران / ارائه‌کننده	برگزار کننده
۱-الف 1A	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	کارگاه آموزشی	**هوش مصنوعی برای همه**	دکتر مسلم تقی‌زاده	کنفرانس ملی فضای سایبر
۱-ب 1B	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	نشست تخصصی	**فلسفه هوش مصنوعی**	دکتر حمید محسنی	کارگروه فلسفه سایبر آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
۱-ج 1C	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	نشست تخصصی	**قانون حاکم بر فضای مجازی: نقدی بر ساختار فنی اینترنت**	دکتر عبدالله رجبی	دانشکده حقوق و بسیج دانشجویی دانشکدگان فارابی دانشگاه تهران
۱-د 1D	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	کارگاه آموزشی	**حکمرانی و آینده سیستم سایبورگ**	دکتر محمد اسماعیل عبداللهی	دانشکده حکمرانی دانشگاه تهران
۱-ه 1E	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	نشست تخصصی	**اقتصاد سیاسی فضای سایبر**	دکتر سید مهدی زریباف، دکتر حمیدرضا مقصودی، دکتر علی سعیدی	معاونت اقتصادی مرکز بررسی‌های استراتژیک ریاست جمهوری، دانشگاه قم و اندیشکده قصد
۱-و 1F	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	نشست تخصصی	**چالش‌های پیام‌رسان‌ها و شبکه‌های اجتماعی بومی**	دکتر مهدی انجیدنی	شرکت گپ و ویراستی
۱-ز 1G	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	کارگاه آموزشی	**تبدیل محتوای دینی به تولیدات رسانه‌ای**	دکتر محمدحسن احمدی، دکتر سید محمدعلی دیباجی، دکتر عبدالله متقی‌زاده، حسین عباسی‌فر	دانشکده الهیات دانشکدگان فارابی دانشگاه تهران؛ آزمایشگاه پژوهشی هنر و رسانه دینی «شهاب مبین»

سه‌شنبه ۹ آبان ۱۴۰۲ – ساعت ۱۵:۳۰ تا ۱۷:۱۵ – نشست‌های تخصصی و کارگاه‌های آموزشی (۲) – قم

کد نشست	زمان	نوع نشست	عنوان	سخنران / ارائه‌کننده	برگزار کننده
۲-الف 2A	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	کارگاه آموزشی	**معماری سازمانی بهینه با رویکرد امنیت اطلاعات**	مهندس سارا سعادت	اداره کل برنامه‌ریزی و معماری سازمانی دانشگاه تهران
۲-ب 2B	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	کارگاه آموزشی	**مبانی و الزامات انقلاب اسلامی در فضای مجازی**	آقای روح‌الله مومن‌نسب	ستاد امر به معروف و نهی از منکر استان تهران
۲-ج 2C	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	کارگاه آموزشی	**هوش مصنوعی و کاربردهای آن در پردازش محتوا**	مهندس احمد ربیعی‌زاده، مهندس حسین سنمار	مرکز تحقیقات کامپیوتری علوم اسلامی (نور)
۲-د 2D	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	نشست تخصصی	**فارنزیک دیجیتال: جرم‌شناسی و استنادپذیری ادله دیجیتال**	مهندس پارسا حاتمی، سرگرد مهدی ربیعی	پلیس فضای تولید و تبادل اطلاعات (فتا) فرماندهی انتظامی جمهوری اسلامی ایران (فراجا)
۲-ه 2E	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	نشست تخصصی	**هوش مصنوعی و تمدن اسلامی**	دکتر بهروز مینایی بیدگلی، دکتر محمدرضا قاسمی	ستاد هوش مصنوعی و رباتیک معاونت علمی، فناوری و اقتصاد دانش‌بنیان ریاست جمهوری و ستاد راهبری فناوری‌های هوشمند حوزه‌های علمیه
۲-و 2F	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	نشست تخصصی	**رصد، پایش و تحلیل فضای سایبر**	دکتر حمیدرضا کشاورز، آقای محمدرسول نصیرزاده، آقای محمدعلی دادگسترنیا	شرکت لایف‌وب
۲-ز 2G	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	نشست تخصصی	**نقد و بررسی فیلم سینمایی «اخت الرضا»**	عوامل سازنده فیلم و استادان حوزه هنر و رسانه دینی	آستان مقدس حضرت فاطمه معصومه (س) و دانشکده الهیات دانشکدگان فارابی دانشگاه تهران

نشست‌های تخصصی و کارگاه‌های آموزشی (تهران)

پنجشنبه ۱۱ آبان ۱۴۰۲ – ساعت ۰۸:۰۰ تا ۰۹:۴۵ – نشست‌های تخصصی و کارگاه‌های آموزشی (۳) - تهران

کد نشست	زمان	نوع نشست	عنوان	سخنران / ارائه‌کننده	برگزار کننده
۳-الف 3A	پنجشنبه ۰۸:۰۰ تا ۰۹:۴۵	کارگاه آموزشی	**هوش مصنوعی برای کسب‌وکار**	دکتر مسلم تقی‌زاده	کنفرانس ملی فضای سایبر
۳-ب 3B	پنجشنبه ۰۸:۰۰ تا ۰۹:۴۵	کارگاه آموزشی	**آینده امنیت سایبری**	آقای بهمن جهانی	دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی
۳-ج 3C	پنجشنبه ۰۸:۰۰ تا ۰۹:۴۵	نشست تخصصی	**بلاگرهای مد و زیبایی، الگوی فعالیت، آسیب‌ها و ابعاد حقوقی مواجهه با آنها**	سرهنگ علی محمد رجبی، سرهنگ سیروس دالوند	پلیس فضای تولید و تبادل اطلاعات (فتا) فرماندهی انتظامی جمهوری اسلامی ایران (فراجا)

پنجشنبه ۱۱ آبان ۱۴۰۲ – ساعت ۱۰:۰۰ تا ۱۱:۴۵ – نشست‌های تخصصی و کارگاه‌های آموزشی (۴) - تهران

کد نشست	زمان	نوع نشست	عنوان	سخنران / ارائه‌کننده	برگزار کننده
۴-الف 4A	پنجشنبه ۱۰:۰۰ تا ۱۱:۴۵	نشست تخصصی	**مدیاسایبرنتیک**	آقای سهیل سلیمی	آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
۴-ب 4B	پنجشنبه ۱۰:۰۰ تا ۱۱:۴۵	نشست تخصصی	**آب، غذا، اینترنت! هبوط انسان از حیات جسمانی به حیات سایبر**	دکتر محمد شمس‌الدینی	دانشگاه جامع امام حسین (ع)
۴-ج 4C	پنجشنبه ۱۰:۰۰ تا ۱۱:۴۵	کارگاه آموزشی	**مدیریت تهدیدات و آسیب‌پذیری‌های فناوری اطلاعات در سازمان‌های پیشرفته**	مهندس سارا سعادت	اداره کل برنامه‌ریزی و معماری سازمانی دانشگاه تهران

پنجشنبه ۱۱ آبان ۱۴۰۲ – ساعت ۱۳:۰۰ تا ۱۴:۴۵ – نشست‌های تخصصی و کارگاه‌های آموزشی (۵) - تهران

کد نشست	زمان	نوع نشست	عنوان	سخنران / ارائه‌کننده	برگزار کننده
۵-الف 5A	پنجشنبه ۱۳:۰۰ تا ۱۴:۴۵	نشست تخصصی	**نظم نوین جهانی، زمینه‌ساز جهان تک‌حکومتی یهود**	دکتر اسماعیل شفیعی سروستانی	مؤسسه فرهنگی هنری موعود
۵-ب 5B	پنجشنبه ۱۳:۰۰ تا ۱۴:۴۵	کارگاه آموزشی	**انتشارات علوم باز و دسترسی آزاد: چگونه فضای مجازی راه را برای برابری هموار می‌کند**	دکتر علیرضا صالحی‌نژاد	مرکز پژوهشی سیاست‌های فضای مجازی دانشگاه تهران
۵-ج 5C	پنجشنبه ۱۳:۰۰ تا ۱۴:۴۵	نشست تخصصی	**سیستم اعتبار اجتماعی**	مهندس علیرضا زینی	آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران

فهرست مقالات

فهرست نویسندگان

متن کامل مقالات فارسی

تأملی بر نحوه‌ی وجود سایبر

احسان کیان‌خواه[۱]

[۱]پژوهشگاه فرهنگ و اندیشه اسلامی
ehsan@kiankhah.com

چکیده

فضای سایبر یا به تعبیر دیگر فضای مجازی با شتاب هیجان‌انگیزی در حال گسترش و سایبری کردن همهٔ امور است. جلوه‌های متنوعی از فضای سایبر در حال خودنمایی است و این تغییرات سریع، مناظر جذاب بیشتری را پدیدار خواهد کرد. از اطلاع‌رسانی، رسانه‌واری و شبکه‌های اجتماعی تا تلفیق مجاز با عالم واقعی نمایشی از این جذابیت هیجان‌انگیز است. این هم‌گرایی فناوری‌های اجتماعی شده عالم نوپدیدی را شکل خواهد داد که طلیعه‌های قابل‌مشاهده و با آینده‌نگری و ژرف‌اندیشی به‌وضوح ابعاد آن قابل‌درک است. وجود شناسی، فضای سایبر با این جلوه‌های متنوع موجب ابتناء صحیح سیاست‌ورزی سایبر خواهد شد. محقق با روش توصیفی - تحلیلی به وجود شناسی سایبر پرداخته است. در این مقاله تلاش می‌شود که از دستگاه فلسفی صدرالمتالهین (ره) برای اکتشاف نحوه وجود سایبر استفاده شود. در ابتدا مختصری از مبانی حکمت متعالیه که ناظر به بحث وجود شناسی است، بیان‌شده و در ادامه کلیاتی از معنا و مفهوم فضای سایبر ناظر به بحث تبیین شده تا بتوان اطلاق‌های متعدد از فضای سایبر را شناسایی کرد. بر این اساس از یک منظر فضای سایبر به‌مثابه وجود رابط و فاقد ماهیت است. از وجهی دیگر، فضای سایبر همانند عرض کیف است. در برداشت سوم سایبر به‌مثابه یکی از جواهر قابل دسته‌بندی است و در نگاه چهارم، سایبر ظرف جدیدی از تحقق هم‌تراز وجود ذهنی و خارجی است. این استنباط به درک صحیح صیرورت فضای سایبر کمک خواهد کرد تا سیاست‌گذاری نافذی برای جهت‌دهی به سایبر شکل گیرد.

کلمات کلیدی: وجودشناسی، فضای سایبر، جوهر، عرض، وجود خارجی، وجود ذهنی، وجود سایبری.

۱ مقدمه

فضای سایبر در حال گسترش است. سرعت سایبری شدن پدیده‌های اطراف ما آن‌چنان با شتاب پیش می‌رود که یا باید منفعلانه تغییرات را نگریست، یا باید در مقابل این تغییرات ایستاد و یا باید همراهی کرد و بر شتاب تغییر افزود تا متهم به قدیمی بودن و بروز نبودن نشد. برون‌رفت از این سه رویکرد که هرکدام درصدی از انفعال را در خود دارد، نیازمند فهم صحیح پدیدهٔ سایبر دارد. این فهم، ادراک سطحی از فضای سایبر را که مبهوت و متحیر شدن از تغییرات فناوری می‌شود را می‌تواند به سمت به‌کارگیری هوشمندانهٔ فضای

سایبر سوق دهد. سایبر از واژهٔ سایبرنتیک اخذ شده است. سایبرنتیک لفظی یونانی و به‌معنای سکاندار است. سکاندار در عین حال که با مجموعه‌ای از حواس به رصد وضعیت محیطی و طبیعی حاکم بر کشتی و وضعیت محاطی و درون کشتی می‌پردازد، برای دستیابی به هدف و رسیدن به غایت ترسیم شده، سکان را به راست و چپ حرکت می‌دهد. از این‌رو سایبرنتیک که لفظ توسعه یافته در اوایل قرن بیستم میلادی است، به تبیین علم تصمیم، فرمان و کنترل در انسان وحیوان پرداخت. نوربرت وینر (Norbert Wiener) در سال ۱۹۴۸ کتابی با موضوع «کنترل و ارتباطات در حیوان و ماشین» (control and communication in the animal and the machine) نگاشت و عنوان کتاب را سایبرنتیک انتخاب کرد. وینر در این کتاب راهی برای شناخت شیوه تصمیم‌گیری و کنترل خودآگاه و ناخودآگاه حیوان ارائه کرد تا بر اساس آن بتوان سیستمی را طرح‌ریزی نمود که خودکار و خودکنترل کار کند. وینر برای این رشته‌ی جدید که تلفیقی از مهندسی برق، ریاضیات، زیست‌شناسی، فیزیولوژی اعصاب، انسان‌شناسی و روان‌شناسی بود، کلمه‌ای یونانی با مفهوم «هنرِ فرمان» (the art of steering) را که نمایش تعامل اهداف، پیش‌گویی، اقدامات، بازخورد و پاسخ در انواع سیستم‌ها است را برگزید (وینر، ۱۹۴۸). علم سایبرنتیک، علم ارتباطات و سیستم‌های کنترلی است که در حوزه ماشین‌ها و موجودات زنده موردبحث قرار می‌گیرد. سایبرنتیک به دنبال طرح‌ریزی ماشینی است که بافرمان و کنترل شبه انسانی قابلیت خودکنترلی دارد. خودکاری در سایبرنتیک با خودکاری کانسیونی (vaucansonien) متمایز است، خودکاری‌های قدیمی با ساعت کار می‌کردند و یک‌بار برای همیشه تنظیم می‌شد، اما خودکاری‌های جدید مبتنی بر سیستم‌های اطلاعاتی است که خود را با وضعیت‌های گوناگون تنظیم می‌کند (مورن، ۱۳۷۴: ۳۱۷-۳۱۸). این علم مبنایی برای دانش‌های کنترل، هوش‌مصنوعی و علم ارتباطات قرار گرفت و به دنبال تلفیق سیستم‌های نامتناجس برای ایجاد دستگاهی است که رفتار حیوانی را تقلید نماید[۱]. شبکه عصبی، الگوریتم ژنتیکی، الگوریتم اجتماع پرندگان، الگوریتم تپه نوردی و شیوه‌ها و الگوریتم‌های متنوع دیگر هوش مصنوعی، حاصل بررسی شیوه تصمیم‌گیری موجودات زنده است[۲]. جذابیت تصمیم و عمل و تلفیق شدن با لغت گنگ سایبرنتیک که از زبان یونانی وارد زبان انگلیسی شده بود، موضوع جذابی برای دانش متنوع قرار گرفت. این ابهام و در عین حال جذابیت و به تعبیر گیبسون که بکار برنده لفظ فضای سایبر در داستان علمی-تخیلی نورمنستر بود، لفظی مد روز (Buzzword) بود و گیبسون که به فلسفه و علم سایبرنتیک توجهی نداشت، صرفا به جذابیت و مد روز بودن این لفظ فکر می‌کرد (ویکی‌پدیا، بی‌تا). بر این اساس تبیین نگارنده از سایبر علی‌رغم اینکه شاید بتوان علوم و فلسفه شناخت، سایبرنتیک و اطلاعات را با برخی فناوری های سازنده یا توسعه دهندهٔ فضای سایبر مرتبط دانست، به صورت مستقل بوده و توجه به آن‌چیزی است که محقق شده، در حال توسعه روز افزون است و فضای سایبر نامیده می‌شود. در حقیقت فضای سایبر که نگارنده در حال بررسی نحوه وجود آن است، آن‌چیزی است که به صورت روزمره ما در حال استفاده از آن هستیم. فضای سایبر، فناوری‌های ممزوج با اجتماع و طبیعت است که در حال توسعه

[۱] درساخت سیستم سایبرنتیکی، هیچ لزومی ندارد که همه اجزاء مصنوعی باشد، ممکن است در کنترل یک سیستم مکانیکی مغز موشی را به‌جای پردازشگر الکترونیکی قرار دهند.

[۲] علی‌رغم ابداع الگوریتم‌هایی بر اساس مطالعه سیستم‌های طبیعی سیستم تصمیم‌گیری انسان و در سطح نازل‌تر حیوان ناشناخته و غیرقابل‌دسترس بوده است. دانشمندان بر اساس شناخت‌های جزیی که داشته‌اند این شیوه‌ها را ابداع نموده‌اند.

و سایبری نمودن همهٔ پدیده‌های طبیعی و مصنوعی است.

در این مقاله تلاش می‌شود که از دستگاه فلسفی صدرالمتالهین (ره) برای اکتشاف نحوه وجود سایبر استفاده شود. برای این منظور حالات متنوعی از فضای سایبر بررسی‌شده و وجودشناسی آن‌ها موردبررسی قرارگرفته است. این حالات موردبررسی، طیفی از گذشته تا آینده فضای سایبر است. برخی تعبیرات ممکن است منسوخ‌شده باشد و برخی دیگر تا تحقق کامل آن شاید سال‌ها باید صبر کرد. در ابتدا مبانی از حکمت متعالیه که ناظر به بحث وجود شناسی است، موردبررسی قرارگرفته و در ادامه فضای سایبر و قابلیت‌های آن موردبررسی شده و درنهایت تطبیق وجود و ماهیت بر سایبر موردبررسی قرارگرفته است. این استنباط به درک صحیح صیرورت فضای سایبر کمک خواهد کرد تا سیاست‌گذاری نافذی برای جهت‌دهی به سایبر شکل گیرد.

۲ مروری بر مبانی وجودشناسی در حکمت متعالیه

اصل اصالت وجود، محوری‌ترین اصل و اساس نظام فکری صدرالمتالهین است و این اصل سایر اصول و تمام مسائل فلسفی موردبحث در حکمت متعالیه را تحت تأثیر قرار می‌دهد. برای به دست آوردن دیدگاه کلی حکمت متعالیه در مباحث وجودشناسی و تأمل بر اساس آن در نحوه وجود فضای سایبر، ابتدا لازم است به‌طور مختصر به مهم‌ترین مباحث وجود شناسی حکمت متعالیه اشاره کرد[۳]. مهم‌ترین مبانی وجودشناسی حکمت متعالیه را می‌توان به‌قرار زیر تقریر نمود:

(۱) بداهت وجود و موجود: از دیدگاه ملاصدرا، موجود و وجود مفاهیمی بسیط و بدیهی هستند که ذهن برای فهم و اثبات آن‌ها نیازمند تعریف و برهان (استدلال) نیست، ازآن‌جهت که وجود و موجود، بسیط هستند، قابل‌تعریف نیستند (ملاصدرا، ۱۹۸۱، ج۱، ۲۵).

(۲) اشتراک معنوی و مفهوم تشکیک وجود: ملاصدرا به‌تبع ابن‌سینا (ابن‌سینا، ۱۴۰۴، ۳۴) وجود را مفهومی می‌داند که بر مصادیقش به‌صورت مشترک معنوی حمل می‌شود (ملاصدرا، ۱۹۸۱، ج۱، ۳۵). حمل به‌صورت مشترک معنوی به این معنی است که مفهوم واحد در تمام مصادیقش به یک معنا به‌کاررفته است. در مقابل، مفهوم مشترک لفظی است که در هرکدام از مصادیقش به معنای متفاوت از مصادیق دیگر به‌کاررفته است. اما مفهوم مشترک معنوی نیز به دودسته تقسیم می‌شود. برخی از مفاهیم مشترک معنوی، متواطی و برخی از آن‌ها مشکک هستند.

(۳) تمایز وجود از ماهیت : ازجمله مبانی دیگر وجودشناسی حکمت متعالیه، تمایز وجود از ماهیت است. علامه طباطبایی در نهایه الحکمه توضیح می‌دهد که با بررسی موجودات، دو مفهوم از آن‌ها در ذهن انسان متمایز می‌شود، مفهوم هستی یا وجود اشیاء و مفهوم چیستی یا ماهیت اشیاء (طباطبایی،

[۳] از آن جهت که هدف این مقاله استفاده از آراء ملاصدرا در وجودشناسی برای بررسی نحوه وجود فضای سایبر است، ورود تخصصی به آراء فلسفی و دیدگاه‌های ملاصدرا در دستور کار این مقاله قرار نمی‌گیرد و لذا به گزارش مختصر دیدگاه‌های وجودشناسی او و شارحانش بسنده شده است.

۱۳۸۲، ۹). از بین این دو مفهوم متمایزی که از یک شیء خارجی انتزاع می‌شود، تنها یکی از آن‌ها حاکی از مصداق خارجی است و دیگری مفهوم تبعی است که بالعرض با آن واقعیت انتساب پیدا می‌کند (جوادی آملی، ۱۳۷۵، بخش یکم از جلد اول، ۲۹۶). از دیدگاه ملاصدرا واقعیت خارجی، مصداق مفهوم هستی یا وجود است و ماهیات اموری تبعی هستند که از حدود و مراتب وجودات خارجی دریافت می‌گردد (همان،۲۹۶-۲۹۷). به‌عبارت‌دیگر بر اساس اصل اصالت وجود، آنچه در خارج تحقق دارد، وجود شیء است و بنابراین آثار خارجی یک شیء از ناحیه وجود آن شیء است.

(۴) تشکیک حقیقت وجود: مفهوم وجود، مفهومی است که در تمام مصادیق آن یعنی موجودات مشترک است و به یک معنا به‌کاررفته می‌رود. آنچه در خارج تحقق دارد، ما به حذاء مفهوم وجود یعنی حقیقت وجود است که عین خارجیّت بوده و آثار خارجی یک شیء متعلق به آن است. بر اساس این مبانی، همان‌گونه که مفهوم وجود مشترک معنوی است یعنی در همه موجودات به یک معنا بوده و تمایزی ندارد، منشأ انتزاع آن یعنی حقیقت وجود نیز امری واحد است و میان تمامی موجودات مشترک است.البته بر اساس اصل تشکیک حقیقت وجود، اشتراک موجودات در وجود، و تمایز و اختلاف آن‌ها نیز در وجود است. یعنی در عین اینکه وجود عامل اشتراک موجودات است، عامل تمایز و اختلاف آن‌ها نیز هست. به‌عبارت‌دیگر بر اساس تشکیک وجود، ما به الاختلاف به همان ما به الاشتراک برمی‌گردد. بر این اساس، وجود حقیقت واحد و درعین‌حال دارای مراتب است که اخلاف مراتب آن به‌شدت و ضعف وجود است (طباطبایی، ۱۳۸۲، ۱۷-۲۰).

(۵) تقسیم وجود به رابط و مستقل: یکی از اصول ابتکاری ملاصدرا که نقش مهمی در فهم نظام مابعدالطبیعی او دارد، تقسیم وجود به وجود مستقل و رابط است. از دیدگاه او در یک تقسیم‌بندی، وجود به دو قسم تقسیم می‌شود: الف: وجود مستقل که قائم بالذات است و به غیر خود وابستگی ندارد و ب: وجود رابط که قائم به نفس خود نیست بلکه قائم به غیر خود است (ملاصدرا، ۱۹۸۱، ج۱، ۷۸-۸۰). علامه طباطبایی معتقد است ممکنات را می‌توان به‌خودی‌خود و بدون در نظر گرفتن مبدء آن‌ها مدنظر قرارداد. در این اعتبار می‌توان نوعی استقلال برای ممکنات در نظر گرفت و لذا می‌توان با لحاظ این استقلال برای آن‌ها، ماهیتی قائل شد و لذا تقسیمات ممکنات ازجمله تقسیم به جوهر و عرض را بر آن‌ها جاری کرد (طباطبایی، ۱۳۸۲، ۳۰-۳۱). علامه طباطبایی در انتها و بر اساس مطالبات فوق، تقسیم‌بندی‌ای را برای موجودات ذکر می‌کند. در این تقسیم‌بندی وجود فی‌نفسه، یعنی وجودی که مستقل است به دو دسته لنفسه و لغیره تقسیم می‌شود. وجود لنفسه وجودی است که ماهیتش تنها عدم را از خودش طرد می‌کند همانند انواع تام جوهری (مثل انسان و فرس)؛ وجود لغیره وجودی است که موجودیتش برای موضوعش است و ماهیتش در عین اینکه عدم را از ذاتش طرد می‌کند، بعینه عدم را از ذات موضوعش نیز طرد می‌کند. همانند وجود اعراض و وجود صور نوعیه (طباطبایی، ۱۳۸۲، ۳۱-۳۳).

(۶) تقسیم موجودات به جوهر و عرض: در حکمت متعالیه نیز به‌تبع ارسطو و ابن‌سینا، موجودات به جوهر

و عرض تقسیم می‌شود. علامه طباطبایی در نهایه توضیح می‌دهد که هر ماهیتی به دو نحو ممکن است در خارج موجود باشد، حتماً باید در موضوعی موجود باشد که آن موضوع نیازی به آن ندارد. در مقابل، ماهیت جوهر، ماهیتی است که اگر در خارج موجود باشد، به موضوعی برای تحقق نیازمند نیست (طباطبایی، ۱۳۸۲، ۹۰). بر اساس تقسیم‌بندی که در بخش قبل ارائه شد، وجود جوهر، وجود لنفسه است که وجودش تنها از ذات خودش طرد عدم می‌کند و وجود عرض، وجود لغیره است که موجودیتش برای موضوعش است.

۳ چیستی فضای سایبر

بررسی نحوه وجود سایبر نیازمند توصیف مناسبی از فضای سایبر است که حالات مختلف آن را قابل‌تصور کند. ویلیام گیبسون در رمان علمی تخیلی نورومنسر با ابداع فضای سایبر (گیبسون، ۱۹۸۴: ۶۹) در شرایطی که شبکه‌ها و سامانه‌های کامپیوتری جهانی امروزی شکل نگرفته بود، فضای سایبر را این‌گونه معرفی کرد : «فضای سایبر یک توهم مورد وفاق است که روزانه میلیاردها اپراتور و کودکانی که مفاهیم ریاضی به آن‌ها داده می‌شود، آن را تجربه می‌کنند (بل، ۱۳۸۹: ۴۶). در حقیقت گیبسون فضایی را توصیف نمود که روح حاکم و حکم‌فرما بر آن، موجودی بسیار هوشمند بود که مفهوم سایبرنتیک[۴] و خودکاری را تداعی می‌کرد. برای فضای سایبر تعاریف متعددی ارائه‌شده است. این تنوع در تعریف نمایانگر پیچیدگی، ذوابعادی و تکامل تدریجی فضای سایبر است.

بر اساس تعاریف جدول ۱، فضای سایبر از منظر سخت‌افزاری و زیرساختی، شبکه‌ای جهانی از کامپیوترهای به‌هم‌پیوسته است که از طریق کانال‌های ارتباطی پرسرعت، و زیرساخت‌های رایانشی، خدمت نوینی را در مقابل انسان قرار داده است. اینترنت به‌عنوان یکی از جلوه‌های فضای سایبر به‌سرعت در حال گسترش است. سیستم‌های محاسباتی پنهان و توکار (Embedded) در حال قرارگیری در تمام اشیاء و محیط‌ها است. هر شیء ای که اطراف ما قرارگرفته به‌گونه‌ای قابلیت قرار دهی سیستم پردازش و هوشمند سازی را دارد. اینترنتِ اشیاء (Internet of things) در حال گسترش است و هر چیز و شیای در حال گرفتن IP و نشانه‌دار شدن و گرفتن هویتی از فضای سایبر است. پذیرش سریع گوشی‌های هوشمند نشان‌دهنده حرکت به سمت جامعه مبتنی بر اینترنت و اینترنتِ اشیاء است. اینترنت اشیاء بیانگر تعداد و تنوع اشیاء فیزیکی متصل‌به‌هم در بستر اینترنت است. در آینده‌ای نزدیک دیگر اتصال به اینترنت محدود به لپ‌تاپ یا گوشی‌های هوشمند نخواهد بود، در آن زمان دستگاه‌ها، اجسام و لباس‌هایی که در حال حاضر به اینترنت متصل نیستند، به شبکه جهانی از تعامل‌پذیری متصل خواهد شد. اتومبیل‌های خود راننده، اشیاء سایبری پوشیدنی و دستگاه‌های پزشکی همراه که به لحظه قابلیت به‌روزرسانی از راه دور توسط بیمارستان و مراکز نظارتی رادارند، گسترش خواهند یافت.

در سطح معنایی فضای سایبر، فضای زیست است. این زیست نوین که ابتناء یافته بر زیرساخت سایبری

[۴] علم سایبرنتیک، علم بررسی نحوهٔ تصمیم و عمل انسان و حیوان است. غایت این علم رسیدن به هوشمندی و ساخت سیستم‌هایی است که مشابه انسان و حیوان عمل کند.

جدول ۱: برخی تعاریف ارائه‌شده برای فضای سایبر

تعریف	مرجع
شبکه جهانی از زیرساخت‌های فناوری اطلاعات به هم وابسته، شبکه‌های مخابراتی و سیستم‌های پردازش کامپیوتری که یک ارتباط برخط در آن انجام می‌شود	راهبرد امنیت سایبر نیوزیلند، ۲۰۱۱
فضای سایبر یک حوزه عملیاتی است به‌منظور بهره‌برداری از اطلاعات از طریق سیستم‌های به‌هم‌پیوسته و زیرساخت یکپارچه آن‌ها، با استفاده از علم الکترونیک است	جوزف نای، ۲۰۱۰
یک دامنه سرتاسری در محیط اطلاعاتی است که شامل شبکه‌های مرتبط به هم از زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه‌های مخابراتی، سیستم‌های کامپیوتری، پردازنده‌ها و کنترلرهای توکار است.	وزارت دفاع آمریکا، ۲۰۱۱
یک مجموعه وابسته به زمان از سیستم‌های اطلاعاتی متصل‌به‌هم و کاربران انسانی است که با این سیستم‌ها تعامل دارند.	اوتیس (Ottis) و لورینت (Lorents)، ۲۰۱۰
جهان الکترونیکی به وجود آمده به‌وسیله شبکه‌های توکار از فناوری اطلاعات و اطلاعات موجود در آن شبکه است. یک مشارکت جهانی که بیش از ۷.۱ بیلیون نفر از افراد برای تبادل آرا، استفاده از سرویس‌ها و دوستی باهم در ارتباط هستند	راهبرد امنیت سایبر کانادا، ۲۰۱۰
فضای سایبر محیط الکترونیکی واقعی است که ارتباط انسان را به شیوه‌ای سریع، فرا جغرافیایی و با ابزارهای خاص مستقیم و زنده میسر می‌سازد، به عبارتی تئوری پیوند (ادغام) مکان در زمان، با تبدیل جهان جغرافیایی به دهکده جهانی، به‌صورت واقعی با رشد و گسترش فضای مجازی اتفاق می‌افتد.	عبدالهی، ۱۳۸۸
جهان موازی و خیلی واقعی و فیزیکی است که به‌واسطه اینترنت شبکه‌ای از ارتباطات کامپیوترهای سراسر جهان و خطوط ارتباطی پدید آمده است و در آن رابطه انسان و کامپیوتر پدیده نوینی را شکل داده که با شبیه‌سازی در موجودیت‌های «محیط فیزیکی، روانی – خیالی غوطه‌ور ساز، امکان تعامل و دادوستد در همه ابعاد و در تعاملات شبکه‌ای شده» بین افراد و آفریده‌های معنوی‌شان را ایجاد کرده است.	خانیکی و بابایی، ۱۳۹۱
یک جغرافیای ذهنی عام است که در مقابل، با اجماع و انقلاب، اصول و تجربه ساخته می‌شود. قلمروی‌ای که مملو از داده‌ها و کذب‌ها، مواد ذهنی و خاطرات طبیعت، با یک‌میلیون صدا و دو میلیون چشم در یک هماهنگی ساکت نسبت به تحقیق، انجام معامله، سهیم شدن در رؤیاها و مشاهدهٔ ساده است.	بل، ۱۳۸۹، ۲۳
فضای سایبر، دنیای دیجیتالی است که بر اساس فضاهای سنتی فیزیکی، اجتماعی و تفکر ایجاد شده است اما این تغییر تفاوت زیادی با فضاهای سنتی دارد.	هانشنگ نینگ، ۲۰۱۸

است، موجب تغییر، تحول یا انقلاب در پدیدها می‌شود. این فضای شکل یافته به هر پدیدهٔ عادت شده‌ای که برخورد می‌نماید یا منجر به تغییر ماهوی و بنیادی پدیده می‌شود و یا دست‌کم برخی تغییرات در آن ایجاد می‌کند. مفهوم روزنامه، خبرگزاری، ارتباطات اجتماعی، خریدوفروش، جهانگردی، آموزش، جنگ، منابع تولید قدرت و حوزه‌های متنوع دیگر انسانی قبل و بعد از عمومی شدن اینترنت و فضای سایبر تغییر یا تحول پیداکرده است. عالم نوین سایبری با همگرایی مجموعه‌ای از فناوری‌ها و قابلیت شکل می‌گیرد که بررسی و شناخت هرکدام می‌تواند در فهم «سایبری شدن» مؤثر باشد. قابلیت‌های متعددی برای فضای سایبر ترسیم کرده‌اند. همگرایی و همراهی این قابلیت‌ها ترسیمی از فضای سایبر آینده را نمایش می‌دهد. برخی از قابلیت‌های مهم فضای سایبر عبارت است از[۵]:

حافظه مجازی: مهم‌ترین خصوصیت مهم اینترنت ظرفیت بالای ذخیره‌سازی آن است و این فرصت را برای کاربرانش فراهم کرده است تا انباشتی از اطلاعات را در خود جای دهد (حافظ نیا، ۱۳۹۰: ۲۲). حجم اطلاعات دیجیتالی در زندگی و مناسبات روزمره در حال افزایش است. حافظه‌های ابری، حافظه‌های همیشه در دسترس در هر نقطه‌ای است که کاربر را از حمل سامانه‌ها و تجهیزات انتقال و ذخیره‌سازی اطلاعات فارغ می‌کند.

تعاملی بودن: سایبر رسانه‌ای چند طرفه است؛ به این معنا که هم تولیدکنندگان و هم مصرف‌کنندگان در تعامل باهم بر پیام مبادله شده تأثیر گذاشته و تأثیر می‌پذیرند. تعاملی بودن این فرصت را برای کاربران اینترنتی فراهم می‌کند که در برخورد با فضای اینترنت فرصت دخالت داشته و نظرات خود را دائماً ارائه و از نظرات دیگران نیز مطلع شوند (همان).

نامرئی بودن زیرساخت فضا: زیرساخت‌های فضای سایبر اگرچه فیزیکی بوده و در فضای واقعی قابل‌رؤیت و احساس است، ولی عملاً وجود چنین زیرساخت‌هایی برای کاربران نامحسوس و نامرئی است (دادج، (Dodge) ۲۰۰۸).

جهانی بودن فضا: هر فرد به‌عنوان کاربر در هر نقطه‌ای از جهان می‌تواند از طریق ورود به فضای سایبر به جدیدترین اطلاعات دست یابد و یا اطلاعات موردنظر خود را به اطلاع سایر کاربران برساند. این دسترسی همگانی، جهانی، گسترده، به‌روز و آزاد به اطلاعات برای همه کاربران معنی‌دار است (حافظ نیا، ۱۳۹۰: ۲۴).

واقعیت مجازی (Virtual reality): (همان) واقعیت مجازی محیط شبیه‌سازی‌شده در رایانه است که به کاربر امکان می‌دهد تجربه مشابهی همانند فضای فیزیکی در محیط مجازی داشته باشد تا بتواند با چالش‌های محیط حقیقی در محیط مجازی مواجه شود. واقعیت مجازی ابزار مناسبی برای آموزش سامانه‌های پرمخاطره است. سامانه‌های شبیه‌سازی کامپیوتری با نمایش‌دهنده‌های ۳۶۰ درجه، حسگرها

[۵] ویژگی‌ها یا قابلیت‌ها بیان شده ممکن است از ابتدا با سایبر بوده یا به مرور زمان به آن افزوده شده باشد.

(Sensors) و عملگرها (Actuators) محیط شبیه‌سازی‌شده را برای کاربر سامانه واقعیت پذیر می‌نماید. کاربر با سامانه‌های واقعیت مجازی حضور خود را در فضای سایبر ملموس‌تر حس می‌نماید.

واقعیت افزوده (Augmented Reality): افزودن داده‌های ذخیره‌شده در فضای سایبر به محیط فیزیکی واقعی است. سامانه‌های واقعیت افزوده عناصر درون دنیای واقعی را از طریق دریافت و پردازش اطلاعات که توسط حسگرهای ورودی صدا، تصویر و موقعیت جغرافیایی (GPS) جمع‌آوری‌شده و اطلاعات موقعیت (GIS) آن از شبکه استخراج‌شده به‌صورت برخط و به لحظه به نمایشگری که کاربر از طریق آن دنیای واقعی را می‌نگرد، می‌افزاید. در واقعیت افزوده معمولاً چیزی از محیط فیزیکی کاسته نمی‌شود بلکه فقط اطلاعاتی به آن ضمیمه می‌شود.

واقعیت ترکیبی (Mixed Reality): اشاره به اختلاط اشیاء مجازی با یک صحنه واقعی و سه‌بعدی دارد، یا معادل گنجاندن عناصر جهان واقعی در یک محیط مجازی است. نوع اول است به تقویت واقعیت با المان‌های اضافه‌شده، اشاره دارد و دومی به مجاز افزوده اشاره دارد (پن و همکاران، ۲۰۰۶). در حقیقت اختلاطی در خلق جهانی متفاوت است.

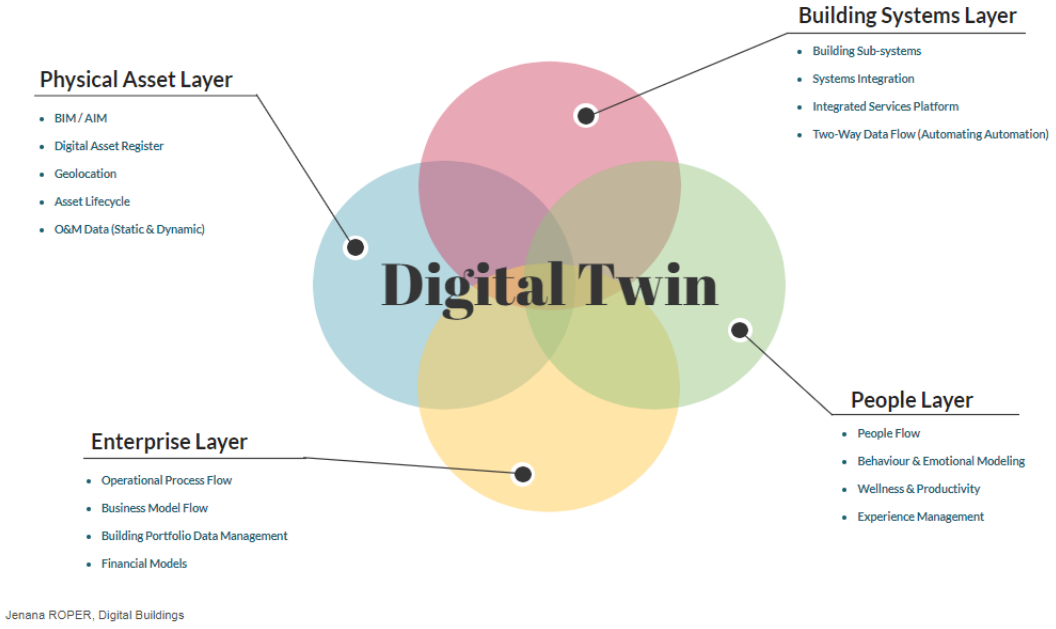
سایبر فیزیکی (Cyber Physical): سایبر هر شی‌ای را به سمت اتصال به شبکه پیش می‌برد. هر عنصری که در زندگی بشر به‌نوعی حضور دارد این قابلیت را داشته که در تعامل با سایر اشیاء قرار بگیرد. به‌عبارت‌دیگر هر شیء که به‌نوعی قابلیت قرار گرفتن در سیستم پردازش و هوشمند سازی پنهان و توکار را داشته باشد با نشان‌دار شدن و گرفتن IP، اینترنتِ اشیاء را شکل داده و به آن هویت سایبری می‌دهد. از طرفی اشیاء فیزیکی سایبر شده به دستان فیزیکی سایبر تبدیل‌شده و فرمان‌های سایبری پا را از فضای سایبر فراتر نهاده و به نقش‌آفرینی در محیط فیزیکی می‌پردازد.

همزاد دیجیتال (Digital Twin): همزاد دیجیتال، مدل دیجیتالی از موجودیت‌های واقعی و همزاد فیزیکی (همانند یک شیء، یک فرایند یا ساختارهای پیچیده) است. این مفهوم هم سایه‌ای دیجیتالی، همزاد فیزیکی است که بازتاب دهنده‌ی وضعیت/عملیات آن است و هم با گذشت زمان موجب تکامل همزاد فیزیکی می‌شود (ساراکو (Saracco)، ۲۰۱۹).

با توسعه و همگراشدن فناوری‌های سایبری در دهه‌های آینده و تصویری و ملموس شدن اشیاء سایبری با واقعیت‌های مجازی، افزوده و ترکیبی، فضای سایبر با ویژگی‌ها و آثار متمایزتری نمایان خواهد شد، که بررسی نحوه وجود سایبری در این گستره صورت خواهد گرفت.

۴ تطبیق فضای سایبر با مباحث وجودشناسی در فلسفه اسلامی

تشخیص نوع وجود سایبر تابع اطلاق و ترسیمی است که از فضای سایبر ارائه می‌شود. براساس تحقیقات و تحلیل‌ها از فضای سایبر، می‌توان چهار اطلاق یا تحقق برای آن در نظر گرفت:



شکل ۱: ابعاد سازنده‌ی همزاد دیجیتال (راپر (Roper)، ۲۰۱۸)

۱. واسطه‌ای بین اطلاعات (محتوی) و اشیاء (این اطلاق، اطلاقی منسوخ‌شده است؛ اما ازآنجایی‌که سیر گسترس سایبر را به تصویر می‌کشد مورد تحلیل قرارگرفته)،

۲. موجودیت فیزیکی سایبری (Cyber Physical Existence)،

۳. موجودیت سایبری محض (Cyber Pure Existence)،

۴. سایبر به‌مثابه عالم نوپدید (Cyber as New World).

در حقیقت، این چهار اطلاق یا تحقق، روندی از تکامل فضای سایبر از گذشته تا آینده را ترسیم می‌کند.

۱.۴ اطلاق اول، سایبر به‌مثابه رابط

توصیف: در اطلاق اول، می‌توان سایبر را به‌مثابه اتصال‌دهنده بین موجودیت فیزیکی و اطلاعات (محتوی) تصور کرد، یعنی به‌طور مثال زید دارای فشارخون خاص، شاخص‌های خونی ویژه خود و فیزیولوژی خاصی است که سایبر می‌تواند زید را به این اطلاعات ارتباط دهد. دیوان حافظ موجودیتی مکتوب دارد، حال سایبر استفاده کننده را به دیوان سایبر متصل می‌کند.

تطبیق: در این تعبیر اطلاعات و به بیان کامل‌تر محتوا جزئی از سایبر نیست بلکه محتوا در فضای دیگری تولیدشده و در معرض استفاده سایبر قرار می‌گیرد. این حد تعریف از فضای سایبر، حد نازل و گذشته‌نگر است.

بر این اساس همان‌طور که بیان‌شده، وجود رابط در هل مرکبه شکل می‌گیرد، وقتی چگونگی زید (به‌طور مثال از حیث فیزیولوژیکی) را بیان می‌کند، نوع وجود سایبر، وجود رابط (رابط بین موضوع و محمول) است زیرا در این شرایط مفهوم سایبر قائم به طرفین است و هیچ‌گونه استقلالی از طرفین خود ندارد و در آن‌ها مستهلک بوده وجودش فی‌غیره است. به بیان دیگر با نبود هریک از طرفین دیگر سایبری نخواهد بود و این همان وجود رابط است.

۲.۴ اطلاق دوم، موجودیت‌هایی با امتداد سایبری

توصیف: اطلاق دوم از تحقق سایبر، موجودیت‌های فیزیکی هستند که بُعد جدید سایبر در حال افزوده شدن به آن‌هاست. درختان طبیعی یک شهر برای نگه‌داری علمی و مبتنی بر ویژگی‌های ذاتی و منطقه‌ای، بُعد سایبری به آن افزوده‌شده است و باغبان در تعامل با درخت سایبری شده که وضعیت و شرایط درخت را بیان می‌دارد، به نگه‌داری‌اش می‌پردازد. ماشین‌ها در جاده‌ها و خیابان‌های درون و برون‌شهری هم با جاده در تعامل‌اند و هم با سایر وسایل نقلیه و رانندگان. کتاب‌ها با سایبری شدن اَبَر کتاب‌هایی را پدید آورده‌اند که به‌صورت زنجیروار مفاهیم را برای فهم ساده‌تر به هم پیوند زده است. انسان‌ها برحسب علاقه‌های باطنی و حقیقی خود هویت‌های جدیدی را برای خود رقم‌زده‌اند. ایده‌هایی نظیر همزاد دیجیتال برای موجودیت‌های سایبری، طرحی از این توصیف‌هاست.

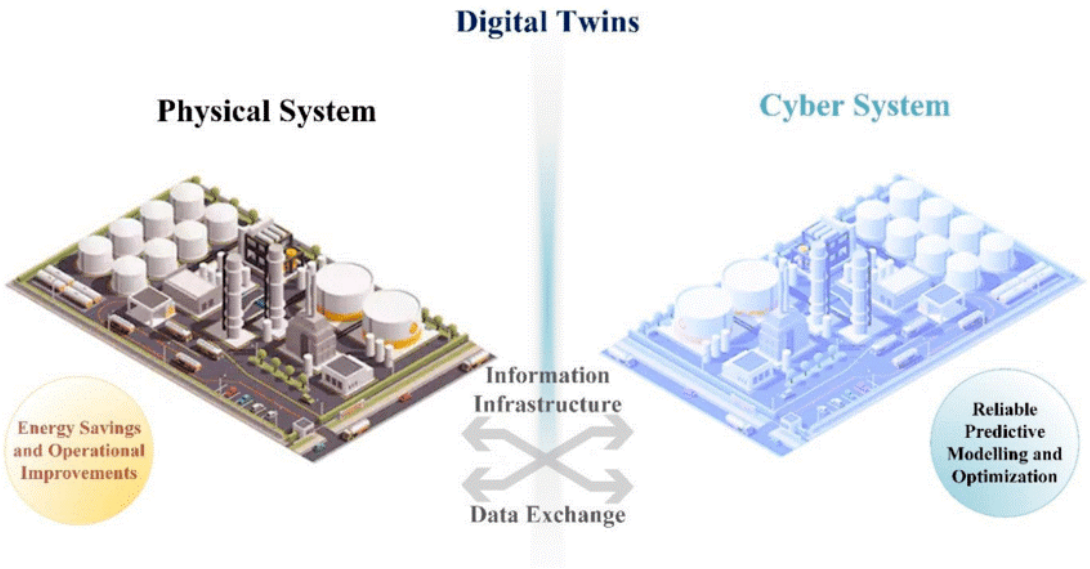
شهرها با طرح‌های هوشمندسازی خود در حال ساخت دوقلوهای دیجیتال خود هستند. ساخت امتداد دیجیتالی شهر به‌منظور راهبری و هدایت مؤثر شهر و حل معضلات ترافیکی، زیست‌محیطی،مدیریت بلایای طبیعی و انواع اقسام مسائل شهری است.وقتی دوقلوی دیجیتالی شهر ساخته می‌شود و داده‌های عظیم ذیل این شبیه‌سازی‌ها جمع‌آوری، پالایش و همگرا سازی می‌شود، پیش‌بینی و حل و برنامه‌ریزی برای عدم وقوع مشکلات آینده ساده‌تر خواهد شد. این تلاش‌ها مسیر را برای نحوه‌ی توزیع زیرساخت‌های شهری و برنامه‌ریزی و هدایت‌گری شهر و توسعه و رشد پایدار آن میسر می‌سازد (فولر (Fuller) و همکاران، ۲۰۲۰).

کارخانه‌ها دارای همزاد دیجیتالی می‌شوند. دوقلوی دیجیتال بر اساس داده‌هایی که ساختار فیزیکی خود می‌گیرد، میزان تولید، قیمت تمام‌شده، درجه‌ی کیفیت محصول، بازار آتی و هرآن چه در مسیر تداوم کسب‌وکارش مطرح هست را مدیریت می‌کند و شرایط تولید در کارخانه‌ی فیزیکی و ملموس تعیین می‌کند (همان).

تطبیق: با این توصیفات سایبر به‌مانند عَرَض کیف است. عَرَض است زیرا برای پدید آمدن نیاز به موضوع دارد و همیشه در چیز دیگری و برای چیز دیگری قابل تحقق است و مستقل نیست. کیف است زیرا نه از کمیّات است و نه نسبتی را بیان می‌کند بلکه عارض بر اشیاء فیزیکی شده و حالت نوینی را رقم‌زده است[۶]. این نوع وجود مستقل بوده و محمول واقع می‌شود ولی وجودش در شیء دیگر محقق می‌شود و وجودش فی‌نفسه لغیره است.

به‌بیان‌دیگر، اولاً در مثالی از کارخانه، امتداد دیجیتالی بویلر و دیگ بخار کارخانه‌ی تولید برق وابسته به

[۶] البته با اندک تامل عرض کم سایبری و اعراض نسبی سایبری قابل اکتشاف است. البته مفهم کم و نسبت سایبری شاید با تعاریف رایج فلسفی آن فاصله داشته باشد.



شکل ۲: همزاد دیجیتالی کارخانه (سین یانگ تنگ (Sin Yong Teng) و همکاران، ۲۰۲۱)

وجود بویلر فیزیکی است. زیرا این داده‌های بویلر فیزیکی است که بویلر دیجیتالی را می‌سازد، رشد می‌دهد و مستهلک می‌کند. ثانیاً، وجود مستقلی هم دارد زیرا می‌تواند با سایر همزادهای دیجیتالی کارخانه همانند شبکه توزیع برق، مخزن نگهداشت سوخت، وضعیت مخزن آب برای بخار شدن و به حرکت درآوردن توربین تولید برق، تعامل کند.

۳.۴ اطلاق سوم، موجودیت‌های محض سایبری

توصیف: واقعیت مجازی (Virtual reality) و در حالت کامل‌تر آن واقعیت ترکیبی (Mix Reality) دست به خلق موجودیت‌های سایبری زده که دیگر امتدادی از جنس موجودیت‌های فیزیکی ندارد بلکه خود دارای امتداد و اثری فیزیکی[۷] است. واقعیت ترکیبی، واقعیت متمایزی را شکل می‌دهد. این ترکیب، تلفیق واقعیت‌های متنوع سایبری چه از حیث فیزیکی و چه از حیث مجازی یا درون سایبری است. این قابلیت به متحد و یکپارچه شدن دنیای واقعی و دنیای دیجیتال منجر می‌شود (پایگاه چشم هوشمند (SmartEye)، ۲۰۲۰). این قابلیت به ساخت موجودیت‌های محض سایبری می‌انجامد و قابلیت تعامل موجودیت‌های فیزیکی را با موجودیت‌های محض سایبری ممکن می‌سازد.

دستیار سایبری محض استاد بر اساس سؤالات دانشجویان و پیشینهٔ علمی و تحقیقاتی، مباحث مرتبط را مشخص می‌کند، دستیار سایبری مذاکره‌کننده در جلسات تجاری و سیاسی به قدرت چانه‌زنی کمک کرده تا بر اساس پشتوانه‌های دانشی و پردازش‌های به‌لحظه، به تصمیم‌سازی کمک کند. گردشگرانی که

[۷] مسامحتا اصطلاح فیزیکی در مقابل سایبر قرار گرفته منظور عالم عادت شده است. منظور از امتداد و اثر فیزیکی عمل سایبری و تاثیر در عالم طبیعت است.

در اماکن تفریحی و گردشگری باراهنمایی ناملموس و سایبری برخورد می‌کنند و این راهنماها به معرفی مسیرها و آثار تفریحی می‌پردازد. موجودیت‌ها سایبری که با ابزارهایی نظیر عینک‌های مخصوص قابل‌درک و مشاهده هستند، دارای عرض و ارتفاع و عمق سایبری تطبیق داده‌شده با موجودیت‌های فیزیکی است. این‌ها نمونه‌هایی از موجودیت‌های تماماً سایبری است که برای پدید آمدن نیاز به موضوع ندارد بلکه خود پذیرندهٔ حالات متنوع است.

تطبیق: در این اطلاق، سایبر به‌مثابه سفیدی نیست که به ظرف تحقق نیاز داشته باشد، بلکه به‌مثابه جوهر مادی است که مستقل بوده و ظرف تحقق اعراض نیست. با این توصیف موجودهای سایبری محض به‌مثابه جوهر است که هم در صورت مادی جوهر دیگری حلول می‌کند و هم‌محل برای جوهر دیگری است. این انکشاف از سایبر نوعی جدیدی از جوهر را نمایان می‌سازد. این نحوه وجود سایبر در عین وجود، مستقل بوده و عدم را از ماهیت خودش طرد می‌کند و وجودش فی‌نفسه و لنفسه است. به بیان دیگر، در این تحقق، سایبر موضوعی است که محمولات متعددی بر آن تحقق می‌یابد. موجودیت‌هایی که اندازه‌ی سایبری خاص و صفات و کیفیت‌های متعدد دارند.

۴.۴ اطلاق چهارم، سایبر به‌مثابه عالمی فراگیر

توصیف: در اطلاق چهارم فضای سایبر به‌مثابه عالم نوپدید است. در جهانی بزرگ‌تر از جهان عادت شده و طبیعی، عالمی محاط و مشرف بر عالم عادت شده در حال شکل‌گیری است که انواع موجودیت‌های سایبری را در خود جای‌داده است. در این عالم نوپدید اشیاء و موجودیت‌های سایبر با یکدیگر در تعامل هستند. این موجودیت‌های سایبری یا امتدادی از عالم طبیعی (عالم فیزیکی و عالم ملموس) در عالم سایبر دارند و یا در سایبر متولدشده و جای گرفته است. این جهان هم‌اکنون نیز وجود دارد (در سطحی نازل‌تر نسبت به آینده بسیار نزدیک) کافی است با تغییر پارادایم و با ابزار متناسب با جهان موازی و متداخل با جهان طبیعی، سیر و صیرورت جدیدی آغاز می‌شود.

متاورس (Metaverse)، تحققی از عالم سایبری است. متاورس شبکه ای از جهان‌های مجازی سه بعدی است که بر ارتباطات اجتماعی متمرکز است (نیوتن ،(Newton) ۲۰۲۱). این ارتباطات تصویری شده با فناوری‌های متعدد سایبری، شق نوینی از تعاملات و زیست را پدید آورده است.

تطبیق: در این نوع اطلاق، می‌توان برای سایبر ظرفی هم‌تراز با دیگر ظروف تحقق موجودات قائل شد. یعنی وقتی گفته می‌شود درخت هست، این وجود داشتن ممکن است خارجی یا ذهنی باشد، اما همین درخت در عین داشتن وجودی در خارج و تحقق عینی؛ یا وجود در ذهن، ممکن است در سایبر نیز تحقق داشته باشد. در اینجا عالم سایبر به پدیدهٔ درخت نوعی «هستی» می‌بخشد. به‌عبارت‌دیگر، درخت، تحققش و هستی‌اش از سایبر گرفته و دارای آثار خاص خود است. در این شرایط شاید بتوان هستی بخشیدن سایبر را ظرف تحققی هم‌تراز با وجود خارجی و وجود ذهنی دانست.

بر این اساس، هرچند به عقیدهٔ غالب حکمای اسلامی هر ماهیتی دو گونه وجود خارجی و ذهنی دارد، اما شاید بتوان براساس آن‌چه استدلال شد، ظرف تحقق یا وجود سومی نیز تصور کرد که از سایبرساخت شدن ماهیت‌ها قابل استنباط است و به عبارت دیگر، شاید بتوان گفت که وجود سایبری نحوه‌ای از وجود ماهیات

است که دارای آثار خاص و ویژه‌ای بر گرفته از فضا و عالم سایبرْ ساخت است و متفاوت از وجود ذهنی و خارجی است.

ممکن است این اشکال مطرح شود که می‌توان وجود سایبری را از اقسام وجود خارجی برشمرد. زیرا ظرف تحقق وجود سایبر، خارج از ذهن است، لذا نوعی وجود خارجی است. در پاسخ باید گفت که آثار وجود خارجی متباین از آثار وجود سایبری است. برای مثال درختی را بررسی می‌کنیم که هم به وجود خارجی و هم به وجود سایبری موجود است. وجود خارجی درخت، میوه مأکول می‌دهد و برای رشد به آب‌وخاک حاصلخیز نیاز دارد؛ اما درخت سایبری خود این آثار را ندارد و دارای حجم و ارتفاع سایبری خاص خود بوده و تعامل‌پذیر است، یعنی می‌توان از وضعیت رشد آن در طی دوره‌های زمانی پرسش نمود، وضعیت جاری، میزان آب مورد نیاز، احیانا آفاتی که درخت دارد را مشاهده نمود و با درخت با تکنیک‌های واقعیت افزوده و واقعیت ترکیبی تعامل سایبری کرد. حال آن‌که آثار درخت در عالم محسوسات این‌گونه نیست.

علاوه بر این، همانطور که بیان شد، موجودات محض سایبری وجود دارند که ظرف تحقق آن‌ها صرفاً در فضای سایبر است. به طور مثال استادیار سایبری که به ارائهٔ اثربخش کلاس کمک می‌کند یا ربات نرم‌افزاری[۸] که مدیریت کارخانه و خط تولید را بر عهده دارد، فاقد وجود خارجی است، ولی در عالم سایبر دارای ویژگی‌ها و تحقق خاصی است که در عالم تحقق خارجی قابل مشاهده نیست. البته باید توجه داشت که اشیاء سایبری فارغ از آثار خاصشان در فضای سایبر، می‌توانند در عالم تحقق خارجی نیز تاثیر گذار باشند. به عنوان مثال، مدیر سایبری محض یک خط تولید در عالم خارج دارای آثاری خارجی همانند متوقف کردن تولید یا بالا و پایین بردن درجهٔ حرارت یک کوره است که از این آثار خارجی می‌توان به وجود و آثار سایبری آن پی برد.

۵ جمع‌بندی و نتیجه‌گیری

مفهوم سایبر در عین سادگی و درک عمومی دارای ابعاد و گستره‌ای ناشناخته است. فضای سایبر عالم نوپدیدی است که طلیعه‌هایی از آن آشکارشده است. عالم نوپدید سایبر نه به‌مثابه عوالمی که حکما از آن یاد می‌کنند بلکه عالم جدید از زیست و زندگی، تحقق موجودات است که تاکنون بشر آن را تجربه نکرده است. این عالم نوپدید در مقابل عالم عادت شده‌ای است که بشر سال‌ها آن را تجربه کرده است. انقلاب کشاورزی و انقلاب صنعتی و تحولات فناورانه ازاین‌دست، همیشه بخشی از عالم محسوسات ما را تغییر داده است؛ به‌عنوان مثال با قوانین فیزیکی خودرو طراحی‌شده، نیروگاه برق تولید شده، نفت استخراج و پالایش‌شده، کشتی روی آب غوطه‌ور شده و هواپیما در آسمان به پرواز درآمده است، اما هم‌اکنون در عالم نوپدید سایبر، می‌توان بر اساس قوانین عالم خیال مصنوعات و محسوساتی را ساخت که دارای آثار سایبری و خارجی هستند. این‌ها تحولات ژرف عالم نوپدید است که با تعاریف ساده از فضای سایبر یا فضای مجازی قابل‌ادراک نیست.

عالم نوپدید سایبر در حال بلعیدن عالم کنونی و شکل دادن زیستْ‌جهانی نوین بر پایه فناوری، شتاب و همگرایی است که همهٔ رفتارهای فردی و اجتماعی را در خود جای‌داده و بزرگ‌تر از عالم عادت شده کنونی

[۸] ربات نرم‌افزاری، برنامهٔ مبتنی بر هوش مصنوعی است که براساس داده‌های مرتبط، پایگاه دانش خود و موتور استناج تعبیه شده، به تصمیم‌سازی و تصمیم‌گیری و عمل سایبری یا غیر سایبری می‌پردازد.

جدول ۲: جمع‌بندی نحوه وجود سایبر

موجودیت	توصیف	نحوه وجود
رابط	اتصال‌دهنده بین اشیاء و اطلاعات	وجود رابط - فاقد ماهیت
موجودیت فیزیکی سایبری	موجودیت‌های فیزیکی که امتداد سایبری دارند	به‌مثابه عرض
موجودیت محض سایبر	موجودیت‌های سایبری محض که امتداد فیزیکی دارد	به‌مثابه جوهر
سایبر به‌مثابه عالم نوپدید	هستی‌بخش هم‌ارز وجود ذهنی، خارجی	وجودی جدید

است، زیرا هر مفهوم و هر پدیده‌ای در این عالم نوپدید دارای بطن‌های مختلف و متنوعی است. عالم سایبر که ما هم‌اکنون در حال گذار و حرکت به سمت آن هستیم، پدیده‌های طبیعی را سایبری می‌کند. خودروی سایبری، کارخانه سایبری، شهر سایبری، پتروشیمی سایبری و حتی درخت سایبری که دارای امتدادی در فضای سایبر هستند و غیر از کنش‌گری در عالم عادت شده با تحقق سایبری‌اش، کنش سایبری نیز دارند. مفاهیمی همچون واقعیت مجازی با کمک سایبر فیزیکال و اینترنت همه‌چیز در حال ساختن اثر فیزیکی برای اجسامی کاملاً سایبری هستند. کمک‌کننده به استاد برای اثربخشی آموزش، دستیار سایبری مذاکره‌کننده برای بیان سطوح پیچیده و کشف ابعاد مذاکره، تصمیم‌سازی راهبردی برای معمار سازمان و فرمانده نظامی یا هر آنچه شما در خیال و تصور خود بسازید، قابلیت تحقق سایبری با اثر فیزیکال دارد.

آنچه از بحث بالا قابل استنباط است، نحوه جدیدی از وجود است که تاکنون فهم نشده است. در این عالم نوپدید موجودات زنده و تعامل‌پذیر سایبری زیست می‌کنند که یا از عالم طبیعی وارد این عالم جدید شده و وجود سایبری پیداکرده‌اند یا در خود عالم سایبر شکل یافته و رشد و نمو می‌کنند. این موجودات سایبری به‌مانند همهٔ موجودات دو حیث وجودی و ماهوی دارند.

در این مقاله پس از اشاره‌ای کوتاه به مباحث موجودشناسی در حکمت متعالیه و تأملاتی در شناخت سایبر، در نهایت چهار اطلاق در خصوص موجودات سایبری ارائه شد و کوشش شد تا این چهار اطلاق با نحوه وجود موجودات در فلسفه اسلامی تطبیق داده شود.

سه اطلاق اول بسته به نوع تحلیل آن‌ها می‌توانند منطبق بر وجود رابط، وجود عرض برای جوهر و یا وجود جوهر باشد. اما علاوه بر تطبیق اطلاق‌های مختلف موجود سایبری بر یکی از انواع وجود فی‌غیره یا وجود فی‌نفسه، می‌توان در اطلاق چهارم ظرف وجود سایبری را نیز بررسی کرد. به نظر می‌رسد وجود سایبری نه کاملاً در ظرف موجود ذهنی موجود است و نه در ظرف موجود خارجی و با وجود اینکه در سنت فلسفهٔ اسلامی بین موجود خارجی و موجود ذهنی واسطه‌ای نیست، به نظر می‌رسد برای تحلیل موجود سایبری باید به‌گونه‌ای از موجود نظر داشت که نه خارجی‌ست و نه ذهنی و هم خارجی است و هم ذهنی. تدقیق و تأمل بیشتر در خصوص این نوع موجود می‌تواند مساله ارزشمندی برای پژوهش‌های آتی باشد.

فهم این‌گونه از سایبر و تحلیل آن به مثابه پدید آوردن عالمی که اشیاء هم تاثیرات وجودی در عالم ذهن

دارند و هم تاثیرات وجود در عالم خارجی و دارای تاثرایت اختصاصی خود نیز هست درکی بالاتر از آن‌چه که هست در تنظیم نظریه‌های سیاستی و حکمرانی سایبری پدید می‌آورد. تبیین این نگرش سایبر را نه سایبر را به مثابه فناوری‌های منضم شده به‌هم می‌داند و نه فناوری اجتماعی و رسانه‌ای بلکه مبدع عالمی با ویژگی‌های خاصی برای زیست است.

مراجع

[۱] ابن سینا (۱۴۰۴ هـ.ق.)، الشفاء، الالهیات، مقدمه: ابراهیم مدکور، تحقیق الاب قنواتی و سعید زاید، قم، مکتبة آیة الله المرعشی،

[۲] بل، دیوید (۱۳۸۹)، درآمدی بر فرهنگ سایبر ۲۰۰۱، ترجمه مسعود کوثری ، حسین حسنی ، چاپ اول، تهران، انتشارات جامعه شناسان.

[۳] جوادی آملی، عبدالله (۱۳۷۵)، رحیق مختوم، قم، اسراء.

[۴] حافظ‌نیا، محمدرضا (۱۳۹۰)، جغرافیای سیاسی فضای مجازی، تهران، انتشارات سمت.

[۵] خانیکی، هادی و بابایی، محمود (۱۳۹۱)، تأثیر سازوکارهای ارتباطی اینترنت بر الگوهای تعامل کنشگران فضای سایبر ایران، فصلنامه علمی - پژوهشی علوم اجتماعی، سال نوزدهم، شماره ۵۶، صفحات ۷۳-۱۱۶.

[۶] عبدالهی، حسین (۱۳۸۸)، اینترنت بستری برای جنگ نرم، برداشت از پورتال کتابخانه الکترونیکی دانشگاه عالی دفاع ملی.

[۷] علامه طباطبایی (۱۳۸۲). نهایة الحکمة.

[۸] فیروزآبادی، ابوالحسن (۱۳۹۴)، تحولات اجتماعی و فرهنگی برآمده از توسعه فناوری ارتباطات و اطلاعات، تهران، انتشارات دانشگاه عالی دفاع ملی.

[۹] ملاصدرا (۱۹۸۱). الحکمة المتعالیة فی الاسفار العقلیة الاربعة، چاپ دار الاحیاء العربی. مورن، ادگار (۱۳۷۴)، روش طبیعتِ طبیعت، ترجمه علی اسدی ، جلد اول ، چاپ اول، تهران، انتشارت سروش.

[10] Canada's Cyber Security Strategy (2010), Cyber Security Strategy, Canada, Public Safety.

[11] Cyberspace (n.d.). Retrieved March 17, 2021, from https://en.wikipedia.org/wiki/Cyberspace.

[12] Department of Defense (2011) Department of Defense Strategy for Operating in Cyberspace. April. Available at: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[13] Dodge, M. (2008). Understanding cyberspace cartographies: a critical analysis of internet infrastructure mapping, University of London.

[14] Fuller, aidan, Zhong Fan, Charles Day, and Chris Barlow (2020). Digital Twin: Enabling Technologies, Challenges and Open Research. IEEE

[15] Gibson, William (1984). Neuromancer. New York: Ace Books. p. 69

[16] Joseph S. Nye, Jr. (2010). Cyber Power. Harvard Kennedy School.

[17] New Zealand Cyber Security Strategy (2011), New Zealand.

[18] Newton, Casey (2021-07-22). "Mark Zuckerberg is betting Facebook's future on the metaverse". The Verge. Archived from the original on 2021-10-25. Retrieved 2021-10-25.

[19] Ning, Huansheng and Mohammed Amine Bouras, Dawei Wei, and Mahmoud Daneshmand (2018). General Cyberspace: Cyberspace and Cyber-enabled Spaces. IEEE Internet of Things Journal

[20] Ottis, R. and P. Lorents (2010). Cyberspace: Definition and implications. International Conference on Cyber Warfare and Security, Academic Conferences International Limited.

[21] Pan, Z., et al. (2006). "Virtual reality and mixed reality for virtual learning environments". Computers & Graphics 30(1): 20-28.

[22] Roper, Jenana (2019). BIM vs Smart Building vs Digital Twin. https://proptech.zone/bim-vs-smart-building-vs-digital-twin-what-is-the-difference/

[23] Saracco, Roberto (2019). Digital Twins: Bridging Physical Space and Cyberspace. IEEE

[24] SmartEye (2020). Mengenal Mixed Reality dan Prediksi Penerapannya di Indonesia. Viewed January 2022. https://www.smarteye.id/blog/mengenal-mixed-reality-dan-penerapannya/

[25] Yong Teng, Sin and Michal Tous and Wei Dong Leong and Bing Shen How and Hon Loong Lam and Vít˘ezslav M´a˘sa (2021). Recent advances on industrial data-driven energy savings: Digital twins. Renewable and Sustainable Energy Reviews 135.

[26] Wiener, Norbert (1948). Cybernetics: Or Control and Communication in the Animal and the Machine.

طراحی و پیاده‌سازی یک مدل هوشمند پرسش و پاسخ برای کووید۱۹

صادق احمد آخوندی[۱]، سعید شیری قیداری[۲]، محمدحسن شیرعلی شهرضا[۲]

[۱] کارشناس ارشد علوم کامپیوتر، هوش مصنوعی و محاسبات نرم، دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیر کبیر (پلی تکنیک تهران)، تهران
sadegh.akhondi@aut.ac.ir
[۲] استادیار، دانشکده ریاضی و علوم کامپیوتر دانشگاه صنعتی امیر کبیر (پلی تکنیک تهران)، تهران
{shiry,hshirali}@aut.ac.ir

چکیده

از زمان ظهور شیوع کووید ۱۹ در چین در سال ۲۰۱۹، این ویروس به سرعت در سراسر جهان گسترش یافته است و بیش از ۷۶۷/۵ میلیون نفر را تحت تأثیر قرار داده و به طور غم انگیزی جان بیش از ۶/۹ میلیون نفر را گرفته است. همانطور که مجلات علمی در تلاش هستند تا با انتشار اطلاعات جدید و دقیق در جهت مبارزه با این پاندمی جهانی اقدام نمایند. همزمان حجم انبوه مقالات و ادعاهای نادرست، چالش‌های مهمی را در دسترسی به داده‌های قابل اعتماد ایجاد کرده است. در این تحقیق، یک سیستم الگوریتمی خواننده-بازیاب دوگانه جدید با استفاده از مدل Pubmedbert توسعه داده شده است. این سیستم پیشرفته نیاز به اطلاعات دقیق را با پاسخ‌گویی مؤثر به سؤالات مرتبط با کووید ۱۹، کمک به شناسایی ویروس و بیماری، تسهیل اقدامات واکنش سریع، و مهار عفونت‌ها و انتقال بیشتر برطرف می‌کند. از طریق ادغام سیستم پاسخگویی به سؤال تدوین شده و مدل قدرتمند PubMedbert، این سیستم به نرخ دقت چشمگیر ٪۸۰/۱۴۸ دست یافته است. این نتایج عملکرد قوی سیستم را در پردازش و ارائه اطلاعات قابل اعتماد نشان می‌دهد، بنابراین در مبارزه با همه‌گیری و هدایت تصمیم‌گیری مبتنی بر شواهد مؤثر واقع خواهد شد.

کلمات کلیدی: هوش مصنوعی، سیستم پاسخ به پرسش، سیستم بازیابی سند، کووید ۱۹، مدل برت، مدل پابمد برت.

۱ مقدمه

عفونت‌های کووید-۱۹ با عنوان قبلی (2019_nCoV)، اولین بار در دسامبر ۲۰۱۹ در ووهان چین شناسایی شد و انتقال سریع در جامعه را با نرخ شیوع بالا نشان داد. همگانی شدن کوویید ۱۹ موجب شد تا سازمان بهداشت جهانی (WHO)، آن را بیماری همه‌گیر (پاندمی) اعلام نماید [۱]. این ویروس تا ژوئن ۲۰۲۳، بیش

از ۷۶۷٫۵ میلیون نفر را مبتلا نمود و باعث مرگ بیش از ۶٫۹ میلیون نفر در سراسر جهان شد [۲]. شدت این بیماری بسته به نوع علائم خفیف تا حاد تنفسی، متفاوت است و خطر قابل توجهی جمعیت‌های آسیب‌پذیر –از جمله افراد مسن و کسانی که بیماری‌های زمینه‌ای دارند– را تهدید می‌کرد.

بر این اساس، از یک سو، دانشمندان و متخصصان بهداشتی در تلاش بودند تا با مطالعه ویروس و توسعه آزمایش‌های تشخیصی به درک دینامیک انتقال، کشف درمان‌های بالقوه و توسعه واکسن‌های ایمن و مؤثر دست یابند. از طریق بسترهای دیجیتال و اشتراک‌گذاری داده‌ها و یافته‌های تحقیقاتی مرتبط، زمینه ارتباط و تبادل نظر را تقویت کرده و سرعت تحقیقات را افزایش دادند. حجم انبوه نشریات و مقالات علمی مرتبط که با سرعتی تصاعدی افزایش می‌یافت، تلاش‌های دستی دانشمندان را برای ردیابی، تجزیه و تحلیل و ترکیب یافته‌های مرتبط مشکل کرد و مانع از دستیابی متخصصان مراقبت‌های بهداشتی، سیاست‌گذاران و محققان به آخرین پیشرفت‌های علمی شد. روش‌های سنتی در مواجهه با همه‌گیری کووید–۱۹ با محدودیت‌های قابل توجهی روبرو بودند. همچنین، ماهیت پویای این بیماری همه‌گیر، دسترسی بلادرنگ به آخرین تحقیقات را ضروری می‌ساخت. دستیابی به حجم گسترده اطلاعات و فراهم نمودن توانایی ارائه پاسخ‌های به‌روز، مفید، مطمئن، مناسب و صحیح به سؤالات مرتبط با کووید–۱۹، نیازمند تلاش سازمان‌های بین‌المللی و مؤسسات علمی معتبر بود تا اطلاعات دقیق را از طریق منابع معتبر در دسترس کارشناسان و عموم مردم قرار دهند. دولت‌ها، متخصصان مراقبت‌های بهداشتی، پژوهشگران، سازمان‌های رسانه‌ای و مردم نقش موثری در ترویج اطلاعات دقیق و مقابله با اطلاعات نادرست داشتند تا تأثیر منفی آن را بر بهداشت عمومی کاهش داده و در راستای مهار گسترش ویروس کرونا اقدام نمایند.

از سوی دیگر، دانشمندان و متخصصان هوش مصنوعی، به‌ویژه در زمینه پردازش زبان طبیعی (NLP) با تلفیق تکنیک‌های یادگیری ماشین، راه‌حلی دگرگون‌کننده را برای غلبه بر چالش‌های ناشی از مشکلاتی نظیر همه‌گیری کووید–۱۹ و بحران‌های مشابه پیشنهاد دادند. استفاده از الگوریتم‌های هوش مصنوعی، غربال و دسته‌بندی حجم وسیعی از ادبیات علمی را به‌طور مؤثر ممکن ساخت. این تکنیک‌ها زمینه استخراج اطلاعات کلیدی را فراهم کرده و بدین ترتیب، بینش‌های ارزشمندی را برای تحلیل و تصمیم‌گیری مبتنی بر شواهد، در اختیار دانشمندان قرار می‌دادند. همچنین، NLP پیشرفت‌های چشمگیری در سیستم‌های پاسخگویی به سؤالات داشت که توانمندی مدل‌ها و سیستم‌های مختلف هوش مصنوعی را به‌خوبی نمایان می‌ساخت. به عنوان مثال، توسعه مدل‌های زبان از پیش آموزش‌دیده در مقیاس بزرگ مانند BERT و GPT، عملکرد وظایف پاسخ‌گویی به سؤال را بسیار توانمند نموده و بهبود می بخشید. این مدل‌ها از معماری‌های یادگیری عمیق و حجم وسیعی از داده‌های متنی برای ارائه پاسخ‌های دقیق و متنی استفاده می‌کردند [۳]. بر این اساس، استفاده از تکنولوژی هوش مصنوعی به عنوان راه‌حل مناسب برای مقابله با همه‌گیری کووید–۱۹ و بحران‌های مشابه در آینده مطرح شده است. با بهره‌گیری از قابلیت‌های هوش مصنوعی، امکان تجزیه و تحلیل همزمان از جدیدترین و دقیق‌ترین یافته‌های علمی از میلیون‌ها نشریه علمی در دسترس، تصمیم‌گیری به‌موقع و آگاهانه در واکنش به بیماری همه‌گیر ممکن می‌شود. ادغام هوش مصنوعی با سیستم دستیابی به پاسخ از حجم بالای اطلاعات مرتبط با بیماری همه‌گیری نظیر کووید–۱۹، امکان دسترسی به آخرین اطلاعات مرتبط و مناسب را فراهم می‌آورد. این فرآیند می‌تواند حجم زیادی از اطلاعات پیچیده و پراکنده

را استخراج، درک و تحلیل نماید. از منابع مختلف نظیر مقالات علمی، گزارش‌ها و داده‌های آماری اطلاعات مفید جمع‌آوری و تفهیم شود. درک صحیح و دقیق از سؤالات و تفسیر صحیح آن‌ها، همچنین مدیریت ابهامات می‌تواند با استفاده از تکنیک‌ها و الگوریتم‌های موجود، توانایی پاسخگویی به سؤالات متنوع را فراهم آورد. رسیدن به یک سیستم پاسخ به پرسش، نیازمند داشتن یک مخزن اطلاعاتی مرتبط و قابل اعتماد است. الزویر یکی از بزرگترین و برترین انتشارات علمی معتبر و معروف جهان در زمینه علوم پایه و پزشکی است که فقط مقالات با کیفیت و معتبر، با رتبه‌بندی بالا و بازبینی شده (peer-reviewed) را در مجلات زیر پوشش خود از طریق PubMed، Scopus و Web of Science منتشر می‌کند.

هدف اصلی این پروژه، افزایش توانمندی سیستم پرسش و پاسخی است که با استفاده از سیستم هوش مصنوعی، امکان دستیابی به آخرین اطلاعات تخصصی منتشرشده در زمینه بیماری کووید-۱۹ را فراهم نماید. این ابزار هوش مصنوعی با تنظیم دقیق مدل‌های زبانی پایه، نتایج بهتری در زمینه‌های پیشگیری، درمان و کنترل این بیماری همه‌گیر ارائه می‌دهد. برای دستیابی به این اهداف، مدل‌های زبانی پایه مختلف مورد بررسی قرار گرفته و بهترین آن‌ها انتخاب می‌شوند. مدل پایه با استفاده از روش ماسک کردن آموزش دیده و با تنظیم دقیق (Fine-tune) روی داده خاص، برای انجام وظایف مدنظر تنظیم می‌شود. سپس، پس از پیش‌پردازش، مدل زبانی پایه بر روی مقالات مرتبط با کووید-۱۹ تنظیم دقیق می‌شود. با استفاده از مدل زبانی پایه و مجموعه داده SQuAD، آموزش پرسش و پاسخ انجام می‌شود و مدل نهایی با استفاده از مجموعه داده پرسش و پاسخ کووید-۱۹ تنظیم دقیق می‌گردد. در نهایت، مدل ارائه‌شده با چهار معیار دقت (Precision)، یادآوری (Recall)، امتیاز F1 (F1 score) و تطبیق دقیق (Exact Match) ارزیابی می‌شود. این مقاله نه تنها یک مجموعه داده را بررسی می‌کند بلکه مفاهیم و تحقیقات مرتبط با این بررسی را مورد بررسی قرار می‌دهد. در ابتدا، به مفاهیم پایه‌ای و مرتبط پرداخته شده و سپس به بررسی مطالعات قبلی در حوزه سیستم‌های پرسش و پاسخ، به‌ویژه در حوزه پزشکی و کووید-۱۹، می‌پردازد. در پایان، گزارشی از نتایج این بررسی ارائه می‌شود.

۲ مروری بر تحقیقات پیشین

محققان در زمینه استفاده از هوش مصنوعی و سیستم‌های الگوریتمی خواننده-بازیاب، به‌ویژه با استفاده از مدل برت، تحقیقات قابل توجهی را در جواب دادن به سؤالات مرتبط با کوید ۱۹ انجام داده‌اند. در مطالعات متعدد، کاربردها و تکنیک‌های هوش مصنوعی (AI) و NLP در زمینه کوید ۱۹ مورد بررسی قرار گرفته‌اند. یکی از رویکردهای برجسته، استفاده از مدل برت است، یک مدل نمایش زبان قدرتمند که در وظایف مختلف NLP عملکرد قابل توجهی داشته است. محققان از مدل برت برای توسعه سیستم‌های الگوریتمی متناسب با پاسخ‌گویی به سؤالات مرتبط با کوید ۱۹ استفاده کرده‌اند. هدف این سیستم‌ها، ارائه اطلاعات دقیق و به موقع در مورد بیماری همه‌گیر، کمک به متخصصان مراقبت‌های بهداشتی، سیاست‌گذاران و عموم مردم در دستیابی به پاسخ‌های قابل اعتماد برای سؤالاتشان است. این سیستم‌ها می‌توانند سؤالات زبان طبیعی مرتبط با ویروس را به طور موثر درک و تفسیر کنند. در سیستم خواننده-بازیاب، جزء خواننده سیستم اطلاعات

مربوطه را از متون موجود استخراج می‌کند، در حالی که جزء بازیابی مرتبط‌ترین مقاله‌ها یا متن‌های حاوی پاسخ‌ها را بازیابی می‌کند. عملکرد این سیستم‌ها معمولاً بر اساس معیارهایی مانند دقت، صحت، یادآوری و امتیاز F1 ارزیابی می‌شود. محققان نتایج دلگرم‌کننده‌ای را گزارش کرده‌اند که برخی از سیستم‌ها به نرخ‌های دقت بالایی دست یافته‌اند و اغلب از عملکرد انسان در وظایف پاسخ‌گویی به سؤالات مرتبط با کوید ۱۹ پیشی می‌گیرند.

در سال‌های اخیر، با معرفی چندین مجموعه‌داده در مقیاس بزرگ مانند MedQA توسط لی و همکاران [۴]، SQuAD توسط راجپورکار و همکاران [۵]، MS MARCO توسط نگوین و همکاران [۶]، SearchQA توسط داون و همکاران [۷]، TriviaQA توسط جوشی و همکاران [۸]، QUASAR-T توسط دهینگرا و همکاران [۹] و PubMedBERT توسط گو و همکاران [۱۰]، شاهد پیشرفت سریع در یادگیری ماشین و به روشی مناسب‌تر در زمینه درک زبانی بوده‌ایم. ما همزمان شاهد معرفی چندین ترانسفورمر و مدل برای انجام وظایفی مانند طبقه‌بندی متن، پیش‌بینی جمله بعدی و پرسش و پاسخ هستیم [۱۱]. ادغام این دو عنصر اساسی مجموعه‌داده‌ها و ترانسفورمرها به ما اجازه می‌دهد تا شاهد یک تحول در این جهت باشیم. در این، به بررسی برخی از تحقیقات پیشین می‌پردازیم.

لی و همکاران [۴ و ۱۲] سیستم پاسخگویی به سؤالات پزشکی به نام MedQA را توسعه دادند، که از پنج مؤلفه شامل طبقه‌بندی سؤال، تولید سؤال، بازیابی اسناد، استخراج پاسخ و خلاصه‌سازی متن تشکیل شده است. آن‌ها همچنین COVIDASK را پیشنهاد دادند، سیستمی که تأخیر پرس و جو را با پیش‌نمایه‌سازی عبارات پاسخ کاهش می‌دهد. کاریکا و همکاران [۱۳] بر استفاده از هوش مصنوعی در زمینه پزشکی و حوزه کووید ۱۹ با استفاده از شبکه‌های عصبی NLP و ابزارهای بازرسی هوش مصنوعی مانند WellAI تمرکز کردند. دنیس دیفن باخ و همکاران [۱۴] یک سیستم پرسش و پاسخ بر مبنای دانش پیشنهاد دادند. یو ونهائو و همکاران [۱۵] TransTQA را توسعه دادند، یک سیستمی که پاسخ‌ها را بر اساس سؤالات مشابه قبلاً پاسخ داده شده بازیابی می‌کند. آباچا بن اسما و همکاران [۱۶] VQA-Med، یک معیار پاسخگویی به سؤالات پزشکی بصری را ارائه کردند. نوگیرا رودریگو و همکاران [۱۷] رتبه‌بندی مجدد متن مبتنی بر پرس و جو را مجدداً پیاده‌سازی کردند. گائو لو و همکاران [۱۸] تکنیک‌های تقطیر را برای جستجوی سریعتر با استفاده از برت بررسی کردند. استوا و همکاران [۱۹] یک موتور جستجوی معنایی رتبه‌بندی مجدد برای سؤالات پیچیده کووید ۱۹ پیاده‌سازی کردند. آباچا و همکاران [۲۰] یک سیستم پاسخگویی سؤال مبتنی بر پرس و جو را برای حوزه پزشکی ایجاد کردند. تانگ و همکاران [۲۱] مجموعه داده QA COVID را ایجاد کردند و یک معماری برای بازیابی اسناد و رتبه‌بندی مجدد پیشنهاد کردند. تیمو مولر و همکاران [۲۲] مجموعه داده پرسش و پاسخ کووید ۱۹ را بررسی کردند و مدلی به نام COVID-QA آموزش را دادند. سو و همکاران [۲۳] یک معماری پیشنهادی برای ماژول پاسخگویی به پرسش CAiRE-COVID ارائه کردند که شامل بازیابی اسناد، پیش پردازش پرس و جو و ماژول های رتبه بندی مجدد است.

بسیاری از این مدل‌ها برای حل مشکل پاسخ‌گویی به پرسش از مجموعه‌ای بزرگ پیشنهاد شده‌اند، و بسیاری دیگر، بر پاسخ‌گویی به سؤالات پزشکی متمرکز شده‌اند، اما قابلیت‌های تصویربرداری نهایی مدل‌ها در مورد یک مجموعه بزرگ ناکارآمد هستند. مدل پیشنهادی ما فاز به فاز قابلیت پاسخگویی را افزایش می‌دهد و

در نتیجه شانس نزدیک‌تر شدن پاسخ نهایی را افزایش می‌دهد و ویژگی‌های پیچیده پرسش و پاسخ را به تصویر می‌کشد. معماری پیشنهادی سعی می‌کند با کاستی‌هایی که در بخش‌های بعدی مورد بحث قرار می‌گیرند، مقابله کند.

۳ مفاهیم اولیه مورد نیاز

۱.۳ مدل‌های زبانی و از پیش آموزش دیده

مدل‌های زبانی در حوزه هوش مصنوعی، مدل‌های محاسباتی هستند که برای درک و تولید زبان انسانی طراحی شده‌اند. این مدل‌ها از مجموعه داده‌های بزرگ متنوع آموزش می‌بینند و می‌آموزند تا احتمالات کلمات را بر اساس اطلاعات زمینه‌ای پیش‌بینی کنند، که آن‌ها را قادر به تولید متن منسجم و مرتبط می‌سازد. مدل‌های زبانی از پیش‌آموزش‌دیده مانند برت، روبرتا، پابمدبرت، سایبرت و غیره، از مقادیر زیادی از داده‌های متنی برای یادگیری ویژگی‌های آماری و الگوهای زبانی استفاده می‌کنند [۲]. یکی از مدل‌های زبانی برجسته، برت است که وابستگی‌های متنی را به صورت دوطرفه ضبط می‌کند و با استفاده از روش‌های توجه و پیش‌بینی، در وظایف مختلف NLP به عملکرد قوی دست یافته است [۲]. همچنین مدل‌های دیگری همچون روبرتا (RoBERTa) و آلبرت (ALBERT) نیز از این دسته به شمار می‌روند. از مدل‌های زبانی بزرگ برای استفاده‌های خاص نیز بهره‌مند شده است؛ به‌عنوان مثال، مدل‌های زبانی در حوزه پزشکی از پیش‌آموزش‌دیده‌اند و برروی داده‌های پزشکی تدریس شده‌اند. PubMedBERT یکی از این مدل‌هاست که برای پردازش متون علمی و پزشکی به کار می‌رود، با آموزش بر روی مقالات PubMed که درک دقیق اصطلاحات و مفاهیم تخصصی در زمینه پزشکی را تسهیل می‌کند [۲۴ و ۲۵]. همچنین به مدل‌های BioBERT و SciBERT نیز اشاره می‌شود که در زمینه‌های مختلف NLP به تحقیقات و برنامه‌های کاربردی مؤثری انجام داده‌اند.

۲.۳ سیستم پاسخگویی به سؤالات (QA)

هدف از سیستم‌های پاسخگویی به پرسش، پردازش خودکار و درک سؤالات زبان انسان و ارائه پاسخ‌های دقیق و مرتبط است. این سیستم‌ها شکاف بین درک زبان انسانی و بازیابی اطلاعات را پر می‌کنند و ماشین‌ها را قادر می‌سازند به طور مؤثر به سؤالات کاربر پاسخ دهند. ساختن یک سیستم QA شامل مراحل کلیدی مانند درک سؤال، بازیابی اطلاعات، استخراج اطلاعات و تولید پاسخ است. سیستم‌های QA را می‌توان به سیستم‌های مبتنی بر قانون و سیستم‌های مبتنی بر یادگیری ماشینی دسته‌بندی کرد، که با مدل‌های یادگیری عمیق منجر به نتایج قابل‌توجهی شده‌اند [۲۶]. علاوه بر این، سیستم‌های مبتنی بر یادگیری ماشین به دو دسته عمده تقسیم می‌شوند: مدل‌های مولد (Generative models) و مدل‌های بازنمایی (Retrieval-based models). این تقسیم‌بندی بر اساس روش و رویکردی است که این مدل‌ها برای پاسخ‌دهی به سؤالات استفاده می‌کنند [۲].

مدل‌های مولد از روش‌های تولید متن برای ایجاد پاسخ‌های جدید و خلاقانه بر اساس دانش موجود و متن

ورودی استفاده می‌کنند. این مدل‌ها از تکنیک‌های آماری و احتمالاتی برای تولید جملاتی استفاده می‌کنند که مجموعه‌ای از قوانین، الگوها و ساختارهای زبانی را در بر می‌گیرد. مدل های مولد از مزیت تولید پاسخ های متنوع و خلاقانه، افزایش تعامل و ارتباط با کاربران برخوردار هستند. آن‌ها همچنین می‌توانند ابهام و عدم قطعیت در سؤالات را مدیریت کنند و پاسخ های ظریف‌تری ارائه دهند [۲۷]. در عین حال، مدل‌های بازنمایی از داده‌ها و منابع نمایش داده شده برای پاسخ به سؤالات با استفاده از متون ورودی و سؤالات به عنوان پرس و جو استفاده می‌کنند. سپس، آن‌ها از روش‌های بازیابی برای جستجوی پاسخ‌های مناسب از متون بهینه ارائه شده استفاده می‌کنند. پاسخ ها معمولاً از مجموعه پاسخ های قبلی در داده های آموزشی یا منابع دیگری که ممکن است شامل دانش عمومی یا تخصصی باشد، بازیابی می شوند. مدل‌های بازنمایی در استفاده از منابع دانش خارجی برتری دارند و می‌توانند پاسخ‌های منطقی و دقیقی بر اساس شباهت و توافق با متن سؤال ارائه دهند. آن‌ها دقت و عملکرد را با استفاده از پاسخ های قبلی و دانش مربوط به دامنه افزایش می¬دهند. مدل‌های بازیابی مبتنی بر زمینه، با استفاده از تکنیک‌هایی مانند بازیابی اطلاعات و بازیابی مبتنی بر رتبه‌بندی، معمولاً در وظایف QA استفاده می‌شوند [۲۶].

۴ نگاشت پیشنهادی

برای دستیابی به هدف، ما از رویکرد چند مرحله‌ای برای تجهیز مدل پاسخگویی به پرسش برت به دانش پزشکی و تخصصی در زمینه‌های علمی استفاده کردیم. در ابتدا، مدل زبان BERT را بر روی مجموعه‌ای از مقالات علمی به دقت تنظیم کردیم، با استفاده از مدل پابمدبرت به آن اجازه دادیم تا متون علمی را بهتر درک کند. سپس، با تمرکز بر مجموعه داده‌ای که به طور خاص به مقالات تحقیقاتی مرتبط با کووید ۱۹ مربوط می‌شود، این مدل را تنظیم دقیق کردیم تا تخصص آن در این حوزه افزایش یابد. در مرحله بعدی، مدل را بر مجموعه داده SQuAD آموزش دادیم تا توانایی پاسخگویی به سؤالات را توسعه دهد و بر اساس متن و سؤالات داده شده، پاسخ‌های دقیق ایجاد کند. در نهایت، با استفاده از مجموعه داده پرسش و پاسخ کووید ۱۹، این مدل را تنظیم کردیم تا پاسخ‌های آموزنده و تخصصی به سؤالات مرتبط با کووید ۱۹ ارائه دهد. به طور کلی، این روش مدل را به دانش تخصصی مجهز کرده و توانایی آن را برای ارائه پاسخ‌های حرفه‌ای در زمینه‌های ادبیات علمی و کووید ۱۹ افزایش داده است.

۱.۴ شرح روش پیشنهادی

در این تحقیق، از دو روش برای دستیابی به اهداف خود استفاده کردیم. روش اول، با سادگی بیشتر و سرعت بیشتری همراه بود، اما نتایج کمتر از حد مطلوب داشت. روش دوم پیچیده‌تر بود، اما به نتایج بهتری منجر شد. در ادامه، هر یک از این روش‌ها را جداگانه مورد بحث و ارزیابی قرار می‌دهیم و نقاط قوت و ضعف هرکدام را برجسته می‌کنیم. پیش از این، یک مرور کلی بر روی کارهای انجام شده داده شده و هدف از این توضیحات، افزایش درک از پیچیدگی‌های هر روش و آینده ارزیابی آن‌هاست. در مرحله اولیه، مدل‌های مختلف زبان بزرگ ارزیابی شدند و BERT به عنوان مدل پایه برای اهداف تحقیقاتی این پژوهش انتخاب

شد. در مرحله بعدی، با هدف افزایش تخصص BERT در صحبت کردن به صورت حرفه‌ای و به عنوان یک متخصص در زمینه علمی، BERT را با تنظیم دقیق بر روی مجموعه‌ای از مقالات علمی با طیف وسیعی از رشته‌های علمی، بهینه کردیم. این فرآیند امکان ایجاد پاسخ‌های بهتر در متون علمی را توسط BERT با بهره‌گیری از دانش قبلی و همسویی با مجموعه داده‌های علمی فراهم کرد.

در مرحله بعد، تمرکز خود را بر روی انتخاب یک مدل زبانی مناسب برای کار با اطلاعات پزشکی و انجام تحقیقات علمی گذاشتیم. چندین مدل از جمله بایوبرت، سای‌برت، و پابمدبرت در این حوزه ارزیابی شدند و پس از یک ارزیابی جامع، پابمدبرت نسبت به دیگر مدل‌های مورد بررسی، عملکرد برتری از خود نشان داد. سپس، توجه خود را به ارتقاء مهارت مدل در زمینه کووید ۱۹ معطوف کردیم. برای این منظور، مدل را بر روی یک مجموعه داده تخصصی متشکل از تقریباً ۲۰۰۰ مقاله تحقیقاتی کووید ۱۹ که از Elsevier به دست آمده بود، به دقت تنظیم کردیم. این عمل باعث شد که مدل درک عمیق‌تری از زبان، اصطلاحات و یافته‌های علمی خاص این حوزه را پیدا کند. به منظور اینکه مدل بتواند پاسخ‌های دقیقی به سؤالات ارائه دهد، آن را با استفاده از مجموعه داده SQuAD آموزش دادیم. از هر دو نسخه ۱ و ۲ مجموعه داده SQuAD استفاده کردیم تا مدل را در مقابل سناریوهای مختلف پرسش و پاسخ قرار دهیم. در طول این فرآیند آموزشی، مدل یاد گرفت که ساختارهای سؤال را درک کند، اطلاعات مربوطه را از متن استخراج کند، و بر اساس ورودی ارائه شده، پاسخ‌های دقیق ایجاد کند.

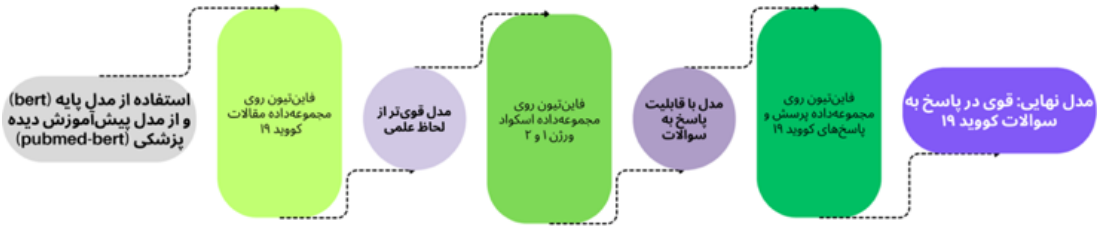
در مرحله نهایی، توانایی مدل را برای پاسخ دادن به سؤالات مرتبط با کووید ۱۹ تنظیم کردیم. این تنظیمات از مجموعه داده پرسش و پاسخ کووید ۱۹ بهره بردند، که شامل ۲۰۱۹ سؤال درباره علائم، انتقال، اقدامات پیشگیری، گزینه‌های درمانی و سایر جنبه‌های مرتبط با کووید ۱۹ است. این مجموعه داده گسترده ترین موضوعات مرتبط با کووید ۱۹ را پوشش می‌دهد. با تنظیم دقیق روی این مجموعه داده، مدل درک خود از دانش و اصطلاحات خاص کووید ۱۹ را افزایش داد و این امکان را فراهم کرد که پاسخ‌های دقیق و حرفه‌ای به سؤالات مرتبط با کووید ۱۹ ارائه دهد.

در ادامه، به بررسی جزئیات روش‌های پیاده‌سازی می‌پردازیم.

۱.۱.۴ روش اول

در روش تحقیق اولیه، به طور اختصاصی روی مجموعه داده پرسش و پاسخ کووید ۱۹، با استفاده از مدل‌های مختلف زبانی تنظیم دقیق صورت گرفت و متعاقباً عملکرد آن‌ها مقایسه گردید. مدل‌های برجسته زبانی، شامل Bert، Albert، Roberta، Biobert، Sybert و PubMedbert، برای انتخاب به ارزیابی گذاشته شدند. فرآیند دقیق تنظیم روی هر مدل انجام شد و عملکرد آن‌ها بر اساس معیارهای مختلف ارزیابی گردید. هدف از این روش، بررسی اثربخشی مدل‌های مختلف زبانی و شناسایی مناسب‌ترین مدل برای پاسخ‌گویی به سؤالات مرتبط با کووید ۱۹ بود.

شکل ۱: مروری بر مراحل روش اول



شکل ۲: مروری بر مراحل روش دوم

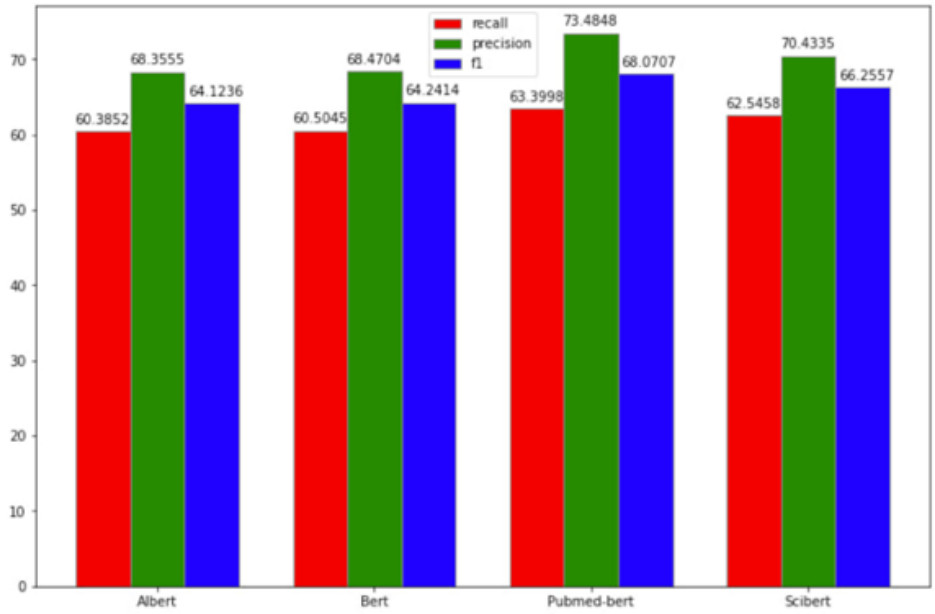
۲.۱.۴ روش دوم

در رویکرد دوم، مدل‌های Bert و PubMedbert به‌عنوان بهترین مدل‌ها از روش اول انتخاب شدند. سپس، با بهره‌گیری از مجموعه داده‌های SQuAD نسخه ۱ و ۲، فرآیند تنظیم دقیق این مدل‌ها ادامه یافت. هدف اصلی این فرآیند، افزایش عملکرد مدل‌ها، به ویژه در وظیفه پاسخ‌گویی به سؤالات بود. این بهینه‌سازی در محیط مجموعه داده SQuAD به مدل‌ها آموزش داد که اطلاعات مربوطه را از متن استخراج کرده و پاسخ‌های دقیقی به سؤالات ارائه دهند. همچنین، اضافه کردن مجموعه داده پرسش و پاسخ کووید ۱۹، بهینه‌سازی اضافی را تسهیل می‌کند و به خصوص بر روی دامنه کووید ۱۹ تمرکز دارد.

بطور کلی، این دو روش باعث شناسایی بهینه‌ترین مدل‌های زبانی شده و عملکرد آن‌ها در پاسخ به سؤالات مرتبط با کووید ۱۹ را افزایش دادند. روش تحقیق شامل دو عنصر اصلی بود: تنظیم دقیق یک مدل زبان آموزش‌دیده برای ارتقاء قابلیت‌های درک زبان و تنظیم دقیق مدل پاسخ‌گویی به سؤال برای بهبود توانایی تولید پاسخ‌های دقیق. این دو جنبه نقش مهمی در پیشبرد مدل‌های موثر و کارآمد برای وظیفه پاسخ‌گویی ایفا کردند.

۵ نتایج

یک ارزیابی جامع از دو روش انجام شد و معیارهای ارزیابی مختلف، از جمله دقت، یادآوری، امتیاز F1 و تطبیق دقیق مورد بررسی قرار گرفت تا اثربخشی مدل‌های زبانی ارزیابی شود و نتایج به‌دست‌آمده از هر روش مقایسه شود. جنبه های کیفی، مانند سازگاری و ارتباط پاسخ‌های مدل نیز برای اطمینان از ارتباطات حرفه‌ای و تخصصی در زمینه‌های مربوطه در نظر گرفته شد.

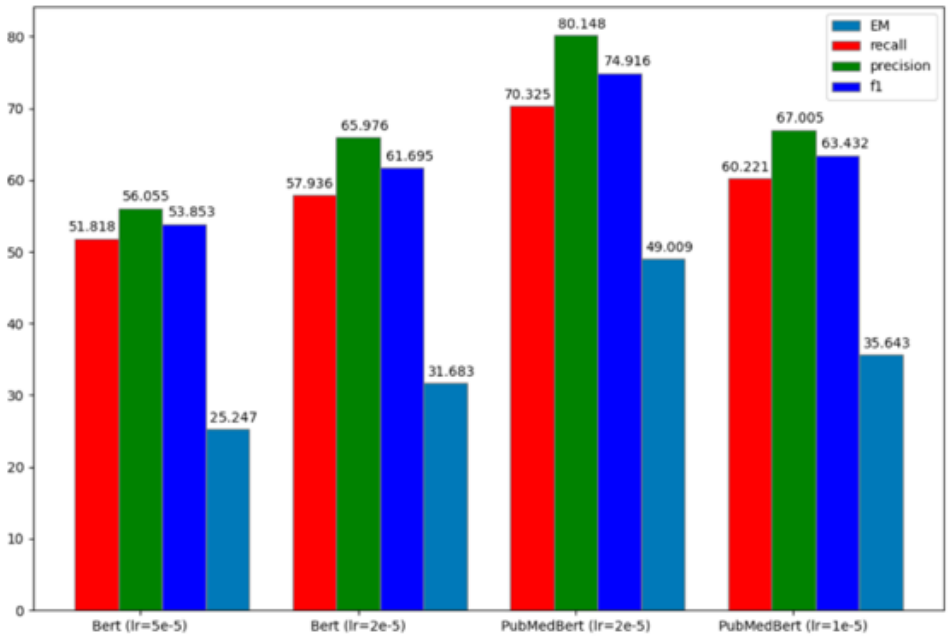


شکل ۳: بررسی عملکرد مدل‌های زبانی در روش اول

ارزیابی روش اول شامل بررسی، آزمایش و آموزش چندین مدل زبان از جمله Bert، Albert، Roberta، Biobert، Scibert و PubMedbert بود. پس از تنظیم دقیق مدل‌ها در مجموعه داده‌های پرسش پاسخ کووید ۱۹، عملکرد هر مدل مورد ارزیابی قرار گرفت. نتایج نشان داد که برت و آلبرت عملکرد مشابهی از خود نشان دادند، در حالی که سایبرت و پاب مدبرت نتایج بهتری را نشان دادند. به طور خاص، مدل PubMedbert از سایر مدل‌ها بهتر عمل کرد و به دقت ۷۳ درصد در پاسخ به سؤالات مرتبط با کووید ۱۹ دست یافت. نتایج ارزیابی اهمیت استفاده از داده‌های آموزشی مرتبط و واقعی را برای بهبود عملکرد نشان داد.

در روش دوم، مدل BERT و PubMedbert برای ارزیابی بیشتر انتخاب شدند. مدل‌ها به طور جداگانه با پارامترهای مختلف، مانند نرخ یادگیری و دوره‌های آموزشی متفاوت، برای بهینه سازی عملکرد خود آموزش داده شدند. نتایج نشان داد که هر دو مدل بسته به مجموعه داده‌ها و شرایط آموزش عملکرد متفاوتی داشتند. مدل BERT بسته به مجموعه داده‌ها نتایج متفاوتی را نشان داد، در حالی که مدل PubMedbert به طور مداوم عملکرد بهتری را نشان داد. به طور خاص، مدل PubMedbert که از قبل بر روی داده های پزشکی و علمی آموزش داده شده بود، به ترتیب به دقت ٪۶۷ و ٪۸۰ و امتیاز F1 ٪۶۳ و ٪۷۵ دست یافت. این نتایج برتری مدل PubMedbert را در پاسخ به سؤالات مرتبط با کووید ۱۹ نشان داد.

با مقایسه روش اول با روش دوم، مشاهده شد که فرآیند تنظیم دقیق در مقالات کووید ۱۹ و مجموعه داده‌های سؤالات، منجر به عملکرد ضعیف‌تر برای مدل BERT در مقایسه با روش اول شد. این نشان دهنده محدودیت‌های مدل BERT در مدیریت اطلاعات خاص و همچنین کوچک بودن مجموعه مقالات کووید ۱۹



شکل ۴: بررسی عملکرد مدل‌های زبانی در روش دوم

استفاده شده است. در مقابل، مدل PubMedbert که از قبل بر روی داده‌های پزشکی و علمی آموزش داده شده بود، عملکرد بهتری را نسبت به روش اول نشان داد. پیش آموزش بر روی داده‌های علمی و پزشکی مرتبط، درک و توانایی مدل را برای پاسخگویی دقیق به سؤالات افزایش داد. مدل PubMedbert با دقت ۸۰ درصد و امتیاز F1 ۷۵ درصد در وظایف پاسخگویی به سؤالات کووید ۱۹ بهترین عملکرد را در بین مدل‌های ارزیابی شده به دست آورد.

به طور کلی، نتایج نشان داد که مدل PubMedbert با دانش و آموزش قبلی خود در مورد مجموعه داده‌های مربوطه، بهترین عملکرد را در پاسخ به سؤالات مرتبط با کووید ۱۹ ارائه می‌کند. یافته‌ها اهمیت مدل‌های پیش‌آموزشی بر روی داده‌های حوزه خاص و اهمیت انتخاب مدل‌های زبانی مناسب برای کارهای تخصصی را برجسته کرد.

۶ نتیجه‌گیری

در این تحقیق، با استفاده از مدل‌های زبانی پیش‌آموزش دیده، سیستمی طراحی شد که قادر است به سؤالات با دقت و صحت بالا پاسخ دهد و از منابع دقیق و تحقیقاتی استفاده کند. نتایج نشان داد که مدل‌های زبانی که از قبل روی منابع علمی و پزشکی آموزش دیده بودند، در پاسخ‌دهی به سؤالات عملکرد بهتری داشتند. امیدواریم که انسان‌ها به زودی امکان بهره‌مندی از اطلاعات صحیح و دسترسی آسان به آن‌ها در یک محیط امن را تجربه کنند.

مراجع

[1] World Health Organization. (2020). Coronavirus disease (COVID-19) pandemic. Retrieved from https://www.who.int/emergencies/diseases/novel-coronavirus-2019.

[2] Centers for Disease Control and Prevention. (2021). COVID-19 overview and information. Retrieved from https://www.cdc.gov/coronavirus/2019-ncov/long-term-effects/index.html.

[3] Devlin, J., Chang, M. W., Lee, K., Toutanova, K. (2019). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In Proceedings of the 2019, Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL-HLT) Vol. 1, pp. 4171-4186.WHO Coronavirus (COVID-19) Dashboard, (2023). https://covid19.who.int/

[4] Lee M., Cimino J., Zhu J., Sable C., Shanker V., Ely J., Yu H., (2006), Beyond information retrieval-medical question answering, in: AMIA Annual Symposium Proceedings, 2006; pp. 469–473.

[5] Rajpurkar, P., Zhang, J., Lopyrev, K., Liang, P. (2016). SQuAD: 100,000+ Questions for Machine Comprehension of Text. In Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing (EMNLP) (pp. 2383-2392).

[6] Nguyen, T., Rosenberg, M., Song, X., Gao, J., Tiwary, S., Majumder, R., Deng, L., (2016), MS MARCO: A Human Generated MAchine Reading COmprehension Dataset, Under review as a conference paper at ICLR.

[7] Dunn, M., Sagun, L., Higgins, M., Guney, VU., Cirik, V., Cho, K., (2017), Searchqa: A new Q&A dataset augmented with context from a search engine , arXiv preprint arXiv:1704.05179 .

[8] Joshi M., Choi E., Weld D.S. Zettlemoyer L., (2017), TriviaQA: A Large Scale Distantly Supervised Challenge Dataset for Reading Comprehension. Allen Institute for Artificial Intelligence, arXiv:1705.03551v2 [cs.CL] 13 May 2017.

[9] Dhingr, B., Mazaitis, K., Cohen WW., (2017), Quasar: Datasets for question answering by search and reading - arXiv preprint arXiv:1707.03904, - arxiv.org.

[10] Gu, Y., Tinn R., Cheng H., Lucas M., Usuyama N., Liu X., Naumann T., Gao J. and Poon H., (2021), Domain-specific language model pretraining for biomedical natural language processing, ACM Transactions on Computing for Healthcare (HEALTH) 3 (1), pp. 1-23.

[11] Jalammar g., (2018), Visualizing A Neural Machine Translation Model (Mechanics of Seq2seq Models With Attention). http://jalammar.github.io/visualizing-neural-machine-translation-mechanics-of-seq2seq-models-with-attention/

[12] Lee, J., Yi, SS., Jeong, M., Sung, M., Yoon, W., Choi, Y, Ko, M., Kang, J., (2020). Answering questions on COVID-19 in real-time, arXiv preprint arXiv:2006.15830.

[13] Kricka, L. J., Polevikov, S., Park, J. Y., Fortina, P., Bernardini, S., Satchkov, D., Kolesov, V., Grishkov M., (2020), Artificial Intelligence-powered search tools and resources in the fight against COVID-19, eJIFCC2020 Vol.31, No2, pp106-116.

[14] Diefenbach, D., Both, A., Singh, K., Maret, P., (2020). Towards a question answering system over the semantic web. Semantic web, vol. 11, no. 3, pp. 421-439. DOI: 10.3233/SW-190343.

[15] Yu, W., Wu, L., Deng, Y., Mahindru, R., Zeng, Q., Guven, S., Jiang, M. (2020): A Technical Question Answering System with Transfer Learning. In: Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: System Demonstrations, pp. 92-99.

[16] Abacha, A.B., Hasan, S.A., Datla, V.V., Liu, J., Demner-Fushman, D. Müller, H., (2019). VQA-Med: overview of the medical visual question answering task at ImageCLEF 2019. In: CLEF (Working Notes).

[17] Nogueira, R., Cho, K., (2020), Passage Re-ranking with BERT, arXiv:1901.04085v5 [cs.IR].

[18] Gao, L., Dai, Z., Callan, J., (2020). Understanding BERT Rankers Under Distillation. In: Proceedings of the 2020 ACM SIGIR on Inter- national Conference on Theory of Information Retrieval, pp. 149-152. https://doi.org/10.1145/3409256.3409838.

[19] Esteva, A., Kale, A., Paulus, R., Hashimoto, K., Yin, W., Radev, D., Socher, R., (2020). Co-search: Covid-19 information retrieval with semantic search, question answering, and abstractive summariza- tion. arXiv preprint arXiv:2006.09595.

[20] Abacha, A.B., Demner-Fushman, D., (2019) A question-entailment approach to question answering. BMC Bioinform. 20(1), 511 (2019) [PMC free article] [PubMed].

[21] Tang R., Nogueira, R., Zhang, E., Gupta, N., Cam, P., Cho, K., Lin, J., (2004). Rapidly bootstrapping a question answering dataset for COVID-19, arXiv preprint arXiv:2004.11339.

[22] Moller, T., Reina,A., Jayakumar,R., Pietsch, M., (2020), COVID-QA: A Question Answering Dataset for COVID-19, Proceedings of the 1st Workshop on NLP for COVID-19 at ACL 2020. https://aclanthology.org/2020.nlpcovid19-acl.

[23] Su, D., Xu, Y., Yu, T., Siddique, FB., Barezi, EJ., Fung, P., (2020). CAiRE-COVID: a question answering and multi-document summarization system for COVID-19 research, arXiv:2005.03975 https://arxiv.org/abs/2005.03975v1.

[24] Yang Z., Liu G., (2019), Hierarchical Sequence-to-Sequence Model for Multi-Label Text Classification, IEEE Access, VOLUME 7.

[25] Jurafsky, D., Martin, J. H. (2019). Speech and language processing: An introduction to natural language processing, computational linguistics, and speech recognition (3 ed.). Pearson Prentice Hall.

[26] Hastie, T., Tibshirani, R., Friedman, JH., Friedman, JH., (2009) Springer , [BOOK] The elements of statistical learning: data mining, inference, and prediction.

[27] Kumar, A., Reddy, V. P., Joshi, S. (2021). Question Answering Systems: Approaches and Challenges. In Proceedings of International Conference on Computational Intelligence and Data Science (pp. 152-158). Springer.

ارزیابی چالش‌های امنیت سایبری در محیط‌های واقعیت مجازی VR

علی ملک‌لی [۱]

[۱] کارشناس ارشد مدیریت فناوری اطلاعات، دانشگاه تهران، مدرس دانشگاه
malekli.ali@gmail.com

چکیده

اگرچه واقعیت مجازی (VR) فناوری جدیدی نیست، اما به تازگی در حوزه های مختلفی به جز سرگرمی مورد استفاده قرار گرفته و این موضوع باعث شده است که جامعه پژوهشیِ امنیت اطلاعات، به تهدیدات جدید سایبری که با آن همراه است توجه کند. تنوع اجزای سیستم، سَطح گستره ای از حملات سایبری را ممکن می سازد که می‌تواند مورد سوء استفاده و بهره برداری غیر مجاز توسط هکرها یا دشمنان شود. در عین حال، تأکید VR بر روی غرق شدن (immersion)، تعامل (interaction) و حضور (presence) به معنای آن است که می‌توان به صورت مستقیم کاربر را مورد هدف حمله سایبری قرار داد، ولی استفاده از دستگاه‌های نصب شده بر روی سر ممکن است، حس و مشاهده و درک این حمله را برای کاربر سخت کند. این مقاله با طبقه‌بندی سیستماتیک تهدیدات سایبری VR موجود در مقابل روشهای دفاعی سایبری مرسوم، به پژوهشگران با زمینه‌های مختلف برای شناسایی بهتر و درک هرچه بیشتر این مخاطرات کمک خواهد کرد.

کلمات کلیدی: واقعیت مجازی، حملات سایبری، امنیت سایبری، حریم خصوصی.

۱ مقدمه

واقعیت مجازی (VR) در حال تبدیل به یک فناوری پرطرفدار می‌شود و انتظار می‌رود تا سال ۲۰۲۵ به ارزش بازار ۲۰/۹ میلیارد دلار برسد. با این‌حال، تحقیقات در مورد خطرات امنیتی VR محدود است. این موضوع می‌تواند یک مشکل باشد؛ زیرا دستگاه‌های VR دید کاربر را کاملاً پوشش می‌دهند و این باعث می‌شود که برای وی سخت باشد تا حملات امنیتی و دستکاری‌های مخرب را مشاهده کند. ما در این مقاله، با طبقه‌بندی سیستماتیکِ چالش‌های امنیتی برای محیط‌های واقعیت مجازی (VREs)، به پژوهشگران کمک می‌کنیم تا با درک بهتر تأثیر تهدیدهای سایبری در این حوزه، بتوانند روش‌های دفاع سایبری جدید را توسعه دهند.

۲ مطالعات پیشین و موضوعات این مطالعه

واقعیت مجازی (VR) یک فناوری است که تجربه‌ای شبیه‌سازی شده را برای کاربر ایجاد می‌کند. این فناوری بیش از ۵۰ سال پیش توسط ساترلند (Sutherland, 1965) پیشنهاد شد. از آن زمان به بعد، تعاریف مختلفی توسط محققان مختلف ارائه شده است. VR یک تجربه فراگیر، چند حسی است که با عینک‌های سه بعدی، حسگرهای ردیابی حرکات بدن در زمینه‌های مختلفی مانند سرگرمی، آموزش و کسب‌وکار استفاده می‌شود. با این حال، تحقیقات در زمینه خطرات امنیت سایبری VR و طبقه‌بندی سیستماتیک از تهدیدهای مختلف یا مکانیزم‌های دفاعی این حوزه بسیار محدود است. هدف این مقاله، برطرف کردن این کمبود دانش با ارائه یک طبقه‌بندی از تهدیدهای سایبری، در ارتباط با ویژگی‌هایی که در محیط‌های مختلف VR به طور مشترک به اشتراک گذاشته می‌شوند، است. این طبقه‌بندی به محققان کمک می‌کند تا تأثیر تهدیدهای سایبری را درک کنند و راه‌حل‌های دفاعی جدیدی را توسعه دهند. این مقاله دو موضوع اصلی دارد:

- طبقه‌بندی سیستماتیک برای سازماندهی چالش‌های امنیتی VR مختلف. این طبقه‌بندی به تصویر کلی یکپارچه از انواع مختلف تهدیدهای سایبری در VR کمک می‌کند.
- بررسی کلی روش‌های دفاعی سایبری موجود و قابلیت اعمال آنها برای تهدیدهای سایبری VR.

۳ طبقه بندی مخاطرات و چالش‌های امنیتی VR

یک سیستم VR می‌تواند به عنوان یک مجموعه سخت‌افزار و نرم‌افزار دیده شود که با حرکت فیزیکی کاربر انسانی تعامل دارد و در عوض تحت تأثیر دریافت حسی انسانی از کاربر قرار می‌گیرد. هر یک از این مؤلفه‌های فنی و انسانی ممکن است به عنوان نقاط نفوذ و جذاب برای حملات سایبری مورد استفاده قرار گیرند. در این راستا ما به چهار سوال بزرگ پاسخ می‌دهیم:

- چه جنبه‌ای از سیستم ممکن است مورد نفوذ و بهره برداری غیرمجاز قرار گیرد؟ این مورد سطح حمله را نشان می‌دهد.
- چه ویژگی امنیتی ممکن است نقض شود؟ این مورد به سه‌گانه محرمانگی–صحت–دسترسی (CIA) از ویژگی‌های امنیتی ارجاع دارد.
- تأثیر چه برداشتی از تجربه VR ممکن است ناشی از نقض امنیتی باشد؟ در اینجا، ما تجربه VR را با تعامل (interaction)، غرق شدن (immersion) و حضور (presence) نشان می‌دهیم.
- حمله، ممکن است به چه آسیبی منجر شود؟ قصد حمله می‌تواند برای آسیب فیزیکی یا غیرفیزیکی باشد.

بر اساس سؤالات فوق، ما چهار دسته‌بندی بزرگ را ارائه می‌دهیم: **بهره‌برداری (exploit)، نقض (breach)، تأثیر (impact) و قصد و نیت (intent).**

۱.۳ بهره‌برداری (exploit)

بهره‌برداری یعنی فرآیند نفوذ به آسیب‌پذیری‌های یک سیستم کامپیوتری، از طریق یک برنامه نرم‌افزاری یا کد مخرب که باعث رفتار ناخواسته و احتمالاً صدمات سایبری، فیزیکی می‌شود. در ارتباط با یک سیستم واقعیت مجازی (VRS)، ما یک نفوذ را به دو موضوع مختلف **سیستمی و انسانی**، گروه‌بندی می‌کنیم.

۱.۱.۳ سیستمی

شبکه: در یک نشست و تعامل واقعیت مجازی، انواع مختلفی از داده‌ها بین منبع و مقصد تبادل می‌شوند که می‌توانند توسط حملات سایبری مانند انکار سرویس (DoS) مختل شود. حملات به شبکه می‌تواند منجر به کاهش سرعت، قطع شدن ارتباط و ... شود.

تاخیر: به تاخیر در انتقال داده‌ها اشاره دارد که کیفیت سرویس (QoS) را در یک محیط شبکه‌ای کاهش می‌دهد و می‌تواند کیفیت بصری و صوتی در جلسه واقعیت مجازی را تحت تأثیر قرار دهد.

پهنای باند: پهنای باند خوب و بالا برای عملکرد بی‌دردسر شبکه و کیفیت تجربه توسط کاربر حیاتی است. حملاتی که شبکه را مختل می‌کنند، می‌توانند به عدم راحتی بصری و عدم دسترسی به محیط واقعیت مجازی منجر شوند.

نمایش: به تصاویری که عینک‌های VR به چشمان کاربر ارائه می‌دهند، اشاره دارد. معماری نمایشگر واقعیت مجازی می‌تواند روش‌های مختلفی را برای حمله ارائه دهد که می‌تواند صدمات سایبری- فیزیکی ایجاد کند. به عنوان مثال، یک حمله‌کننده می‌تواند با پوشاندن یا ارائه محتوای ناخوشایند یا مخرب خود، جلسه واقعیت مجازی را به دست بگیرد.

سنسورها: سنسورها به سیستم‌های IMU و دوربین که در پیگیری داده‌های موقعیتی و جهت‌گیری کاربر استفاده می‌شوند، اشاره دارند. اگر این داده‌ها به نحوی به دست مهاجم بیفتد، می‌تواند به حریم شخصی کاربر آسیب بزند. مهاجم ممکن است سعی کند داده‌های موقعیتی و جهت‌گیری کاربر را جمع‌آوری کرده، تا به شکلی از آن استفاده کند که می‌تواند منجر به تخریب سایبری یا جاسوسی در محیط فیزیکی کاربر شود.

۲.۱.۳ انسانی

این موضوع به خروجی موارد حسی اشاره دارد که فناوری VR برای ایجاد حس غرق شدن در جهان مجازی استفاده می‌کند. دستگاههای VR از حس بصری و شنیداری استفاده می‌کنند، اما برخی از آنها نیز از لمس با استفاده از کنترلرها استفاده می‌کنند. هدف فناوری VR این است که مغز انسان به گمان اینکه با اشیاء در جهان مجازی در حال تعامل است، بازسازی شود. هر چه بیشتر از این حس‌ها در فضاهای VR وجود داشته باشد، کاربر ممکن است به حملات سایبری، آسیب پذیرتر باشد.

حس بصری: دستگاه‌های VR جهان مصنوعی از پیش تعریف شده‌ای را به منظور تحریک حس بصری کاربران ایجاد می‌کنند. حس بینایی، حس برجسته‌ای در انسان‌هاست و کاربران به شیوه‌های مختلف که از طریق نمایشگر VR به آنها ارائه می‌شود، پاسخ می‌دهند. با این حال، حس بینایی کاربران به حملاتی مانند آزار و اذیت کردن و مهندسی اجتماعی آسیب پذیر است.

حس شنیداری: دستگاه‌های VR از بلندگوها برای تقلید از حس شنوایی کاربران از طریق صدای فضایی استفاده می‌کنند. یک نفوذگر یا هکر می‌تواند بر روی حملاتی که از طریق نشانه‌های صوتی مانند آزار و اذیت کردن استفاده می‌کند، تمرکز کند.

حس لمسی: سیستمهای VR از کنترلرهایی استفاده می‌کنند که بازخورد لمسی را فراهم می‌کند. یک حمله احتمالی که می‌تواند از کنترلرهای لمسی بهره ببرد این است که یک کنترلر مجازی که نامرئی است، به یک حمله‌کننده اجازه دهد تا کنترل کامپیوتر کاربر را به دست بگیرد.

حس بویایی: فناوری VR هنوز حس بو را به مقیاس گسترده‌ای به کار نبرده است. با این حال، تولید بویی که مخرب باشد، مانند فراخواندن یک خاطره منفی در یک فرد با اختلال استرس یا نگرانی از تهدید فیزیکی مانند دود در خانه، می‌تواند تأثیرات آسیب زا داشته باشد.

۲.۳ نقض و نفوذ

نقض و نفوذ امنیتی به معنای دسترسی غیرمجاز به سیستم کامپیوتری، دستگاه، شبکه یا برنامه با هدف ایجاد آسیب فیزیکی یا غیرفیزیکی با عبور از مکانیزم‌های امنیتی است. طبقه‌بندی ما بر اساس سه خصوصیت مهم **محرمانگی، صحت و دسترسی (CIA)** است.

۱.۲.۳ محرمانگی

محرمانگی در VR به محافظت از داده‌های حساس در برابر دسترسی غیرمجاز اشاره دارد. هدست‌های VR داده‌های رفتاری بیومتریک و حرکت کاربر را جمع آوری می‌کنند و کاربران می‌توانند اطلاعات شخصی مانند رمز عبور و اطلاعات ورود به سیستم را وارد کنند. Casey و همکاران (۲۰۱۹) نشان دادند که با پیاده سازی مجموعه‌ای از حملات سایبری بر روی OpenVR، که به عنوان یک رابط مدیریت برنامه جهانی بین سخت افزار VR و برنامه‌ها در SteamVR عمل می‌کند، نفوذی در محرمانگی رخ می‌دهد. برای نمونه: حمله دسترسی به دوربین با دسترسی به فایل‌های پیکربندی JSON رمزگذاری نشده SteamVR می‌تواند به حمله‌کننده اجازه دهد که دوربین را بدون هشدار کاربر فعال کند.

۲.۲.۳ صحت

صحت به تغییرات یا اصلاحات غیرمجاز داده‌ها اشاره دارد. داده‌های VR می‌توانند برای ایجاد آسیب سایبری یا دستکاری در سیستم تغییر یابند. به عنوان مثال: حمله ایجاد گیجی برای کاربر توسط Casey و همکاران

(۲۰۱۹)، شامل تغییر اسکریپت JSON برای فایل پیکربندی chaperone می‌شد که به کاربر حس گیجی و عدم تعادل را القا می‌کرد.

۳.۲.۳ دسترسی

دسترسی به معنای دسترسی ساده و مجاز کاربران به داده‌ها و سیستم‌های مورد نیازشان است. یکی از ویژگیهای اصلی یک سیستم VR، توانایی فراهم کردن غرق شدن و حضور به کاربرانش است. برای رسیدن به این هدف، باید ارتباط بی‌وقفه بین اجزای مختلف سیستم VR وجود داشته باشد، به طوری که هرگونه وقفه باعث شکست غرق شدن و حضور شود. یک مثال از حمله انکار سرویس (DoS) به یک سیستم VR، که توسط Odeleye و همکاران (۲۰۲۱) و Valluripally و همکاران (۲۰۲۰) نشان داده شده است.

۳.۳ تأثیر (Impact)

این بخش نشان دهنده تأثیر نفوذ سایبری بر تعامل، غرق شدن و حضور است.

۱.۳.۳ تعامل

تعامل در VR شامل تبادل داده‌های حسگرها برای انطباق حرکت فیزیکی به یک محیط مجازی است. برای دستیابی به این هدف از کنترلرهای لمسی و دوربین‌های عمق استفاده می‌شود. تعامل را می‌توان به ناوبری، انتخاب و مدیریت تقسیم کرد. ناوبری به حرکت در فضای VR اشاره دارد که به روش‌های مختلفی انجام می‌شود. انتخاب شامل تعامل با اشیاء مجازی مانند برداشتن آنها یا کلیک کردن روی آنها است. مدیریت به کاربران اجازه می‌دهد تا شکل، موقعیت یا جهت اشیاء مجازی را تغییر دهند. حملات سایبری می‌توانند به آسیب پذیری‌های این تعاملات، مانند تغییر اشیاء یا پیگیری حرکت فیزیکی، بهره ببرند.

۲.۳.۳ غرق شدن

غرق شدن در VR شامل تبادل داده‌های حسگری با ردیابی موقعیت و جهت بدن کاربر، با دقت بالا است. معمولاً با استفاده از کنترلرهای لمسی یا دوربین‌های عمق، حرکات دست واقعی را در محیط VR بازتاب می‌دهد. این تعامل باعث می‌شود که VR به یک هدف جذاب برای حملات سایبری تبدیل شود. یک مثال از یک حمله که می‌تواند از حرکت فیزیکی کاربر در فضای VR بهره ببرد، توسط Casey و همکاران (۲۰۱۹) توصیف شده است.

انتخاب کردن اشیاء مجازی، مانند برداشتن اشیاء یا کلیک کردن روی آنها است. یک حمله‌کننده می‌تواند الگوهای حرکات دست کاربران را از طریق اطلاعات وضعیت کانالی که توسط سیگنال‌های WiFi تولید شده است، استخراج کند و از الگوریتم‌های یادگیری ماشین برای تشخیص کلیک‌های کاربران استفاده کند، همانطور که توسط Al Arafat و همکاران (۲۰۲۰) نشان داده شده است.

۳.۳.۳ حضور

حضور تجربه ذهنیِ بودن در یک جهان VR است که به غرق شدن و مشارکت وابسته می‌باشد. این به کاربر اجازه می‌دهد تا به صورت ذهنی به جهان مجازی واکنش نشان دهد، همانند آنچه در جهان فیزیکی انجام می‌دهد. حضور، حس قابل اعتمادی را ایجاد می‌کند. تکنولوژی VR بر روی بینایی و صدا در محیط‌های سه بعدی مصنوعی تمرکز می‌کند. واقعیت مجازی می‌تواند ترس از ارتفاعات را در کاربر ایجاد کند یا کاربر را در یک جعبه پر از مارهای مختلف در جهان VR غرق کند و حس واقعی از تجربه ترس را به کاربر انتقال دهد. یک حمله‌کننده ممکن است محیط مجازی را به زور به یک کاربر از ترس‌هایش القا کند. برای پرداختن به تأثیرات چالش‌های امنیت سایبری در محیط VR، حضور را به حضور فیزیکی و حضور اجتماعی تقسیم‌بندی کردیم.

حضور فیزیکی: حضور فیزیکی درجه‌ای است که یک محیط مجازی به یک فرد در جهان VR واکنش نشان می‌دهد یا به آن پاسخ میدهد. یک مثال از یک حمله هدفمند به حضور فیزیکی، حمله «جوی استیک انسان» است که در آن کاربر به حرکت به مکان فیزیکی هدف بدون دانستن خود فریب می‌خورد. یک حمله‌کننده ممکن است محیط مجازی را به زور به یک کاربر از ترس‌هایش افشا کند.

جابجایی فیزیکی VR: به کاربر اجازه می‌دهد تا به صورت فضایی در یک فضای هندسی حرکت کند. راه‌هایی مانند راهنمایی هدایت شده، حسگرها و دیگر «تلاش‌های دریافتی مجازی – فیزیکی» که ظرفیت کاربر را برای تعامل با VR فراتر از آنچه که به طور معمول فیزیکی ممکن است، گسترش می‌دهد که می‌تواند خطرناک باشد. این‌گونه مدیریت‌ها از دانش مرزهای ادراک انسان برای ایجاد تغییرات در حرکات فیزیکی کاربر استفاده می‌کنند. یک حمله‌کننده ممکن است محیط مجازی را به زور به یک کاربر از ترس‌هایش افشا کند.

تعامل فیزیکی: تعامل فیزیکی قابلیت تعامل با اشیاء در فضای VR را فراهم می‌کند. یک کاربر که در مراحل دوم یا سوم غرق شدن است، می‌تواند به راحتی با اشیاء مخرب در فضای VR تعامل کند که می‌تواند محرمانگی، صحت و دسترسی را نقض کند. یک حمله‌کننده ممکن است یک پنجره‌ی بازی را که نیاز به تعاملی از کاربر دارد، به کاربر ارائه دهد. حضور اجتماعی: حضور اجتماعی توانایی درک دیگران و پاسخ مناسب با آنها را شامل شده که باعث رفتارهای اجتماعی و اخلاقی مشابه با رفتارهای جهان واقعی می‌شود. کاربران به حملات سایبری مانند آنچه در جهان واقعی اتفاق می‌افتد، واکنش نشان می‌دهند. یک حمله‌کننده ممکن است با استفاده از آواتار یک کاربر معتبر، با هدف گرفتن اطلاعات از شخصی که توسط آن شناخته شده است یا هک کردن یک رویداد یا فضای مجازی، به محیط مجازی وارد شود تا محتوای نامناسبی را نمایش دهد.

ارتباط: ا ارتباط در فضای VR می‌تواند به صورت مستقیم مانند جهان واقعی باشد که دو فرد به صورت مستقیم با یکدیگر ارتباط برقرار می‌کنند و این فرصت را برای حملات مهندسی اجتماعی فراهم می‌کند.

حملات شبکه می‌توانند کیفیت صدا در طول ارتباط را تحت تأثیر قرار دهند.

عوامل مجازی: عوامل مجازی شخصیت‌های کامپیوتری مبتنی بر هوش مصنوعی هستند که با کاربر در یک محیط مجازی تعامل می‌کنند. عوامل مجازی در چندین برنامه برای تقویت تعامل انسانی در فضاهای VR استفاده شده‌اند. یک حمله‌کننده ممکن است از یک عامل مجازی تقلید شده برای مهندسی اجتماعی کاربر استفاده کند.

۴.۳ هدف، قصد و نیت (Intent)

یک هکر ممکن است به سیستم VR حمله کرده و باعث آسیب رساندن به کاربر یا خود سیستم VR شود. حملات فیزیکی می‌توانند در طول تجربه VR، آسیب جسمی یا ناراحتی فیزیکی ایجاد کنند. سیستم‌های VR شامل اجزای سخت افزاری و نرم افزاری هستند که در برابر حمله قرار دارند. حملات غیر فیزیکی می‌توانند آسیب روانی ایجاد کنند، مانند مهندسی اجتماعی یا اختلال در تجربه سیستم واقعیت مجازی. دستگاه‌های VR انواع مختلفی از داده‌ها را جمع آوری می‌کنند که ممکن است بدون رضایت کاربر به صورت بدبینانه دسترسی پیدا کنند و باعث نقض حریم خصوصی و تأثیر روانی شوند. حملات می‌توانند کیفیت غوطه‌وری تجربه شده توسط کاربر را کاهش دهند. بسیار مهم است که از خطرات سلامتی مرتبط با فناوری VR، مانند سقوط یا ضربه به سر یا شکست عضو، آگاه باشید.

۴ بررسی راه‌های دفاع امنیت سایبری در واقعیت مجازی

همان‌طور که برای محیط‌های دیجیتال نسبتاً جدید معمول است، بیشتر تحقیقات در زمینه محافظت در برابر تهدیدهای امنیتی سایبری در واقعیت مجازی بر روی پیشگیری و از طریق احراز هویت تمرکز داشته است، اما در اواخر دیده می‌شود که فعالیت‌هایی در زمینه حفظ حریم خصوصی، ارزیابی ریسک سایبری و تشخیص نفوذ برای واقعیت مجازی نیز وجود دارد.

۱.۴ احراز هویت

تحقیقات در زمینه ریسک‌های امنیتی VR محدود است که می‌تواند یک مشکل باشد زیرا حملات سایبری می‌توانند تحریک حسی را تغییر دهند و آگاهی و رفتار هدفمند را تغییر دهند. روش‌های مختلفی برای احراز هویت کاربران در VR وجود دارد، مانند استفاده از احراز هویت بیومتریک یا سیستم‌های احراز هویت موجود در دنیای واقعی. به عنوان مثال: RubikAuth و RubikBiom از احراز هویت بیومتریک مبتنی بر دانش استفاده می‌کنند، درحالی‌که RepliCueAuth قابلیت اجرای روش احراز هویت مبتنی بر نشانه‌های صفحه نمایشی را بررسی می‌کند. تحقیقات دیگر از تکنیک‌هایی استفاده می‌کنند که در بیشتر محیط‌های دیجیتال معمولی غیرقابل اجرا هستند، اما در VR معنی دارند. به عنوان مثال: Iskander و همکارانش (۲۰۱۹) استفاده از هر دو چشم و فعالیت‌های عضلانی چشم برای تأیید هویت کاربر در حین استفاده از VR را نشان

دادند. یکی‌دیگر از خصوصیات مطلوب احراز هویت، قابلیت اجرا در دستگاه‌های مختلف VR است. مثالی که در Miller و همکارانش (۲۰۲۰) ارائه شده است، احراز هویت مبتنی بر رفتار در دستگاه‌های مختلف VR مانند Oculus Quest، HTC Vive و HTC Vive Cosmos را نشان می‌دهد. در زمینه احراز هویت، یکی دیگر از مسائل مورد علاقه، شناسایی کاربران در بین گروه‌های کوچک کاربران، مانند خانواده یا دفتر است. به عنوان مثال: Pfeuffer و همکارانش (۲۰۱۹) رابطه بین بخش‌های انتخاب شده بدن را برای افزایش شناسایی و احراز هویت کاربران بررسی کردند.

۲.۴ تشخیص نفوذ

تشخیص نفوذ یک جنبه مهم از امنیت VR است. کارهای اولیه به هدف توسعه چارچوب‌هایی برای تعیین سطح حمله و پیامدهای محتمل که می‌تواند منجر به تدابیر تشخیص نفوذ در آینده شود، انجام شده است. Valluripally و همکارانش (۲۰۲۰) از یک ابزار نظارت رویداد برای محیط‌های آموزشی VR استفاده کرده‌اند که بر اساس سنسورهای ساده، هشدارها را فعال می‌کند. Odeleye و همکارانش (۲۰۲۱) اولین سیستم تشخیص نفوذ را که برای حملات سایبری مبتنی بر نرخ فریم در VR اختصاصی است، توسعه داده‌اند. آنها از یک روش یادگیری ماشین ساده بدون نظارت برای ارائه هشدار زودهنگام از چنین حملاتی استفاده کرده‌اند که احتمالاً قبل از اینکه تأثیر قابل توجهی بر سیستم VR و کاربرشان داشته باشد، شناسایی می‌شوند.

۳.۴ ارزیابی ریسک سایبری

Gulhane و همکارانش (۲۰۱۹)، Valluripally و همکارانش (۲۰۲۱) یک چارچوب شامل آسیب‌پذیری و ارزیابی جامع را ارائه کرده‌اند که برای اختلالات سایبری در محیط‌های آموزشی VR اجرا شده است، اما می‌تواند در امنیت VR به طور گسترده‌تری نیز به کار رود. این چارچوب شامل ایجاد یک مدل درخت حمله–خطای نوین است، سپس تبدیل این درخت‌ها به الگوریتم‌های زمان‌بندی تصادفی و استفاده از بررسی مدل آماری برای تعیین سناریوهای تهدید است که می‌تواند باعث بروز بیشتر اختلالات سایبری شود. این چارچوب می‌تواند با نشان دادن جایگاه و نحوه یکپارچه‌سازی اصول طراحی تقویت، تنوع و تکرار برای حفظ ایمنی کاربر موثر باشد.

۴.۴ حفظ حریم خصوصی

Maloney و همکارانش (۲۰۲۰) مصاحبه‌هایی را انجام دادند و متوجه شدند که کاربران در فضاهای اجتماعی VR با افشای اطلاعات شخصی خود راحت هستند، اما نگران افشای اطلاعات به غریبه‌ها هستند. آنها چهار راهبرد برای حمایت از حریم خصوصی کاربران پیشنهاد دادند، از جمله آموزش کاربران، استفاده از مدولاتور صدا، تولید آواتارهای غیر قابل شناسایی و تطبیق تنظیمات حریم خصوصی رسانه‌های اجتماعی.

Falchuk و همکارانش (۲۰۱۸) یک ابزار حفظ حریم خصوصی را پیشنهاد دادند که به کاربران امکان کنترل گزینه‌های حفظ حریم خصوصی ارائه شده به آنها در حین استفاده از VR را می‌دهد. چندین تکنیک حفظ حریم خصوصی مورد بحث قرار گرفت، مانند ایجاد ابر از کلون‌های آواتار کاربر، اجازه به کاربران برای

سکونت در یک کپی خصوصی از دنیای مجازی و اجازه به کاربر برای تبدیل شدن به نامرئی برای آواتارهای دیگر به مدت مشخصی.

John و همکارانش (۲۰۱۹) یک راه‌حل مبتنی بر فاکوس برای حفاظت از داده‌های ردیابی چشم با یک مکانیزم سخت‌افزاری که یک فیلتر ماتی را به تصاویر چشم پیش‌تصویرگری شده اعمال می‌کند، پیشنهاد دادند تا قبل از آنکه این ویژگی توسط حسگر دوربین چشم ضبط شود، آن را حذف کند.

۵ مطالب و حوزه‌ها برای تحقیقات بیشتر

تحقیقات در زمینه امنیت سایبری VR هنوز در مراحل اولیه خود است و بسیاری از حوزه‌ها نیاز به بررسی بیشتر دارند. این حوزه‌ها شامل الگوهای جدید حمله، پاسخ خودکار به نفوذ و مجموعه داده‌ها و آزمایشگاه‌ها هستند.

۱.۵ الگوهای جدید حمله

حملات فعلی بر سیستم‌های VR به طور اصلی بر روی بهره‌برداری از تحریکات بصری تمرکز دارند. بااین‌حال، پژوهشگران باید به آسیب‌پذیری‌های معرفی شده از طریق جنبه‌های صوتی، لمسی و بویایی و همچنین سطح حمله نیز نگاه کنند. آنها همچنین باید حملاتی را که از شباهت رفتاری بهره می‌برند و کاربر به واسطه قانون عملکرد فرضی فریب داده می‌شود را نیز مورد مطالعه قرار دهند.

۲.۵ پاسخ خودکار به نفوذ

تحقیقات فعلی در زمینه روش‌های دفاع سایبری در این حوزه به طور اصلی درباره تدابیر پیشگیرانه برای احراز هویت و حفظ حریم خصوصی، از جمله ارزیابی ریسک سایبری، بوده است. هنوز هیچ‌کاری مربوط به پاسخ به یک نقض امنیتی انجام نشده است. پژوهشگران می‌توانند همچنین توصیه‌های عملیاتی به کاربر و عملیات خودکار توسط سیستم را مورد پژوهش و تحقیق قرار دهند.

۳.۵ ایجاد مجموعه داده‌ها و آزمایشگاه‌ها

پیشرفت در امنیت سایبری VR به دلیل عدم وجود مجموعه داده‌های عمومی در مورد رفتار عادی و حمله، و همچنین عدم دسترسی به آزمایشگاه‌ها محدود شده است. توسعه یک آزمایشگاه برای انجام تحقیقات سایبری VR نیاز به تلاش و ترکیب مهارت‌های توسعه VR و سایبری است که به طور معمول در یک گروه تحقیقاتی یکسان یافت نمی‌شود.

۶ نتیجه‌گیری

واقعیت مجازی به عنوان یک فناوری جدید نیست، اما تنها در چند سال گذشته نقش برجسته‌تر آن باعث جذب توجه جامعه تحقیقاتی امنیت سایبری شده است. به همین دلیل، ما تنها در حال حاضر شروع به درک

تهدیدهای سایبری مختلفی هستیم که با پذیرش گسترده آنها همراه است. به تازگی، تقریباً تمام تحقیقات مرتبط بر روی احراز هویت کاربر بوده که در آن فرض بر این بود که جلوگیری از استفاده بدون احراز هویت برای مقابله با بخش عمده چالش کافی است. این درحال تغییر است زیرا تحقیقات جدید نشان می‌دهد که چگونه حملات مختلفی در VR انجام می‌شود. ما یک طبقه‌بندی را به عنوان یک روش برای ارائه دید کلی از چشم‌انداز تهدید سایبری VR ارائه دادیم و این در عوض به ما کمک کرد تا جنبه‌های استفاده از VR را که هنوز توسط دفاع‌های موجود پوشش داده نشده‌اند، شناسایی کنیم. در نهایت، ما مثال‌هایی را ارائه دادیم که در تحقیقات آتی امنیت سایبری VR مفید خواهد بود.

مراجع

[1] Casey, P., Baggili, I., Yarramreddy, A., 2019. Immersive virtual reality attacks and the human joystick. IEEE Trans. Dependable Secure Comput..

[2] Al Arafat, A., Guo, Z., Awad, A., 2021. VR-spy: a side-channel attack on virtual key-logging in VR headsets. In: Proceedings of the IEEE Virtual Reality and 3D User Interfaces (VR). IEEE, pp. 564–572.

[3] Gulhane, A., Vyas, A., Mitra, R., Oruche, R., Hoefer, G., Valluripally, S., Calyam, P., Hoque, K.A., 2019. Security, privacy and safety risk assessment for virtual real-ity learning environment applications. In: Proceedings of the 16th IEEE Annual Consumer Communications , Networking Conference (CCNC). IEEE, pp. 1–9.

[4] Valluripally, S., Gulhane, A., Hoque, K.A., Calyam, P., 2021. Modeling and defense of social virtual reality attacks inducing cybersickness. IEEE Trans. Dependable Secure Comput..

[5] Maloney, D., Freeman, G., 2020. Falling asleep together: what makes activities in social virtual reality meaningful to users. In: Proceedings of the Annual Sympo-sium on Computer-Human Interaction in Play, pp. 510–521.

[6] Falchuk, B., Loeb, S., Neff, R., 2018. The social metaverse: battle for privacy. IEEE Technol. Soc. Mag. 37 (2), 52–61.

[7] John, B., Jörg, S., Koppal, S., Jain, E., 2020. The security-utility trade-off for iris authentication and eye animation for social virtual avatars. IEEE Trans. Vis. Com-put. Graph. 26 (5), 1880–1890.

[8] Pfeuffer, K., Geiger, M.J., Prange, S., Mecke, L., Buschek, D., Alt, F., 2019. Behavioural biometrics in VR: identifying people from body motion and relations in virtual reality. In: Proceedings of the CHI Conference on Human Factors in Computing Systems, pp. 1–12.

[9] Iskander, J., Abobakr, A., Attia, M., Saleh, K., Nahavandi, D., Hossny, M., Nahavandi, S., 2019. A K-NN classification based VR user verification using eye movement and ocular biomechanics. In: Proceedings of the IEEE International Conference on Systems, Man and Cybernetics (SMC). IEEE, pp. 1844–1848.

[10] Sutherland, I., 1965. The ultimate display.

[11] Market, V., 2020. Virtual reality market with COVID-19 Impact analysis by offer-ing (hardware and software), technology, device type (head-mounted display, gesture-tracking device), application (consumer, commercial, enterprise, health-care) and geography - global forecast to 2025.

[12] Aliman, N.-M., Kester, L., 2020. Malicious design in AIVR, falsehood and cybersecu-rity-oriented immersive defenses. In: Proceedings of the IEEE International Con-ference on Artificial Intelligence and Virtual Reality (AIVR). IEEE, pp. 130–137.

تأثیر فناوری واقعیت افزوده در تعامل با محیط زیست

صادق عسگریلو [۱]، شکوه کرمانشاهانی [۱]

[۱] گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه بین‌المللی امام خمینی(ره)، قزوین، ایران
sadeghasgarilou@gmail.com ،kermanshahani@eng.ikiu.ac.ir

چکیده

به دلیل آسیب‌های شدید وارده به منابع زیستی به ارتقای سطح آگاهی‌های عمومی برای حفاظت از محیط‌زیست بیش از پیش نیاز داریم. روش‌های سنتی آموزش محیط‌زیست، به دلیل نداشتن فاکتورهایی چون جان‌بخشی، حضور و تعلق به مکان، چندان کارا نبوده‌اند. این مقاله به بررسی استفاده از بازی فراگیر مبتنی بر واقعیت افزوده برای آموزش محیط زیست می‌پردازد و بعنوان نمونه کاربردی، باغستان تاریخی قزوین مورد بررسی قرار گرفته است. باغستان قزوین یکی از معدود نمونه‌های زنده بوم‌سازگان‌های اطراف شهر است که هنوز کارکرد، جامعیت، خصوصیات پیچیده و تا حد زیادی حکمرانی خرد مبتنی بر تعامل با شهر را حفظ کرده است. در عین حال باغستان در معرض تهدید جدی ناشی از عدم شناخت شهرنشینان و تصمیم‌گیران قرار دارد. در این پژوهش پس از بررسی ویژگی‌های باغستان سنتی قزوین و مطالعه پژوهش‌های نظری و برنامه‌های کاربردی مشابه، تاثیر بازی فراگیر مبتنی بر واقعیت افزوده در ایجاد حس تعلق به محیط زیست سنجیده شده است. نتایج نشان میدهد که استفاده از واقعیت افزوده شیوه تعاملی موثری برای افزایش حس تعلق به محیط زیست و رویکرد آموزشی و حساسیت‌زایی محیط زیست است.

کلمات کلیدی: آموزش محیط زیست، بازی فراگیر، واقعیت افزوده.

۱ مقدمه

آموزش‌های محیط زیستی [۱] که در محدوده کلاس و بدون ارتباط با محیط واقعی صورت می‌گیرد، در برانگیختن شور و اشتیاق دانش‌آموزان چندان موفق نیستند و افراد از نظر احساسی، ارتباط لازم را برقرار نمی‌کنند [۴]، [۵]. بسیاری از مطالعات مهم نشان می‌دهند که احساسات، یکی از فاکتورهای مهم در یادگیری است که معمولا نادیده گرفته می‌شود [۶]، [۷]. همچنین تجسم‌بخشی به آموزه‌ها، در آموزش‌های محیط‌زیستی، نقش حیاتی دارد. اگرچه استفاده از تصاویر و فیلم می‌تواند در این مورد تا حدی راهگشا باشد، اما حضور در محیط واقعی، و تعامل حسی و فیزیکی با محیط، اثرگذاری و پایداری بیشتری دارد [۴]،[۷].

[1] Eco-Education

این پژوهش، با این فرض که می‌توان آموزش و حساسیت‌زایی محیط‌زیستی کودکان و نوجوانان را با کمک ابزارهای مورد علاقه آنها نظیر رایانه‌های سیار موثرتر کرد، برنامه‌ریزی شد.

آموزش محیط زیستی، در محیط واقعی و فضای بیرون، می‌تواند به شکل‌های مختلفی ارائه شود. رویکرد آموزشی متداول در زمینه آموزش‌های محیط زیستی در محیط واقعی، این است که یک راهنما دانش‌آموزان را در محیط مورد نظر، راهنمایی و هدایت می‌کند. با این همه، این روش نیز یک روش منفعل است که در آن تجربه‌ها و اکتشاف محیط برای دانش‌آموزان محدود می‌شود. به طور کلی، یادگیری مبتنی بر تجربه، با آموزش مبتنی بر معلم از نظر روش و اثربخشی متفاوت است؛ یادگیری مبتنی بر تجربه بر روی قضاوت مستقل، فکر کردن آزاد و تجربه شخصی تاکید ویژه دارد [۴]. از مهم‌ترین ویژگی‌هایی که آموزش محیط‌زیستی می‌بایست دنبال کند، و در روش مبتنی بر تجربه بیشتر قابل حصول است، «حس تعلق یا دلبستگی» به مکان یا همان عرصه محیط زیستی است [۸]. انتخاب و به‌کارگیری صحیح فناوری آموزشی مناسب، برای ارتقاء حس تعلق به محیط‌زیست در دانش‌آموزان، مهم‌ترین هدف این پژوهش است.

ما در این پژوهش، از طریق بهره‌گیری از فناوری «واقعیت افزوده[۲]» در آموزش و به شیوه بازی برای کودکان و نوجوانان، ارتقاء «حس تعلق یا دلبستگی» به یک عرصه محیط زیستی را برنامه‌ریزی کردیم، با مرور پژوهش‌های مرتبط، عوامل موثر در ارتقاء آموزش و حساسیت‌زایی محیط زیستی را شناسایی و سپس یک بازی فراگیر[۳] طراحی کردیم، و از طریق یک مطالعه کاربری[۴] در محیط واقعی و به روش اکتشافی[۵] نیلسون تاثیر روش جدید آموزش را بر دانش‌آموزان سنجیدیم. ابتدا مورد کاربرد پروژه خود را معرفی می‌کنیم.

۱.۱ مورد کاربرد: باغستان سنتی قزوین

مورد کاربرد ما در این پژوهش، باغستان سنتی قزوین است. باغستان ویژگی‌هایی دارد که آن را از سایر عرصه‌های محیط زیستی و کشاورزی متمایز می‌کند. باغستان سنتی قزوین با قدمت بیش از هزار سال و در حال حاضر به وسعت ۲۷۸۰ هکتار، از سه طرف، شهر قزوین را در بر گرفته است. باغستان سنتی قزوین تاثیر محیط زیستی فراوانی بر شهر قزوین و حتی شهرها و استان‌های اطراف قزوین دارد، اما در دهه‌های اخیر در معرض تهدید جدی قرار گرفته و بخش قابل توجهی از آن تخریب شده است [۱].

علاوه بر عواملی مانند توسعه نامتوازن و ناپایدار و عدم توجه به ظرفیت‌های اکولوژیکی، بی‌توجهی عمومی به حفظ منابع زیستی، و عدم شناخت از اهمیت حیاتی این منابع و به طور خاص باغستان سنتی قزوین، عامل مهم و زیربنایی دیگری است که زمینه این تخریب‌ها را تقویت کرده است. لزوم تدوین برنامه آموزشی باغستان برای همه رده‌های سنی و به ویژه دانش‌آموزان، زمانی مشخص می‌شود که بدانیم باغستان تا چند دهه پیش مانند حلقه‌ای سبز شهر را در بر گرفته بود و وسعت آن حدود ۴۰۰۰ هکتار بود [۱].

باغستان ویژگی‌هایی دارد که آن را از سایر عرصه‌های محیط زیستی و کشاورزی متمایز می‌کند [۱].

[2] Augmented Reality
[3] Pervasive Game
[4] Usability Study
[5] Heuristic Evaluation

هر ابزار آموزشی که بر روی پهنه اکولوژیک طراحی می‌شود، باید با شرایط و ساختار باغستان سازگار باشد. بخشی از ویژگی‌های باغستان سنتی قزوین، که باید در تدوین یک برنامه آموزشی مورد توجه خاص قرار بگیرد، عبارت از موارد زیر است [۱]، [۲]:

- یکی از خصوصیات باغستان این است که این عرصه یکپارچه، از کنار هم قرار گرفتن بخش‌های متعدد کوچک‌تری تشکیل شده است که هر کدام مالک خصوصی دارند؛ بنابراین حفظ آن منوط به همکاری این مالکان در یک نظام مشارکتی است.
- باغستان محور یک سامانه آبخیزداری/آبخوانداری است. آب چهار رودخانه فصلی در زمستان و بهار، وارد شبکه نهرهای باغستان می‌شوند. باغ‌های باغستان، همگی مانند استخرهای کوچک هستند و با کَرت‌هایی (دیوارها) به ارتفاع ۱ تا ۵.۱ متر از هم جدا می‌شوند؛ آب هر رودخانه به نوبت وارد باغ‌ها می‌شود و باغ‌ها تا ارتفاع کرت‌ها غرقاب می‌شوند. نوبت آب بر مبنای طومار تاریخی آب انجام می‌شود (بیش از ۷۰۰ سال که مهر جغرافیدان و مورخ ایرانی، حمداله مستوفی، را نیز ذیل خود دارد). دانش بومی تقسیم آب باغستان، در فهرست آثار ملی به ثبت رسیده است [۳].
- «دخو» یکی از مهم‌ترین شخصیت‌های باغستان است. از میان باغبانان هر محل، آن کس که مجرب‌تر بوده باشد، به امور باغبانی و منافع مشترک محل مدیریت می‌کند، و در رفع اختلافات، رسیدگی به باغ‌های رها شده، سهم‌بندی محصول، برقراری امنیت و ... مرجع باغبانان و باغداران محل می‌شود؛ متاسفانه در چند دهه اخیر نقش دخو در باغستان کمرنگ شده است.

۲ پژوهش‌های مشابه

آموزش به دانش‌آموزان با استفاده از واقعیت افزوده و بازی فراگیر، موضوع جدیدی است؛ بنابراین تحقیقات و کارهای کمی در این زمینه انجام شده است. با این وجود، نتایج پژوهش‌های انجام شده بیانگر این نکته است که استفاده از واقعیت افزوده و بازی فراگیر، تاثیر مثبتی در نحوه ارتباط دانش‌آموزان با محیط زیست دارد [۴]، [۱۳]، [۱۴]. در این بخش به بررسی پژوهش‌های مشابه‌ای می‌پردازیم که از بازی‌های فراگیر مبتنی بر واقعیت افزوده در حوزه آموزش، به ویژه آموزش‌های محیط زیستی استفاده کرده‌اند؛ همچنین عوامل و عناصر مختلف بازی‌های توسعه داده شده در این پژوهش‌ها، مورد بررسی قرار می‌گیرند.

در بازی «مد سیتی میستری[۶]» که در سال ۲۰۰۷ اجرا شده است، دانش‌آموزان راز مرگ یک شخصیت مجازی را کشف می‌کردند. هدف این پژوهش بررسی میزان مشارکت دانش‌آموزان در آموزش موضوعات علمی است. بر اساس نتیجه این پژوهش، چنین بازی‌هایی ظرفیت جذب دانش‌آموزان را در استدلال‌های علمی معنادار دارند [۱۵].

بازی طراحی شده توسط روزنباوم و همکاران [۱۵] در سال ۲۰۰۷ اجرا شده است. در این پژوهش دانش‌آموزان در قالب گروه‌ها و با همکاری یکدیگر و از طریق ارتباط با محتوای مجازی، می‌بایست منبع یک

[6] Mad City Mistery

بیماری را پیدا کرده و از گسترش آن جلوگیری کنند. نتیجه این پژوهش حاکی از این است که شرکت‌کنندگان در فرآیند بازی جذب شده و ماهیت موضوع مورد آموزش را درک کرده‌اند.

هدف برنامه آموزش طراحی شده توسط دونلوی و همکاران [۶]، آموزش دروس ریاضی، هنرهای زبانی و تاریخچه علم به دانش‌آموزان دوره راهنمایی و دبیرستان است. سناریوی این بازی شامل کاوش در محیط، مصاحبه و مکالمه با شخصیت‌های مجازی، جمع‌آوری سرنخ‌های مجازی، حل مسائل ریاضی، هنر و علم است. نتایج این پژوهش، بیانگر این است که با استفاده از واقعیت افزوده و رویکرد آموزشی استفاده شده در این پژوهش، دانش‌آموزان علاقه بیشتری به مشارکت در مباحث دروس مختلف دارند.

در یک بازی طراحی شده برای آموزش تاریخ شهر آمستردام در سال ۲۰۱۲، از یک صفحه داستانی[۷] واقعی برای طراحی بازی استفاده شده است. دانش‌آموزان در این بازی نقش یک افسر پلیس را بازی می‌کنند و به منظور برطرف کردن مشکل مواد مخدر با شخصیت‌های مجازی ملاقات می‌کنند. در قالب این داستان و سناریو دانش‌آموزان در طول بازی با مکان‌های مهم آمستردام و تاریخ آن آشنا می‌شوند. در این پژوهش چهار معیار مختلف شامل رویکرد استفاده از بازی برای آموزش، رابط کاربری، محتوای مجازی و داستان بازی، پس از آزمایش بر روی شرکت‌کنندگان مورد ارزیابی قرار گرفته‌اند و این معیارها، از دید شرکت‌کنندگان بازی قابل قبول ارزیابی شده‌اند [۱۶].

در برنامه طراحی‌شده توسط برسلر و بودزین [۱۷] در سال ۲۰۱۳، داستان کلی برنامه کشف ماجرای یک دزدی است. در این پژوهش دانش‌آموزان به گروه‌های ۳ یا ۴ نفری تقسیم شده‌اند. سناریوی این بازی به گونه‌ای طراحی شده است که گروه در طول بازی در کنار هم بازی را ادامه داده و اعضای آن از یکدیگر جدا نمی‌شوند. نتایج این پژوهش حاکی از این است که استفاده از بازی‌های مبتنی بر واقعیت افزوده در افزایش علاقه‌مندی دانش‌آموزان به موضوعات علمی تاثیر مثبت دارد.

برنامه آموزشی طراحی شده توسط کاماراینن و همکاران [۱۷] در سال ۲۰۱۳، مبتنی بر کار گروهی است. فرآیند این بازی به گونه‌ای طراحی شده است که دانش‌آموزان در محیط یک حوضچه محلی درگیر داستان بازی شده و از این طریق با مسائل محیط زیستی آشنا می‌شوند. نتایج نظرسنجی از دانش‌آموزان و بازخورد معلمان نشان می‌دهد که استفاده از این مجموعه فن‌آوری، مزایای بسیاری برای تدریس و یادگیری دارد.

برنامه طراحی شده در پژوهش هووانگ و همکاران [۴] سال ۲۰۱۶، در محیط موزه ملی طبیعی تایچونگ کشور تایوان اجرا شده است. هدف این بازی آموزش محیط زیست به دانش‌آموزان و همچنین بررسی نقش راهنما در بازی‌های مبتنی بر واقعیت افزوده است. این بازی نیز به صورت گروهی انجام می‌شود. نتیجه این پژوهش نشان می‌دهد که استفاده از فناوری نو که برای دانش‌آموزان جذاب است، علاقه آن‌ها را به یادگیری افزایش می‌دهد.

بازی فراگیر طراحی شده در پژوهش مظفری و همکاران [۱۹] سال ۲۰۲۳ در محیط دانشگاه بین المللی امام خمینی(ره) در قزوین انجام شد. هدف بازی کمک به آموزش زبان فارسی به غیر فارسی‌زبانان بوده است

[7] Storyboard

و بازی بر ایجاد انگیزه جهت تعامل بهتر زبان‌آموزان با مردم در محیط دانشگاه تمرکز کرده است. نتایج این پژوهش نشان می‌دهد که بازی فراگیر به‌خوبی می‌تواند ترس ارتباط با محیط را کاهش دهد، و بر کیفیت آموزش زبان بیفزاید.

برخی از عناصر و اجزای بازی فراگیر، مانند انجام بازی به صورت گروهی، ارتباط افراد با محیط طبیعی و ترکیب عناصر مجازی با دنیای واقعی، در پژوهش‌های انجام شده مشترک است. تعداد دیگری از عناصر مانند زمان بازی و تعداد شرکت‌کنندگان نقش خاصی در تاثیرگذاری روند آموزشی ندارند. اما تعدادی از عناصر و اجزای بازی فراگیر در فرآیند آموزش تاثیرگذار بوده و همچنین در پژوهش‌های انجام شده به صورت متفاوت به کار گرفته شده‌اند. این عناصر و اجزای بازی‌های فراگیر که الهام‌بخش ما در توسعه و طراحی بازی فراگیر آموزش باغستان سنتی قزوین بوده است، از پژوهش‌های مختلف استخراج شده است.

۳ طرح بستر آزمایشی

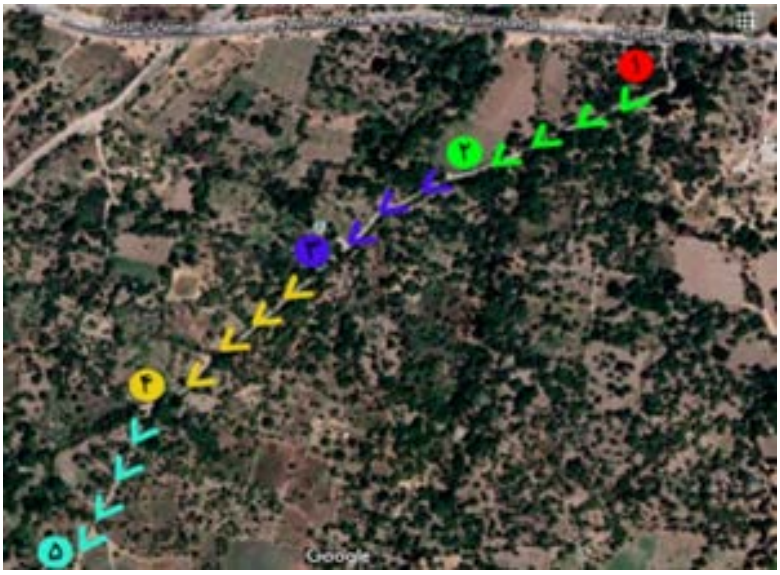
گام اول برای توسعه برنامه طراحی شده برای آموزش ترویجی باغستان سنتی قزوین، مشخص کردن سکویی[۸] است که برنامه بر روی آن اجرا خواهد شد. فناوری سکوی پیشنهادی برای پیاده‌سازی برنامه آموزشی مبتنی بر واقعیت افزوده در محیط باغستان، تلفن‌های همراه مبتنی بر سیستم عامل اندروید است. مهم‌ترین مزایای تلفن همراه شامل قابل حمل بودن، هزینه کمتر، در دسترس بودن، سادگی در استفاده و انجام عملیات مستقل است [۱۹]؛ به موارد ذکر شده باید آشنایی عمومی با تلفن‌های همراه هوشمند را هم بیفزاییم.

در عین حال استفاده از تلفن هوشمند چالش‌هایی هم دارد که باید به آن‌ها توجه کرد. به دلیل آموزش در محیط خارج از کلاس درس، عواملی نظیر صدای محیط، نور آفتاب و محدودیت باتری برای تلفن‌های همراه می‌توانند بر تعامل افراد تاثیر گذار باشند، و حتی منجر به تجربه‌ای منفی برای افراد استفاده کننده شود [۹].

از آنجا که در این پژوهش، تمرکز بر روی ارائه یک برنامه آموزشی است که مورد پذیرش جامعه هدف قرار گیرد و نیز تاثیر گذار باشد، استفاده از یک روش تعامل و رابط کاربری که کار با آن برای جامعه هدف (دانش‌آموزان) ساده و یادگیری آن آسان باشد، ضروری است [۱۰].

پس از تعیین سکوی توسعه و انتخاب شیوه تعامل و رابط کاربری، گام بعدی تعیین سناریوی بازی است. قدم نخست در طراحی برنامه آموزش محیط زیست بر بستر بازی فراگیر، تعیین داستان کلی برنامه آموزشی است؛ سایر قسمت‌های برنامه بر مبنای این داستان طراحی می‌شوند و بدون آن برنامه انسجام نخواهد داشت. داستان کلی باید بر مبنای هدف آموزشی و جامعه هدف طراحی شود [۱۱]؛ باید این نکته را در نظر گرفت که سناریو بر مبنای داستان انتخاب شده به گونه‌ای طراحی شود که دارای پایان مشخص باشد و افراد بتوانند جواب معمای داستان را کشف کنند. برای نسخه ابتدایی برنامه، کشف مکان گنج موجود در باغستان را به عنوان چارچوب داستان بازی آموزشی انتخاب کردیم؛ به همین دلیل برنامه خود را با نام «گنج باغستان» برای تلفن‌های همراه مبتنی بر سامانه عامل اندروید طراحی کرده‌ایم. فعالیت دانش‌آموزان در طول بازی با

[8] Platform



شکل ۱: نقاط داغ تعیین شده در باغستان برای ملاقات دانش آموزان با باغداران

هدف پیدا کردن این گنج صورت می‌گیرد.

معمولا دانش‌آموزان در بازی‌های فراگیر آموزشی مبتنی بر واقعیت افزوده که در محیط بیرون اجرا می‌شوند، در هر مکان برای رسیدن به مرحله بعدی، باید اقدام به انجام وظیفه‌ای خاص و یا حل معمایی کنند [۱۲]. به عبارت دیگر سناریوی برنامه‌های آموزشی باید شامل تعدادی مرحله باشد که دانش‌آموز در هر کدام از آن‌ها توقف کرده و با حل مسئله مربوط به آن مرحله مجوز راه‌یابی به مرحله بعد را پیدا می‌کند [۱۸]. بازی پیشنهادی شامل ۵ مرحله است. هر محله در یک مکان خاص از باغستان انجام می‌شود. در کارهای مشابه انجام شده این مکان‌ها در بازی به نقاط داغ[۹] معروف هستند، مانند طرح مسیر شکل. بازی به طور کلی عبارت است از تکرار این فرآیند :۱- حضور در نقطه داغ مربوط به هر مرحله ۲- حل معمای موجود در نقطه داغ ۳- پیدا کردن نقطه داغ بعدی. بنابراین نیاز است مسیر مراحل مختلف در نقشه مشخص شود. این نقاط داغ که شامل نقاط کلیدی برای آموزش باغستان به دانش‌آموزان هستند، بر اساس مشورت با باغداران تعیین شدند. سپس برای هر نقطه داغ بر اساس داستان کلی برای هر نقش گروه یک معما طراحی شد. معماها از ترکیب مواد درسی متناسب با دانش‌آموزان، ویژگی‌های باغستان و داستان کلی بازی طراحی شده است. وظایف معماها علاوه بر تشویق دانش‌آموزان به شرکت در بازی و پیدا کردن راز بازی، آموزش نکات مربوط به باغستان است[۱۰].

[9] Hot Spot

[۱۰] شرح جزییات بازی و راهنمای کار با آن در پایان نامه کارشناسی ارشد صادق عسگریلو در دانشگاه بین المللی امام خمینی(ره) ثبت شده است.

۴ مطالعه کاربری

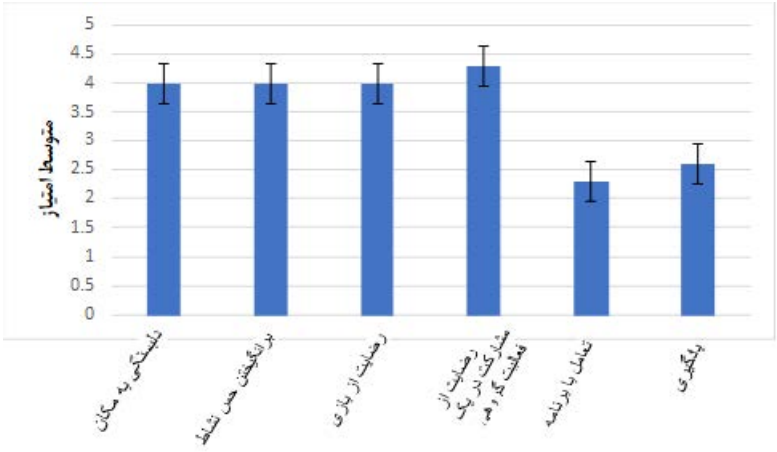
برای ارزیابی عملکرد طرح بازی، از طریق یک مطالعه کاربری اقدام کردیم. در این مطالعه از روش ارزیابی اکتشافی مبتنی بر نظر متخصصان بهره بردیم. برای ارزیابی اصول اکتشافی نیلسون [۱۵] و اصول استخراجی از پژوهش‌های مشابه، از ۹ متخصص حوزه آموزش و تعامل انسان و کامپیوتر با سابقه بیش از ۸ سال برای ارزیابی و تکمیل پرسشنامه کمک گرفته شد. ابتدا کارشناسان از طریق فیلم تهیه شده بر اساس آزمایش عملی بازی در محیط باغستان و فایل متنی راهنمای برنامه، که در آن قسمت‌های مختلف برنامه به طور کامل تشریح شده است، با آن آشنا شدند. سپس از طریق ارتباط مجازی و پاسخ به سوالات آن‌ها، نکات مبهم این برنامه را برای آنها برطرف کرده تا مطمئن شویم به طور کامل با برنامه ارتباط برقرار کرده‌اند. در نهایت کارشناسان با توجه به میزان رعایت شدن هر کدام از معیارها در بازی طراحی شده، به عبارت‌ها امتیاز داده و نظرات یا مشکلات موجود را در بخش توضیح مربوط به هر عبارت بیان می‌کنند. در این بخش نتیجه این ارزیابی‌ها به تفکیک هر معیار ارائه خواهد شد. میانگین نمره‌هایی که کارشناسان برای هر کدام از این معیارهای ارزیابی اثرگذاری آموزشی و شیوه تعاملی برنامه آموزش محیط زیست در نظر گرفته‌اند در شکل ۲ قابل مشاهده است.

برنامه آموزشی طراحی شده به میزان قابل قبولی در تقویت حس دلبستگی به مکان در دانش‌آموزان موفق (امتیاز ۴ از ۵) بوده است. جذابیت مراحل بازی، رابط کاربری مناسب و سطح استاندارد معماهای مطرح شده در طول بازی در تقویت این حس موثر است. برنامه نمره متوسطی از رعایت معیار تعامل دریافت کرده است (۳.۲ از ۵). خطا در سامانه موقعیت‌یابی جهانی (جی.پی.اس.)، عامل اصلی دریافت نمره متوسط اصل تعامل افراد با برنامه است. جلوگیری از این خطا از امکانات این پژوهش فراتر است، اما میتوان امید داشت که در آینده و با پیشرفت این فناوری بروز خطا در این زمینه کاهش پیدا کند. همچنین بر مبنای نظر کارشناسان می‌توان اظهار کرد که استفاده از این روش در برانگیختن حس نشاط دانش‌آموزان تا حدودی موفق است و می‌تواند در نهایت حس دلبستگی به مکان را در دانش‌آموزان تقویت کند.

۵ نتیجه‌گیری

این پژوهش با تمرکز بر افزایش حس تعلق به محیط در فرآیند آموزش محیط زیست طراحی شده است. استفاده از بازی فراگیر به کمک فناوری واقعیت افزوده ایده‌ای است که در پژوهش‌های مرتبط نیز به کار گرفته شده است اما مورد کاربرد این پژوهش، باغستان سنتی قزوین، شرایط خاصی را بر فرآیند آموزش الزامی می‌کند. به دلیل تخریب‌های صورت گرفته، بخشی از عوامل موثر در این عرصه زیستی از میان رفته‌اند و لذا باید به کمک فناوری به بستر آموزشی اضافه شوند. همچنین بعضی موقعیت‌های اجتماعی–اقتصادی موثر در عدم توجه به ویژگی‌های خاص این عرصه زیستی هم اکنون حضور دارند، لذا طرح بازی می‌بایست این عوامل را مورد توجه قرار دهد.

بر اساس پژوهش‌های بررسی شده، مردم در صورتی نسبت به یک مکان حس قوی دلبستگی دارند که تجربه فعالیت، آرامش، بازتولید و یا گذران اوقات فراغت و آسودگی در آن مکان را داشته باشند. تعامل مکرر



شکل ۲: میانگین نمرات کارشناسان به اصول استخراجی بر اساس میزان رعایت این اصول در برنامه.

با یک مکان و بازدید زیاد از یک محیط، احساسات، شناخت و جنبه‌های ابراز دلبستگی نسبت به آن محیط را ارتقا می‌دهد.

نتایج ارزیابی این پژوهش نشان می‌دهد که طرح پیشنهادی بازی فراگیر مبتنی بر واقعیت افزوده در دل‌بستگی به مکان و برانگیختن نشاط دانش‌آموزان بسیار موثر بوده است. تقویت حس دل‌بستگی به مکان یکی از مزایای بازی فراگیر است؛ دل‌بستگی به مکان منجر به ایجاد حس خوشبختی و پرورش حس تعلق می‌شود؛ همچنین می‌توان از آن برای فعالیت‌های حفظ محیط زیست استفاده کرد. بنابراین حس دل‌بستگی به مکان اهمیت فراوانی در یک برنامه آموزشی محیط زیست دارد و باعث اثرگذاری آموزش محیط زیستی می‌شود. به این معنی که دانش‌آموزان به صورت دراز مدت و نهادینه، برای حفظ آن محیط تلاش خواهند کرد.

مراجع

[۱] کرماشاهانی، ش. (۱۳۹۵) «فراز و فرود تمدن شهری متاثر از مدیریت شرایط زیستی؛ باغستان سنتی قزوین»، کنگره ملی تاریخ معماری ایران.

[۲] ارزانی، ک. (۱۳۸۲) «نگرشی بر اهمیت، حفظ، نگهداری، اصلاح و مدیریت مناسب باغ های سنتی ایران»، اولین همایش باغ های سنتی.

[۳] رضایی، م. (۱۳۹۸) «دانش بومی مدیریت و مهار سیلاب در باغستان سنتی قزوین: سزاوار نگاهی نو در زمینه حفاظت و احیا»، هشتمین همایش ملی سامانه های سطوح آبگیر باران،

[4] Huang, T. C., Chen, C. C. & Chou, Y. W. (2016). ”Animating eco-education: To see, feel, and discover in an augmented reality-based experiential learning environment”. Computers and Education, 96, 72–82.

[5] Dalim, C. S. C., Kolivand, H., Kadhim, H., Sunar, M. S., & Billinghurst, M. (2017). "Factors influencing the acceptance of augmented reality in education: A review of the literature". Journal of Computer Science, 13(11), 581–589.

[6] Dunleavy, M., Dede, C., & Mitchell, R. (2009). "Affordances and limitations of immersive participatory augmented reality simulations for teaching and learning". Journal of Science Education and Technology, 18(1), 7–22.

[7] Balog, A. & Pribeanu, C. (2010). "The Role of Perceived Enjoyment in the Students' Acceptance of an Augmented Reality Teaching Platform : a Structural Equation Modelling Approac". Journal of Studies in Informatics and Control, 19(3), 319–330.

[8] Brown, G. & Raymond, C. (2007). "The relationship between place attachment and landscape values : Toward mapping place attachment". Journal of Applied Geography, 27, 89–111.

[9] Martínez, H., Skournetou, D., Hyppölä, J., Laukkanen, S. & Heikkilä, A. (2014). "Drivers and Bottlenecks in the Adoption of Augmented Reality Applications". Journal of Multimedia Theory and Applications, September, 2(1), 27-44.

[10] Bhorkar, G. (2017). "A Survey of Augmented Reality Navigation". Journal of Foundations and Trends in Human-Computer Interaction, 8(2), 73–272.

[11] Azuma, R. T. (1997). "Survey of Augmented Reality". Massachusetts institute of Technology, 6(4), 355–385.

[12] Oleksy, T. & Wnuk, A. (2017). "Catch them all and increase your place attachment! The role of location-based augmented reality games in changing people - place relations". Computers in Human Behavior, 76, 3-8.

[13] Dede, C. J., Jacobson, J., & Richards, J. (2017). "Introduction: Virtual, Augmented, and Mixed Realities in Education". Springer, Singapore, 1, 1–16.

[14] Metcalf, S. J., Reilly, J. M., Kamarainen, A. M., King, J., Grotzer, T. A. & Dede, C. (2018). "Supports for deeper learning of inquiry-based ecosystem science in virtual environments - Comparing virtual and physical concept mapping". Computers in Human Behavior, 87, 459–469.

[15] Nielsen, J. & Molich, R. (1990). "Heuristic evaluation of user interfaces". Conference on Human Factors in Computing Systems, 1, 249–256.

[16] Squire, K. D. & Jan, M. (2007). "Mad city mystery: Developing scientific argumentation skills with a place-based augmented reality game on handheld computers". Journal of Science Education and Technology, 16(1), 5–29.

[17] Ternier, S., Klemke, R., Kalz, M., Ulzen, P. & Specht, M. (2012). "AR Learn: Augmented reality meets augmented virtuality". Journal of Universal Computer Science, 18(15), 2143–2164.

[18] Bressler, D. M. & Bodzin, A. M. (2013). "A mixed methods assessment of students ' flow experiences during a mobile augmented reality science game". Journal of Computer Assisted Learning, 29, 505–517.

[19] Sonia Mozaffari, Hamid Reza Hamidi, “Impacts of augmented reality on foreign language teaching: a case study of Persian language”, Multimedia Tools and Applications (2023) 82:4735–4748.

آموزش زبان خارجی با کمک فناوری واقعیت افزوده

سونیا مظفری [۱]، حمیدرضا حمیدی [۱]

[۱] گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه بین المللی امام خمینی(ره)
soniamozaffari@gmail.com ،hamidreza.hamidi@eng.ikiu.ac.ir

چکیده

بکارگیری فناوری اطلاعات در حوزه آموزش زبان خارجی بصورت ابزار کمکی بسیار مورد توجه است. در کلاس آموزش زبان خارجی، مکان تنها یک مفهوم انتزاعی است؛ جایی که در آن زبان از جامعه، فرهنگ و مکان‌هایی که در آنها مورد استفاده قرار می‌گیرد، جدا می‌شود. واقعیت افزوده فناوری است که در آن اجزای مجازی با محیط واقعی بصورت همزمان ترکیب شده و محتوای موردنیاز را نمایش می‌دهد. هدف ما در این پژوهش بررسی تأثیر واقعیت افزوده مبتنی بر مکان در آموزش زبان فارسی بعنوان یک زبان خارجی است. در این پژوهش پس از صحبت با اساتید حوزه آموزش زبان فارسی و بررسی پژوهش‌ها و کارهای مشابه به این نتیجه رسیدیم که برای آموزش زبان فارسی با استفاده از واقعیت افزوده کاری صورت نگرفته است. بنابراین طرح یک آزمایش انجام گرفت و سپس ارزیابی انجام شد. در ارزیابی از تعدادی زبان‌آموز استفاده شد. بازخوردهای زبان‌آموزان نشان می‌دهد که استفاده از واقعیت افزوده برای آموزش زبان فارسی باعث افزایش رضایتمندی، اشتیاق و تعامل با محیط و افراد می‌شود و همچنین فرآیند یادگیری و به‌خاطر سپاری مفاهیم را بهتر و مؤثرتر می‌کند.

کلمات کلیدی: واقعیت افزوده، آموزش زبان، زبان خارجی.

۱ مقدمه

واقعیت افزوده به کاربر این اجازه را می‌دهد که ترکیبی از محیط واقعی و مجازی را داشته باشد؛ در واقع اشیای مجازی با محیط واقعی ترکیب شده‌اند و همزمان با هم ارائه می‌شوند [۴]. هر سیستم واقعیت افزوده دارای سه ویژگی است [۴]: (۱) محیط واقعی و مجازی را ترکیب کند، (۲) در محیط واقعی به‌صورت تعاملی باشد و (۳) محتوا به‌صورت سه‌بعدی نمایش داده شود.

واقعیت افزوده به دو صورت مورد استفاده قرار می‌گیرد: واقعیت افزوده بر پایه‌ی عناصر دیداری[۱] و واقعیت افزوده بر پایه‌ی مکان[۲]. واقعیت افزوده بر پایه‌ی عناصر دیداری، خود به دو دسته تقسیم می‌شود.

[1] Vision-based Augmented Reality
[2] Location-aware Augmented Reality

دسته‌ی اول بر پایه‌ی نشانه[3]؛ محتوا به‌صورت نشانه یا برچسب دوبعدی ثبت می‌شود. سپس توسط یک دوربین این برچسب که حاوی اطلاعاتی است که در آن قرار دارد به‌صورت سه‌بعدی نمایش داده می‌شود. این نشانه‌ها می‌توانند روی دیوار، درون کتاب یا روی اشیا قرار بگیرند. دسته‌ی دوم بدون نشانه؛ که از برچسب استفاده نمی‌شود و هر جزئی از محیط واقعی می‌تواند برای فعال‌کردن اجزای مجازی استفاده شود [۵]. در واقعیت افزوده بر پایه‌ی مکان از حسگرهای تعیین مکان[4] که در دستگاه سیار (کامپیوتر لوحی یا گوشی تلفن همراه) وجود دارد، استفاده می‌شود. محتوای مجازی در یک موقعیت خاص قرار گرفته و سپس این عنصر می‌تواند توسط دوربین ردیابی و شناسایی شود و هنگامی‌که به آن مکان مورد نظر رسید، اطلاعات مورد نظر نمایش داده شوند [۶، ۷].

هنگامی‌که صحبت از استفاده از واقعیت افزوده می‌شود، بیشترین چیزی که به ذهن می‌رسد کاربرد آن در حوزه‌هایی مانند بازاریابی و سرگرمی است؛ درحالی‌که امروزه از آن در حوزه آموزش هم به‌طور گسترده استفاده می‌شود. تقریباً تمام پروژه‌های واقعیت افزوده هدف آموزش دارند حتی اگر خیلی مشخص نباشد [۹، ۱۰]. تحقیقات نشان داده است که واقعیت افزوده می‌تواند یک روش بسیار جذاب برای بهبود روش آموزشی مانند کیفیت نوشتن، مهارت‌های ریاضی و یادگیری زبان خارجی باشد [۹]. این فناوری می‌تواند مهارت‌هایی را در دانش‌آموزان تقویت نموده و رشد دهد. به‌عنوان مثال باعث می‌شود تا افراد تعامل بیشتری با محیط برقرار کنند و توانایی تفکر خلاقانه و حل مسئله‌ای داشته باشند [۱۰، ۱۱]. استفاده از واقعیت افزوده فقط مختص به یک مکان یا سطح آموزشی خاصی نیست بلکه از آن می‌توان در مقاطع مختلف از ابتدایی تا دانشگاه استفاده کرد. این فناوری به‌خوبی توانسته در برخی موارد درسی مثل علوم، ریاضی، زیست‌شناسی و... مورد استفاده قرار بگیرد؛ ولی استفاده از آن در آموزش زبان خیلی چشمگیر نبوده است [۱۱].

در کلاس‌های آموزش زبان خارجی، مکان تنها یک مفهوم انتزاعی است؛ جایی که در آن، زبان از جامعه، فرهنگ و مکان‌هایی که در آنها مورد استفاده قرار می‌گیرد، جدا می‌شود [۱۲]. در آموزش و یادگیری یک زبان خارجی، محیط[5] بسیار مهم است و می‌تواند تأثیر زیادی در فرآیند آموزش داشته باشد. وقتی زبان‌آموز در محیط قرار دارد و متناسب با آن محیط، کلمات، عبارات و جملات مرتبط را می‌بیند و با آنها تعامل برقرار می‌کند، فرآیند یادگیری سریعتر و ماندگاری آنها در ذهن بیشتر می‌شود [۱۱]. بنابراین یادگیری باید در محیط مرتبط با محتوای آموزشی انجام گیرد چون یک فرایند اجتماعی است که از طریق آن افراد جدید با مشارکت در فعالیت‌های روزانه یاد می‌گیرند که عضوی از یک جامعه فعال باشند [۱۳].

پژوهش‌ها نشان می‌دهند که برای یادگیری و آموزش زبان خارجی، روشی مناسب است که چند ویژگی را داشته باشد: به‌صورت تعاملی باشد، جنبه‌های احساسی و ادراکی را در آموزش در نظر بگیرد، از ابزارهای مختلفی برای آموزش استفاده کند، مهارت‌های مختلفی مثل تفکر انتقادی و حل مسئله را افزایش دهد، چالش‌برانگیز باشد، به زبان‌آموزان انگیزه مشارکت در فرآیند آموزش و یادگیری را بدهد، سرگرم‌کننده باشد و موجب رشد و پیشرفت روانی زبان‌آموز شود [۲، ۳، ۸].

[3] Marker-based
[4] Geographical Positioning Sensors (GPS)
[5] Context

در این پژوهش تلاش شد تا تأثیر به‌کارگیری فناوری واقعیت افزوده برای آموزش زبان فارسی به زبان‌آموزان خارجی مورد ارزیابی قرار گیرد. ابتدا مروری از پژوهش‌های مشابه در حوزه آموزش زبان خارجی مبتنی بر واقعیت افزوده ارائه می‌کنیم. سپس یک بازی مبتنی بر واقعیت افزوده که برای این پژوهش طراحی و تولید شده است را معرفی نموده و سپس آن را مورد ارزیابی قرار می‌دهیم.

۲ به‌کارگیری واقعیت افزوده در آموزش زبان خارجی

ما نتوانستیم هیچ پژوهشی درخصوص به‌کارگیری واقعیت افزوده در آموزش زبان فارسی بیابیم. اما پژوهش‌های متعددی در آموزش زبان‌های دیگر انجام گرفته است. در ادامه مروری از این پژوهش‌ها بسته به نوع واقعیت افزوده استفاده شده، ارائه می‌کنیم.

۱.۲ واقعیت افزوده بر پایه نشانه

اَمَر[۶] و همکارانش از واقعیت افزوده برای آموزش زبان انگلیسی به کودکان استفاده کردند و سعی در بررسی مؤثربودن این روش داشتند [۶]. این تحقیق عملی در مهد کودکی در کویت صورت گرفت که در آن از ۴۲ کودک که به‌صورت تصادفی انتخاب شده بودند، استفاده شد. افراد به دو دسته که یکی از دسته‌ها از روش سنتی و دسته‌ی دیگر از واقعیت افزوده استفاده می‌کردند، تقسیم شدند. بعد از استفاده از این برنامه‌ها، به بررسی میزان تأثیرگذاری واقعیت افزوده برای ارائه محتوای علمی و تعامل دانش‌آموزان و همین‌طور میزان یادگیری آنها از الفبای انگلیسی پرداختند. در ادامه به این نتیجه رسیدند که گروهی که در آن از واقعیت افزوده استفاده شده بود نسبت به گروه دیگر، سطح تعامل و میزان یادگیری حروف و کلمات انگلیسی بسیار بالاتری داشته‌اند [۶].

سنتوس[۷] و همکارانش از واقعیت افزوده بر اساس علامت برای آموزش کلمات زبان آلمانی و فیلیپینی استفاده کردند [۱۴]. در این مطالعه دو روش یادگیری با واقعیت افزوده و بدون واقعیت افزوده را مقایسه کردند. برای آزمایش یادگیری زبان فیلیپینی، آن‌ها از ۳۱ شرکت‌کننده استفاده کردند که شامل ۲۶ مرد و ۵ زن بین سن‌های ۲۳ تا ۴۲ سال بودند و همین‌طور برای آموزش زبان آلمانی از ۱۴ شرکت‌کننده که ۸ نفر آنها مرد و ۶ نفر زن در رده سنی ۱۶ تا ۲۰ سال بودند، استفاده شد. این آزمایش طی ۵ روز انجام شد. بعد از فرآیند یادگیری، شرکت‌کنندگان به سؤالات که در قالب پرسش‌نامه مطرح شده بود، پاسخ دادند. بعد از بررسی پاسخ‌ها به این نتیجه رسیدند که استفاده از واقعیت افزوده می‌تواند نتایجی از قبیل تفاوت در تجربه یادگیری، بهبود توجه و افزایش حس رضایت را داشته باشد [۱۴].

بژورکوئز[۸] و همکارانش، برنامه کاربردی لوتریا[۹] را برای آموزش زبان مایو[۱۰] (مالزی) و بر اساس تصاویر و

[6] Ammar
[7] Santose
[8] Bojorquez
[9] Loteria
[10] Mayo

صداهایی که از واقعیت افزوده و کارت‌هایی با تصاویر مختلف استفاده می‌کنند، طراحی کردند. این برنامه در محیط دانشگاه و توسط تعدادی از دانشجویان کارشناسی به‌کار گرفته شد و از نظر سهولت استفاده از آن، مفیدبودن آن و تمایل به اجرای آن، مورد آزمایش قرار گرفت که نتایج خوبی را به همراه داشت [۱۵].

لیو[11] و همکارانش برنامه کاربردی به نام هِللو[12] را برای آموزش زبان انگلیسی به دانشجویان تایوانی طراحی کرده‌اند [۱۶]. برای ارزیابی مؤثربودن و کاربرپسندبودن بازی، پرسش‌نامه‌ای به ۲۰ دانشجو که بازی را انجام داده بودند، داده شد که هرکدام از سؤالات آن ۷ گزینه داشت؛ ۱ مخالفت کامل تا ۷ موافقت کامل. در نتیجه بیشتر دانشجویان بر این اعتقاد بودند که هِللو برای یادگیری زبان بسیار مؤثر است، کار با آن ساده است و همین‌طور باعث افزایش اشتیاق آنها به یادگیری می‌شود؛ به‌طوری‌که بیشتر آنها می‌خواستند تا از هِللو در ساعات غیر از دانشگاه نیز استفاده کنند. آنها معتقد بودند که این بازی مهارت‌های خواندن، گوش‌کردن و صحبت‌کردن را تقویت می‌کند اما روی مهارت نوشتن آنها تأثیری ندارد [۱۶].

هدید[13] و همکارانش از واقعیت افزوده برای آموزش زبان انگلیسی در کلاس درس استفاده کرده‌اند [۱۷]. این نرم‌افزار ریدربادی[14] نام دارد که از کُد کیو. آر. استفاده می‌کند. این کُدها در صفحات مختلف کتاب قرار داده می‌شود و هنگامی‌که دانش‌آموز تلفن همراه خود را به سمت آن بگیرد، تصویر، تلفظ و فیلمی در مورد آن کلمه نمایش داده می‌شود. این نرم‌افزار بیشتر برای کتاب‌های علمی طراحی شده است [۱۷].

جدول ۱ ، جمع‌بندی این پژوهش‌ها را نشان می‌دهد.

جدول ۱: جمع‌بندی پژوهش‌های آموزش زبان خارجی با واقعیت افزوده‌ی مبتنی بر نشانه.

نام برنامه/ پژوهشگر	زبان مورد آموزش	جامعه آماری
اَمَر و همکارانش	زبان انگلیسی	کودکان
سنتوس و همکارانش	کلمات زبان آلمانی و فیلیپینی	۲۳ تا ۴۲ و ۱۶ تا ۲۰ سال
لوتریا	آموزش کلمات به زبان مایو (مالزی)	دانشجویان
هللو	تمام مهارت‌های زبان انگلیسی	دانشجویان
هدید و همکارانش	کلمات زبان انگلیسی	–

۲.۲ واقعیت افزوده بر پایه‌ی مکان

منتیرا[15] اولین بازی سیار واقعیت افزوده بر پایه‌ی مکان است که برای توسعه مهارت‌های زبان اسپانیایی طراحی شد [۱۲]. این بازی رمز و راز یک قتل است که متشکل از حوادث داستانی جاری و منحصر به فرد می‌باشد. بازیکن در محیط واقعی و از طریق تعامل با شخصیت‌های بازی به دنبال حل معمایی است. ساختار اصلی بازی، مکالمات بین بازیکن و شخصیت‌های داستانی مربوط به قتل و راه‌حل آن است. نتایج ارزیابی بازی روی دانشجویان جهت تعامل با محیط و افزایش اشتیاق زبان‌آموزان رضایت‌بخش بوده است [۱۲].

[11] Liu
[12] HELLO (the Handheld English Language Learning Organization)
[13] Hadid
[14] Reader Buddy
[15] Mentira

پوکمون گو[16] بازی‌ای است که در سال ۲۰۱۶ معرفی شد و برای آموزش زبان انگلیسی مورد استفاده قرار می‌گیرد [۱۷، ۱۸]. این بازی باعث شد تا افراد تحرک بیشتری داشته باشند و دقت و تمرکز آنها روی محیط بیشتر شود و اضطراب آنها کاهش یابد [۹].

ویلسن و بریک[17] از تیل بلیزر[18] برای آموزش زبان ایتالیایی در محیط دانشگاه، توسط دانشجویان با سطح ابتدایی زبان ایتالیایی استفاده کردند. دانشجویان در این بازی سعی در حل‌کردن یک مسئله رمزآلود سفر در زمان دارند. این بازی سعی در آموزش هم‌زمان هر ۴ مهارت گوش‌کردن، خواندن، نوشتن و صحبت‌کردن دارد [۱۹].

برنادت پری[19] برنامه کاربردی اکسپلورز[20] را برای آموزش زبان فرانسه برای دانشجویان سال اول دانشگاه ویکتوریا[21] در فرانسه طراحی کرد. با استفاده از سامانه اطلاعات جغرافیایی (جی. پی. اِس)، اکسپلورز، دانشگاه ویکتوریا را به یک دنیای مجازی فرانسوی تبدیل می‌کند که در آن، دانش‌آموزان با شخصیت‌ها، عناصر و رسانه‌ها ارتباط برقرار می‌کنند تا مهارت‌های زبان فرانسه خود را بهبود بخشند و دانشگاه خود را کشف کنند. این برنامه کاربردی به دانش‌آموزان این امکان را می‌دهد تا مهارت‌های ورودی و خروجی زبان به هر دو صورت نوشتاری و گفتاری را بهبود بخشند. این برنامه از سه سطح تشکیل شده که در هر سطح حداقل ۳ سؤال مطرح می‌شود. مأموریت‌ها شامل چالش‌هایی مانند گرفتن عکس از اشیای مشخص‌شده، جمع‌آوری اشیای مجازی و کاوش مکان‌ها در نقشه می‌شوند. این برنامه کاربردی از طریق پرسش‌نامه‌هایی که بین بازیکنان تقسیم شده بود، مورد بررسی قرار گرفت و بیشتر آنها این بازی را آموزنده، سرگرم‌کننده و مفید می‌دانستند [۲۰].

جمع‌بندی پژوهش‌های مربوط به آموزش زبان خارجی با استفاده از واقعیت افزوده‌ی مبتنی بر مکان در جدول ۲ ارائه شده است.

جدول ۲: جمع‌بندی پژوهش‌های آموزش زبان خارجی با واقعیت افزوده‌ی مبتنی بر مکان.

نام برنامه/ پژوهشگر	زبان مورد آموزش	جامعه آماری
منتیرا	مهارت صحبت‌کردن به زبان اسپانیایی	دانشجویان
پوکمون گو	زبان انگلیسی	دانشجویان
تیل بلیزر	تمام مهارت‌های زبان ایتالیایی	دانشجویان
اکسپلورز	مهارت نوشتاری و گفتاری زبان فرانسه	دانشجویان

بعد از بررسی پژوهش‌های متفاوت به نتیجه رسیدیم که برای آموزش زبان خارجی از واقعیت افزوده استفاده شده است؛ اما در آموزش زبان فارسی پژوهشی انجام نشده است. در حوزه آموزش زبان فارسی

[16] Pokemon go
[17] Wilson and Brick
[18] Tale Blazer
[19] Bernadette Perry
[20] Explorez
[21] Victoria

برای زبان‌آموزان خارجی یکی از مشکلات اصلی یادگیری، فاصله مطالب آموزشی با محیط واقعی است [۲۱]. تحقیقات مرتبط نشان داده است که واقعیت افزوده می‌تواند کمک کند تا این فاصله کمتر گردد.

۳ آزمون طراحی‌شده

در این پژوهش، یک بازی کامپیوتری قابل اجرا روی کامپیوترهای سیار (اندروید) بنام پارسی‌شو طراحی شد. هدف اصلی، افزایش اشتیاق زبان آموزان و افزایش تعامل با محیط است.

داستان مورد نظر بازی را با کمک اساتید آموزش زبان فارسی طراحی و پیاده‌سازی کردیم. محیط تعاملی، محوطه دانشگاه بین‌المللی امام خمینی(ره) است که زبان‌آموزان مرکز آموزش زبان فارسی، لازم است در دوره آموزشی زبان با آن در تعامل باشند. در این سناریو، سعی شد تا حد مطلوبی به تمام مهارت‌های خواندن، صحبت‌کردن، گوش‌کردن و نوشتن پرداخته شود. همچنین، سعی شد تا افراد بتوانند با محیط خود و حتی افرادی که در آن محیط حضور دارند تعامل برقرار کنند و دید بهتری نسبت به محیط پیدا کنند.

بازی پارسی‌شو از دوازده مرحله تشکیل شده است که سعی شده تا در هر مرحله، به مکان‌های پررفت‌وآمدی که دانشجویان با آنها سروکار دارند، بپردازیم. در هر مرحله، زبان‌آموزان باید به سؤالاتی در آن مرحله مطرح می‌شود پاسخ دهند و جواب مورد نظر را در مکان مربوط به آن بنویسند که این قسمت برای یادگیری و تمرین صحیح‌نوشتن کلمات توسط زبان‌آموزان طراحی شده است.

بازی به‌صورت مرحله به مرحله انجام می‌گیرد و پس از پایان هر مرحله، برای یافتن مرحله بعدی، راهنماهایی در داخل بازی طراحی شده است. این راهنمایی یا به‌صورت واضح محل بعدی را به‌صورت متن نمایش می‌دهد که این قسمت از برنامه به هدف تمرین خواندن کمک می‌کند و یا به‌صورت سؤال مطرح می‌شود تا زبان‌آموز با توجه به اطلاعات داده‌شده و با مراجعه به اطلاعات قبلی خود و یا صحبت و پرس‌وجو با افراد حاضر در محیط، مرحله بعدی را کشف کند.

در هر مرحله، زبان‌آموز با فعل‌های پرکاربردی که در آن مکان مورد استفاده قرار می‌گیرد و همچنین با تلفظ و دیکته آشنا می‌شود که این قسمت‌ها به هدف تمرین شنیدن و به‌خاطرسپاری بهتر کلمات مرتبط به هر محیط طراحی شده است. همچنین در برخی مراحل، افعال در قالب یک جمله و یا یک عبارت که به‌صورت نوشتاری و یا به‌صورت صدای ضبط‌شده است، معرفی می‌شوند. به‌عنوان‌مثال در مکان کافه، زبان‌آموزان با تصویر، تلفظ و دیکته‌ی مربوط به هر کلمه آشنا می‌شوند. همچنین در این مرحله، مکالمه‌ای پخش می‌شود تا زبان‌آموزان با نحوه ادای کلمات به‌صورت محاوره‌ای آشنا شده و مهارت گوش‌کردن را نیز تمرین کنند. در این بازی سعی شده تا زبان‌آموز با برخی فرهنگ‌ها و جاذبه‌های ایران آشنا شود که یکی از آن مکان‌ها مسجد است[۲۲].

[۲۲] شرح جزئیات بازی و راهنمای کار با آن در پایان‌نامه‌ی کارشناسی‌ارشد با عنوان «استفاده از واقعیت افزوده برای یادگیری زبان خارجی، موردمطالعه: زبان فارسی» در دانشگاه بین‌المللی امام خمینی (ره) ثبت شده است.

۴ ارزیابی عملی

برای ارزیابی تأثیر بازی طراحی‌شده در آموزش زبان، به طور معمول باید از ارزیابی زبان‌آموزان بهره ببریم. حداقل تعداد ۱۵ زبان‌آموز برای ارزیابی لازم است [۲۸]. به‌دلیل وجود بیماری کووید ۱۹ و تمام محدودیت‌هایی که به‌خاطر این بیماری به‌وجود آمد، سعی کردیم تا از روشی دیگر برای ارزیابی نتایج استفاده کنیم که مؤثر، کاربردی و قابل استناد باشد. یک مطالعه کاربری انجام دادیم که از تعداد اندکی زبان‌آموز بهره بردیم. تعداد کم کاربر موجب می‌شود که ارزیابی از دقت مناسب برخوردار نباشد.

در ارزیابی کاربر از تعداد اندک زبان‌آموزان خواسته شد تا برنامه را در محیط دانشگاه بین‌المللی امام خمینی(ره) به‌کار بگیرند و سپس بر اساس نظرات و سؤالات مطرح‌شده در پرسش‌نامه، برنامه‌ی موردنظر را ارزیابی کنند. برای این منظور از تعداد محدود ۳ زبان‌آموز غیرایرانی استفاده گردید که دانش آنها از زبان فارسی در سطح متوسط بود. در ابتدا، نحوه انجام بازی به طور کامل برای آنها شرح داده شد و سپس هرکدام با توجه به مراحلی که در بازی در نظر گرفته شده بود به‌صورت جداگانه اقدام به انجام بازی کردند. بعد از به پایان رساندن بازی، با در اختیار داشتن پرسش‌نامه، برنامه را مورد ارزیابی قرار دادند و نظرات خود را در مورد بازی بیان کردند. هرچند تعداد اندک کاربران موجب می‌شود تا نتایج اعتبار آماری مناسب را نداشته باشند؛ ولی امکان‌پذیری و قابلیت اجرایی بازی در محیط واقعی و با کاربر هدف سنجیده شده است.

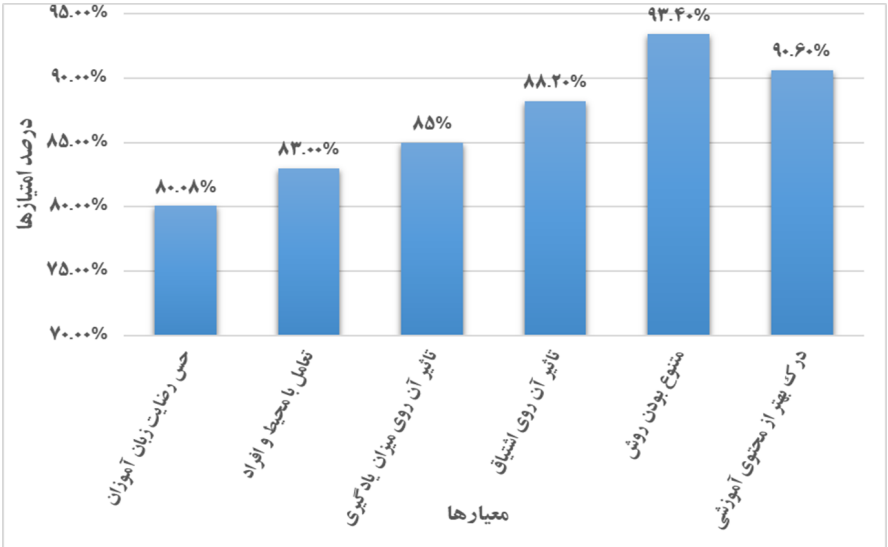
معیارهای مورداستفاده در این پژوهش، با توجه به پژوهش‌های مشابه، استخراج و خلاصه شده‌اند و سپس در طراحی پرسش‌نامه‌ی مربوط به زبان‌آموزان به‌کار رفتند. این معیارها عبارت‌اند از [۹، ۱۴، ۱۵، ۲۰، ۳۰، ۳۱]:

۱. حس رضایتمندی زبان‌آموزان
۲. تعامل با محیط و افراد
۳. تأثیر آن روی میزان یادگیری
۴. تأثیر آن روی اشتیاق به یادگیری
۵. متنوع‌بودن روش‌ها
۶. درک بهتر از محتوای آموزشی

برای ارزیابی بازی، ابتدا توضیحاتی در مورد بازی و نحوه انجام آن به ارزیاب‌ها داده شد و آنها با توجه به عبارات درنظرگرفته‌شده در پرسش‌نامه، برنامه را ارزیابی نمودند. پرسش‌نامه‌ها به این صورت طراحی شده‌اند که زبان‌آموزان برای پاسخ به هر عبارت، ۵ انتخاب دارند که عبارت‌اند از کاملاً موافق، موافق، نظری ندارم، مخالف و کاملاً مخالف. برای امتیازدهی از مقیاس لیکرت[۲۳] (۵ کاملاً موافق، ۴ موافق، ۳ نظری ندارم، ۲ مخالف و ۱ کاملاً مخالف) استفاده شد.

[23] Likert

شکل ۱ نتایج ارزیابی کاربران را نشان می‌دهد.



شکل ۱: نتایج ارزیابی کاربران

در مورد معیار احساس رضایت، هر ۳ زبان‌آموز با این عبارات موافق بودند و فقط یکی از زبان‌آموزان معتقد بود که استفاده از این برنامه کمی برای او مشکل بوده و بر این باور بود که برنامه باید به‌صورت ساده‌تر و گویاتر طراحی می‌شد. زبان‌آموزان بر این عقیده بودند که استفاده از این برنامه باعث شد تا با دقت بیشتری به محیط اطراف توجه کنند و همچنین باعث شد تا برای یافتن مکان بعدی و پاسخ به سؤالات مطرح‌شده در بازی، با افراد مختلف تعامل داشته باشند که این نشان‌دهنده‌ی تأثیرگذاری بر افزایش تعامل آنها با محیط و افراد است. درعین‌حال زبان‌آموزان معتقد بودند که راهنمایی‌های داخل بازی، جهت برقراری ارتباط با افراد و محیط می‌تواند واضح‌تر بیان گردد.

طبق بررسی‌های انجام‌شده بر اساس پاسخ زبان‌آموزان، امتیاز معیار تأثیر بر میزان یادگیری ۸۵ درصد است. دراین‌خصوص زبان‌آموزان معتقد بودند که چون از عناصر مختلف آموزشی مانند صدا، تصویر و متن در این بازی استفاده شده است، یادگیری مفاهیم راحت‌تر و مؤثرتر شده است. زبان‌آموزان بسیار مشتاق بودند تا از این بازی به‌منظور یادگیری زبان فارسی در مکان‌های دیگر نیز استفاده کنند. همچنین معتقد بودند که یادگیری زبان فارسی با این روش بسیار جذاب است و باعث می‌شود تا با اشتیاق بیشتری فرایند یادگیری طی شود.

معیار متنوع‌بودن با ۹۳.۴ درصد بالاترین امتیاز را بین معیارهای دیگر کسب کرده است. طبق نظرهای ارائه‌شده توسط زبان‌آموزان، دلیل آن، استفاده از محتواهای مختلف آموزشی در مکان‌های مختلف، تحرک بیشتر و دقت به محیط اطراف است که باعث خستگی ناشی از یکنواخت‌بودن فضای آموزشی نمی‌شود. معیار درک بهتر از محتوای آموزشی نیز با کسب امتیاز ۹۰.۶ درصدی دومین معیار با امتیاز بالا محسوب

می‌شود. زبان‌آموزان بر این عقیده بودند که ارتباط محتوای استفاده‌شده در بازی، با محیطی که آن محتوا آموزش داده می‌شود، تأثیر خیلی زیادی روی فهم و درک مفاهیمی که یاد می‌گیرند دارد.

۵ جمع‌بندی

با ارزیابی انجام‌شده در این پژوهش، به این نتیجه رسیدیم که استفاده از واقعیت افزوده، می‌تواند یک گام خیلی مؤثر در آموزش زبان فارسی باشد. همچنین بر اساس نظر زبان‌آموزان، استفاده از برنامه‌های مبتنی بر واقعیت افزوده، به‌دلیل به‌کاربردن عناصر مختلفی مانند صدا، تصویر و متن به‌صورت هم‌زمان در محیط واقعی، باعث درک بهتر مفاهیم آموزشی شده و در نتیجه، فرآیند یادگیری و به‌خاطرسپاری آن مفاهیم را بهتر و مؤثرتر می‌کند. بر اساس نظر برخی از کارشناسان، استفاده از عناصر بازی‌نمایی مانند امتیاز باعث ایجاد انگیزه و اشتیاق بیشتر برای یادگیری می‌شود. استفاده از مکان‌های مختلف در طراحی برنامه، باعث تحرک بیشتر و کشف محیط اطراف شده و در نتیجه، این امر باعث شادابی و عدم خستگی ناشی از یکنواخت‌بودن محیط می‌شود. طبق نظر زبان‌آموزان و کارشناسان، چون در این برنامه افراد باید با محیط و افراد مختلف جهت یافتن محل بعدی یا پیداکردن پاسخ سؤالات، ارتباط مؤثر و درست برقرار کنند، پس این ویژگی باعث افزایش تعامل زبان‌آموزان با محیط اطراف و افراد حاضر در محیط می‌شود.

مراجع

[۱] م. ریاحی چلوانی، «تهیه متون فرهنگی خواندن برای سطح متوسط فارسی‌آموزان غیرفارسی‌زبان»، ۱۳۹۳.

[۲] حمیدرضا مقامی، مریم رجبیان دهزیره، سکینه شریفاتی، «تأثیر چندرسانه‌ای آموزشی مبتنی بر الگوی آشور بر جو انگیزشی درک شده و بهزیستی ذهنی دانشجویان»، راهبردهای شناختی در یادگیری، دوره ۸، شماره ۱۵، پاییز و زمستان ۱۳۹۹.

[۳] شراره السادات میرصفدری، یعقوب محمدی فر، «نقش رسانه‌های مجازی دیجیتال در آموزش مفاهیم شناختی میراث فرهنگی به کودکان»، راهبردهای شناختی در یادگیری، دوره ۹، شماره ۱۶، بهار و تابستان ۱۴۰۰.

[4] Azuma, R. T. (1997), ‘A survey of augmented reality’, pp.2-9.

[5] Khoshnevisan, B., Nhu, L. (2019), ‘Augmented Reality in Language Education: A Systematic Literature Review’, Conference Paper, pp.2.

[6] Ammar H. S., Al-Jafar, A. A. and Al-Yousefi, Z. H., (2016), ‘ The Effectiveness of Using Augmented Reality Apps in Teaching the English Alphabet to Kindergarten Children: A Case Study in the State of Kuwait’, EURASIA Journal of Mathematics Science and Technology Education 2017 13(2) DOI 10.12973/eurasia.2017.00624a.

[7] Godwin-Jones, R. (2016), ‘Augmented reality and language learning: From annotated vocabulary to place-based mobile games’, Language Learning & Technology 20(3), pp. 9–19. Retrieved from http://llt.msu.edu/issues/october2016/emerging.

[8] Fauziati, E. (2017) ‘From traditional to scientific approach: the changing winds and shifting sands of foreign language teaching method’, pp.1-7, Eltic conference, Vol 2, No 01 (2017).

[9] Geroimenko, V. (2020), 'Augmented Reality in Education: A New Technology for Teaching and Learning', ISSN 2195-9056 ISSN 2195-9064 (electronic) Springer Series on Cultural Computing ISBN 978-3-030-42155-7 ISBN 978-3-030-42156-4 (eBook) https://doi.org/10.1007/978-3-030-42156-4.

[10] Wu, H.-K. Lee, S. W.-Y. Chang, H.-Y. and Liang, J.-C. (2012), 'Current status, opportunities and challenges of augmented reality in education. Computers and Education', Received 27 January 2012, Computers & Education 62 (2013), pp. 41–49.

[11] Scrivner O., Madewell J. and Buckley, C. (2016), 'Augmented Reality Digital Technologies (ARDT) for Foreign Language Teaching and Learning'.

[12] Holden, C. L. and Sykes, J. M. (2011), 'Leveraging Mobile Games for Place-based Language Learning', International Journal of Game-Based Learning, v1 n2 p1-18 2011, DOI: 10.4018/ijgbl.2011040101.

[13] Collins, A., Brown, J., & Newman, S. (1988), 'Cognitive apprenticeship thinking. Thinking', The Journal of Philosophy for Children, 8(1), pp. 2–10. doi:10.5840/ thinking19888129

[14] Santos, M. E., Lübke, A.W., Taketomi, T., Yamamoto, G., Rodrigo M. M. T., Sandor, C. and Kato, K. (2016), 'Augmented reality as multimedia: the case for situated vocabulary learning', pp.1-10, Research and practice in technology enhanced learning a springer open journal, DOI 10.1186/s41039-016-0028-2.

[15] Bojorquez, E. M. Villegas, O. V. Sanchez, V. G. C. Garcia-Alcaraz, J. L. and Vara, J. F., (2016), 'Study on mobile augmented reality adoption for Mayo language learning', Received 20 April 2016, http://dx.doi.org/10.1155/2016/1069581.

[16] Liu, T. -Y. Tan, T. -H. and Chu, Y. -L. (2021), 'QR Code and Augmented Reality-Supported Mobile English Learning System', © Springer-Verlag Berlin Heidelberg.

[17] Hadid, A. Mannion, P. Khoshnevisan, B. (2022), 'Augmented Reality to the Rescue of Language Learners', Florida Journal of Educational Research, Volume 57, Issue 2. pp.3-9.

[18] Akcay, M. Akçayır, G. (2020), 'Advantages and challenges associated with augmented reality for education: A systematic review of the literature'.

[19] Cervi-Wilson, T., and Brick, B. (2018), ' ImparApp: Italian language learning with MIT's TaleBlazer mobile app. In F. Rosell-Aguilar, T. Beaven, & M. Fuertes Gutiérrez (Eds), Innovative language teaching and learning at university: integrating informal learning into formal language education (pp. 49-58). Research-publishing.net. https://doi.org/10.14705/rpnet.2018.22.775.

[20] Bernadette Perry (2015), 'Gamifying French Language Learning: a case study examining a quest-based, augmented reality mobile learning-tool', Procedia - Social and Behavioral Sciences 174 (2015) 2308 – 2315, pp. 2-8, doi: 10.1016/j.sbspro.2015.01.892.

[21] Chapelle, C. (1997), ' CALL in the Year 2000: Still in Search of Research Paradigms?', Language Learning & Technology Vol. 1, No. 1, July 1997, pp. 19-43.

[22] Savitri, A.S. (2023), ‘ The use of language games to improve the students’ speaking ability of class vii A of SMP MA’ARIF TERPADU MUNTILAN in the academic year of 2012/2013’. pp. 3-10. Master thesis,Yogykarta State University.

[23] Javadi-Safa, A. (2018), ‘A Brief Overview of Key Issues in Second Language Writing Teaching and Research’, International Journal of Education & Literacy Studies, pp.1-3, ISSN: 2202-9478, www.ijels.aiac.org.au.

[24] Rao, P.S. (2019), ‘Teaching of Writing Skills to Foreign or Second Language Learners of English’, ELT Vibes: International E-Journal For Research in ELT. 5(2). 136-152, pp.2-8.

[25] Yurko N.A., Styfanishyn I.M. (2020), ‘Listening skills in learning a language: the importance, benefits, and means of enhancement’, DOI 10.36074/rodmmrfssn.ed-1.04.

[26] Walker, N. (2020), ‘Listening: the most difficult skill to teach’, Encuentro 23, 2014, ISSN 1989-0796, pp. 2-3.

[27] Nielsen, J. Molich, R. (1990), ‘ Heuristic evaluation of user interfaces’, CHI 90 Proceedings.

[28] Wilson, C. (2014) ‘Heuristic Evaluation’, https://doi.org/10.1016/B978-0-12-410391-7.00001-4.

[29] Tuli N. Mantri, A. (2019), ‘Usability Principles for Augmented Reality based Kindergarten Applications’, 9th World Engineering Education Forum, WEEF 2019. pp.3-7. Procedia Computer Science 172 (2020) 679–687.

[30] Freitas, R. Campos, P. (2008), ‘SMART: a System of Augmented Reality for Teaching 2nd Grade Students’, Published by the British Computer Society.

[31] Ko, S. M. Chang, W. C. and Ji, Y. G. (2013), ‘Usability Principles for Augmented Reality Applications in a Smartphone Environment’, International Journal of Human Computer Interaction, 29:8, 501-515, pp.4-8, DOI: 10.1080/10447318.2012.722466.

بررسی تأثیر فناوری متاورس بر دگرگونی سنت روابط سیاسی کشورهای حاضر در ساختار نظام بین‌الملل

امید نوری[۱]، محمد لعل علیزاده[۲]

[۱] کارشناسی ارشد علوم سیاسی، دانشگاه پیام نور، تهران
[۲] استادیار گروه علوم سیاسی، دانشگاه پیام نور، تهران
m.lalalizadeh@pnu.ac.ir

چکیده

امروزه با وجود فناوری‌های مختلف به‌عنوان ابزارهای مؤثر بر کمک و ارتقاء همه‌جانبه زندگی انسان‌ها، به‌طور مداوم شاهد پدیدار گشتن فناوری‌های ارتقاءیافته‌تر و بهینه‌تر هستیم. در حوزه فناوری‌های اطلاعاتی و ارتباطی، آخرین تحولی که صورت گرفته ظهور فناوری متاورس است؛ متاورس با دارا بودن ماهیت منحصربه‌فرد خود می‌تواند دگرگونی‌های متعددی را در حوزه‌های مختلف برای جوامع و روابط بین آن‌ها رغم زند که این پژوهش ارتباط بین این فناوری و نحوه اثرگذاری آن بر روابط سنتی شکل‌گرفته بین‌المللی را بررسی کرده است. ضمن بررسی مهم‌ترین یافته‌ها از منابع کتابخانه‌ای، به مطالعه نظرات و افکار اندیشمندان و متفکران در حوزه فناوری متاورس و روابط بین‌الملل پرداخته شد. نتیجه یافته‌های تحقیق نشان داد ارتباط و تأثیرگذاری قابل‌توجهی بین فناوری متاورس و روابط سنتی شکل‌گرفته بین کشورها در ساختار بین‌الملل وجود دارد. بنابراین فناوری مذکور علاوه بر ویژگی ذاتی و خاص خود، نشان داد که با رویکرد صحیح کشورها و سازمان‌های بین‌المللی، توانایی دگرگونی سازی قابل‌ملاحظه‌ای در حوزه‌های مختلف اقتصادی، سیاسی، فرهنگی، اجتماعی در بین کشورها را دارد و نقطه عطفی در روابط جاری بین کشورها تلقی می‌شود.

کلمات کلیدی: پیشرفت، دگرگونی روابط، فناوری متاورس، قدرت سیاسی، کشورهای توسعه‌نیافته و توسعه‌یافته، نظام بین‌الملل.

۱ مقدمه

با شروع انقلاب فناوری که منجر به پیدایش ابزارهای مختلف و متنوعی همچون ماهواره‌ها، تلفن همراه، اینترنت و علوم جدید اطلاعاتی و ارتباطی گردیده، روابط انسانی نیز به‌تبع آن دچار دگرگونی‌هایی شده است. امروزه دیگر زندگی بدون این فناوری‌ها عملاً غیرممکن است. تغییر بر روابط انسانی باعث می‌شود کشورها نیز از آن تأثیر پذیرفته و خود را با شرایط به وجود آمده منطبق سازند. کشورها با حفظ و استفاده از این فناوری‌ها سعی در رشد و توسعه و قدرت اقتصادی، سیاسی، فرهنگی سرزمین خود و رقابت و برتری با سایر

رقبای خود در سطح بین‌الملل هستند. یکی از فناوری‌های نوظهوری که اخیراً پدیدار گشته و مورد تحقیق و پژوهش قرار خواهد گرفت، «فناوری متاورس» است. متاورس عمدتاً بر پایه حذف فضا و مکان خلق شده است. با به‌کارگیری از آن افراد در سراسر جهان می‌توانند با یکدیگر به تعامل و ارتباط بپردازند. این فناوری با دگرگون‌سازی روابط انسانی، نقطه آغاز شکاف بین مرزبندی سیاسی، فرهنگی، اقتصادی و ... بین کشورهای موجود در جوامع بین‌الملل است. طبق آمارها و نظرسنجی‌های صورت‌گرفته، به طور روزانه بر میزان استقبال، علاقه‌مندی و محبوبیت نسبت به استفاده از این فناوری افزوده می‌گردد. بر اساس این آمارها، تعداد کاربران حوزه متاورس از ابتدای سال ۲۰۲۰ تا ژوئن ۲۰۲۱ ده برابر شده است و پیش‌بینی می‌شود تا سال ۲۰۲۶ حدود ۲۵ درصد از مردم سراسر دنیا در این فضا حضور داشته باشند. عطف به مباحث فوق، مسئله اصلی و پیشرو این است که با شروع فناوری متاورس نظم سنتی شکل‌گرفته در ساختار بین‌الملل، متأثر و دچار دگرگونی می‌شود و عکس‌العمل و راهکارهای کشورها، سازمان‌ها و نهادهای بین‌المللی در جهت مقابله یا درک و پذیرش این فناوری، دچار چالش و آزمون جدی قرار خواهد گرفت.

با توجه به نوظهور بودن فناوری متاورس، تاکنون پژوهش و یافته‌های بسیار اندکی در این زمینه وجود دارد. احمد سلطانی نژاد، محسن اسلامی و محمد زمان راست‌گو در مقاله‌ی خود با نام «فناوری اطلاعات و ارتباطات پیشرفته و تحول مفهوم حاکمیت در روابط بین‌الملل» بهار ۱۳۹۵؛ تأثیر این فناوری را بر تحول مفهومی حاکمیت مورد بررسی قرار داده. ضمن تبیین و توضیح مفهومی حاکمیت، به عصر اطلاعات می‌رسد و فرضیه خود را این‌گونه بیان می‌سازد که فناوری اطلاعات و ارتباطات پیشرفته با دسترسی آزاد و گسترده افراد به اطلاعات و افزایش آگاهی و با کاهش هزینه‌های پردازش و ... زمینه بروز کنشگران جدید را فراهم ساخته است. محمد برجعلی‌زاده، علی جعفری و ناهید کردی در مقاله‌ای دیگر تحت عنوان «نقش فناوری‌های نوین ارتباطی در گسترش دیپلماسی در عرصه بین‌الملل» بهار ۱۴۰۰ که در فصلنامه پژوهش‌های ارتباطی انتشاریافته، به بررسی عنوان پژوهش خود می‌پردازند؛ ایشان با اشاره به نقش مهم فناوری‌های نوین در گسترش دیپلماسی در عرصه بین‌الملل، با گردآوری اطلاعات از طریق پرسش‌نامه و جامعه آماری که مدنظر بوده به این نتیجه می‌رسند که فناوری‌های نوین ارتباطی از طریق فضای مجازی و واقعیت مجازی، شبکه‌های اجتماعی، ماهواره و ... بر گسترش دیپلماسی در عرصه بین‌الملل تأثیرگذارند. ملودنا استیونز[1] در مقاله‌ی لاتین خود تحت عنوان "متاورس و حاکمیت آن"۲۰۲۲؛ اعلام می‌دارد، درحالی‌که متاورس به‌عنوان یک مفهوم، سطح پیشرفته‌ای دارد؛ اما ما هنوز در آن مرحله‌ی پیشرفته‌ای که باید باشیم نیستیم. بااین‌حال متاورس درس‌های ارزشمندی به ما می‌دهد که ممکن است به هدایت و مدیریت زمان حال کمک کند. ادوارد مانگادا، ویکتوریا سمور، تاتسواکی تسوکودا و باستین ویونونت نیز در پژوهش اخیر خود تحت عنوان «متاورس، چالش‌ها و مسائل نظارتی» ۲۰۲۲؛ تمرکز و بحث اصلی خود را به دولت‌ها و سازمان‌های بین‌المللی معطوف می‌دارند. طبق بررسی آن‌ها، متاورس با تغییر سبک زندگی و مسائل اقتصادی و منفعت‌طلبی فعالان در این حوزه می‌تواند آینده جوامع را به خطر بیندازد.

به هر حال می‌توان گفت آثار مورد اشاره نگاهی تک‌بعدی به موضوعات فناوری‌های نوین و اثربخشی

[1] Melodena Stephens

یک‌سویه آن‌ها در روابط بین‌الملل داشته‌اند و شاید به دلیل نو بودن فناوری متاورس اشاره مستقیمی به آن نشده، درحالی‌که هدف از این مقاله گردآوری و ارائه محتوای غنی و نو با رویکردی پیشنهادی و راهکاری و همچنین پر کردن شکاف و خلائی است که به‌واسطه ظهور متاورس در روابط بین‌الملل شکل‌گرفته و خواهد گرفت. این پدیده بسیاری از بخش‌های علوم‌انسانی و اجتماعی را با پرسش‌های اساسی روبه‌رو ساخته است، به‌طوری‌که بسیاری از اساتید و تحلیل‌گران روابط بین‌الملل بر این باورند که حوزه علوم سیاسی و روابط بین‌الملل نیز به همانند بسیاری دیگر از حوزه‌های دیگر تحت‌تأثیر جهان متاورسی قرار خواهد می‌گیرد و به همین علت باید از هم‌اکنون حوزه سیاست و روابط بین‌الملل نیز به دنبال تحقیق و توسعه و پاسخ‌های مشخص و صریحی برای این پرسش‌ها داشته باشد. موضوع مورد نظر با یک سؤال اصلی و محوری آغاز خواهد شد؛ «نقش و اثرات فناوری متاورس بر روابط بین‌الملل چگونه است؟ و این فناوری چه تغییرات و دگرگونی‌هایی در روابط سنتی حاکم بر جوامع و ساختار بین‌الملل ایجاد خواهد کرد؟» به همین منظور سعی شده بر اساس فرضیه «فناوری متاورس نقش راهبردی و مؤثری در روابط بین‌الملل ایفا و باعث تغییر و دگرگونی حوزه‌های مختلفی نظیر؛ سیاست و دیپلماسی، اقتصاد، فرهنگ و... در روابط سنتی جوامع حاضر در ساختار بین‌الملل خواهد شد» به سؤال مذکور پاسخ داده شود. در پژوهش حاضر از روش کیفی و بر پایه اسناد، مقالات و منابع کتابخانه‌ای و استفاده از دیدگاه متخصصین امر استفاده شده است. مطالب مقاله بعد از بیان تعاریف و نظریات، ابتدا متغیر وابسته (روابط سیاسی سنتی کشورها) و سپس متغیر مستقل (فناوری متاورس) تشریح خواهند شد؛ در نهایت نیز با عنوان «متاورس و دگرگونی روابط سنتی میان کشورها» داده‌ها، تحلیل و نتایج حاصله بیان می‌گردد.

۲ تعاریف و مفاهیم

۱.۲ فناوری

فناوری[۲] یا فنّاوری جزء جدایی‌ناپذیر زندگی روزمره‌ی انسان‌ها در تمام نقاط کره زمین به شمار می‌رود. در همه بخش‌های زندگی‌مان از فناوری استفاده می‌کنیم، برای تمامی بخش‌های کسب‌وکارمان به فناوری نیاز داشته و در نهایت زندگی‌مان پیوند عمیقی با فناوری برقرار ساخته است. فناوری دانشی است که در خدمت خلق ابزار، پردازش امور و استخراج مواد به کار گرفته می‌شود. مفهوم اصطلاح فناوری بسیار وسیع است و هر فرد دارای درک شخصی از معنی فناوری است. از فناوری برای انجام وظایفی مختلف در زندگی روزمره‌مان استفاده می‌کنیم. از فناوری برای افزایش توانایی‌هایمان استفاده می‌کنیم، و همین مسئله منجر می‌شود انسان‌ها به بااهمیت‌ترین بخش از سامانه‌ی فناورانه تبدیل شوند (جلالی، ۱۳۷۹: ۲-۲۲).

[2] Technology

۲.۲ متاورس

واژه متاورس[۳] در واقع ترکیبی از دو کلمه "Meta" به معنای فراتر و"Universe" به معنای جهان است. این جهان دیجیتال، به‌عنوان یک فضای مشترک مجازی تعریف می‌شود که با تلاقی واقعیت مجازی، واقعیت افزوده و اینترنت معنی پیدا می‌کند. مثال‌های مختلفی وجود دارند که ممکن است از قبل با آن‌ها آشنا باشید؛ مانند بازی‌های رایانه‌ای محبوب[۴]

۳ نظریه ها

۱.۳ لیبرالیسم و همکاری بین‌المللی

لیبرالیسم در رشته بین‌الملل بر این باور است که به دلیل سه جریان عمده در عرصه بین‌المللی، کشورها به سمت همکاری بیشتر قدم برمی‌دارند: ابتدا، روند وابستگی متقابل بین کشورها، به‌ویژه در عرصه‌های مختلف اقتصادی و تجاری است که باعث شده کشورها به دلیل همکاری با یکدیگر منفعت فراوانی ببرند و هم‌زمان دریابند که هزینه منازعه افزایش‌یافته است. دوم این‌که وابستگی متقابل اقتصادی فزاینده موجب بروز و ظهور یک سلسله هنجارها، قواعد و نهادهای بین‌المللی می‌شود که برای تشکیل، تسهیل و همکاری بین کشورها به وجود می‌آیند و سوم این‌که جریان دموکراسی شدن بین‌المللی که طی آن حکومت‌ها بیشتر دموکراتیک می‌شوند، باعث کاهش منازعه و افزایش همکاری‌های بین‌المللی می‌شود. کاب[۵] و الدر[۶] طبق رویکرد ارتباطات، مدلی را برای مطالعه همکاری بین‌المللی ارائه کرده‌اند. این مدل بین عوامل زمینه‌ای[۷] مختلف ازیک‌طرف، و ایجاد مناسبت‌های رفتاری متقابل بین دو ملت (از طریق مبادلات و تعاملات آن‌ها) و آنگاه سطوح همکاری بین‌المللی از طرف دیگر ارتباط برقرار می‌کند (وحید بزرگی، ۱۳۷۵: ۷۸۳).

۲.۳ مکتب انگلیسی و همکاری بین‌المللی

از نظر مکتب انگلیسی، در شرایط عدم همکاری، هر نظمی که در نظام بین‌المللی وجود داشته باشد، ناشی از عوامل مادی است و نه فرهنگی. از این دیدگاه، هرچه نظام بیشتر از تعارض به سمت همکاری حرکت بشتابد، تناسب رهیافت معناگرایانه نیز فزونی می‌یابد و از اعتبار و اهمیت رهیافت مادی‌گرایانه کاسته می‌شود. پیروان مکتب انگلیسی بر نقش نهادها، هنجارها و قواعد در نظام بین‌الملل همواره تأکید داشته و برای آن‌ها نهادهای بین‌المللی از اهمیت فراوانی در کاهش تعارضات و افزایش همکاری‌ها برخوردارند. از نظر مکتب انگلیسی، همکاری در شرایط آنارشی نه‌تنها ممکن است، بلکه در عمل نیز وجود دارد.

---

[3] Metaverse

[۴] بازی‌های رایانه‌ای محبوبی همچون Fortnite و Roblox و Animal Crossing

[5] Cobb

[6] Elder

[7] Background Factors

۳.۳ رئالیسم و همکاری بین‌المللی

این نظریه که ریشه در اندیشه و فلسفه مورخان و فیلسوفان مغرب‌زمین، مانند توسیدید، ماکیاولی، و هابز دارد، بعد از جنگ جهانی دوم به‌صورت منظم توسط «هانس مورگنتا»[۸] در حوزه روابط بین‌الملل معرفی گردید. فلسفه بدبینانه ماکیاولی و هابز، انسان را موجودی شرور، خودخواه و منفعت‌طلب تعریف می‌کرد که شرارت، پرخاشگری، خودپرستی و خشونت را درذات‌خود به همراه دارند. اعتقاد رئالیست به ناهماهنگی منافع در جهان، و تأکید آنان بر منازعه‌آمیز بودن روابط بین‌الملل، چشم‌انداز همکاری را در این دیدگاه ضعیف نموده است؛ بنابراین، عامل عمده در چشم‌انداز رئالیست‌ها که مانع همکاری می‌شود ملاحظات مربوط به دستاوردهای نسبی و نگرانی از فریب است. بااین‌حال، همکاری ازنظر رئالیست‌ها غیرممکن نیست. دولت‌ها تنها زمانی دست به همکاری خواهند زد که این سیاست در خدمت منافع ملی به منزله قدرت آن‌ها باشد و این اقدام قدرت ملی آن‌ها را افزایش دهد.

۴.۳ پست‌مدرنیسم و همکاری بین‌المللی

اکثر کسانی که به بحث درباره پست‌مدرنیسم می‌پردازند، به‌دشواری یا ناممکن بودن ارائه تعریف دقیقی و صریحی از آن اعتقاد دارند. واسکوئز در ارزیابی تأثیرات پست‌مدرنیسم بر حوزه مطالعاتی روابط بین‌الملل به پنج بعد مهم از این اندیشه اشاره می‌کند: ۱-نفی این ایده که مدرنیسم پایان تاریخ است؛ ۲-انتخابی بودن و برساخته بودن هر آنچه هست؛ ۳-نقش باورها و رفتارها به‌عنوان خالق واقعیت‌ها؛ ۴-قائل شدن فرایند هویت‌یابی و برساخته شدن هویت به‌عنوان شکلی از قدرت؛ ۵-رها نبودن تحقیق علمی از ارزش‌ها و نقش زبان و چارچوب‌های مفهومی در خلق شیوه‌های زندگی.

۴ جهانی‌شدن و نظام بین‌الملل

جهانی‌شدن به‌عنوان موضوعی مهم و اثرگذار در روابط بین‌الملل، طی چند دهۀ اخیر موجب پدیدار گشتن تغییراتی شگرف در نظام بین‌الملل شده است. عوامل مختلفی مثل: تشدید تعامل‌های فرامرزی، تنوع در نوع و تعداد بازیگران، ارتباطات و پیوندهای بینا مرزی، وابستگی متقابل بین کشورها، تغییر در ماهیت قدرت، گسترش حیطه‌ها و عرصه‌های تعاملات بین‌المللی و گشتار در نحوه تأثیرگذاری بازیگران بر فرایندهای تصمیم‌گیری در روابط بین‌الملل من‌جمله این پیامدها محسوب می‌شوند (دهشیری، ۱۳۹۳: ۷-۴۴).

۱.۴ ارتباطات بین‌الملل

ارتباطات بین‌المللی، نتیجه فناوری‌های جدید ارتباطی، انقلابی جهانی محسوب می‌شود که به‌نوعی نابودی یا کم‌رنگ‌شدن مرزهای ملّی و تقویت هویت جهانی و فرهنگ بین‌المللی، از جمله نتایج آن است. ارتباطات بین الملل در ابتدا به‌عنوان یک نظریه در موضوع وسایل ارتباط‌جمعی در جهان بیان شد و به دلیل جایگاه و اهمیت فراوان، با نام انقلاب ارتباطی در جهان معرفی گشت که در آن علاوه بر حذف فاصله‌ها، مهره‌های

[8] Hans Morgenthau

مورد استفاده در بازی‌های سیاسی نیز دچار گسترش و تحول گردید. رابطه ارتباطات بین‌المللی و روابط بین‌المللی: ارتباطات بین‌المللی و روابط بین‌المللی لازم و ملزوم یکدیگر و محصول شرایط تاریخی بعد از قرون‌وسطی و شرایط تغییر یافته بعد از آن دوران محسوب می‌گردند. بهره‌برداری دولت‌ها از مطبوعات، اولین استفاده از ارتباط‌جمعی در روابط بین‌الملل بوده است.

۲.۴ فناوری‌های نوین ارتباطی

اگر بخواهیم ریشه شکل‌گیری فناوری‌ها را بیان کنیم باید ریشه آن را از انسان‌های اولیه جست‌وجو کرد؛ ابزارهای سنگی و چوبی در واقع جزو اولین فناوری‌ها به شمار می‌آیند. تاریخ نشان داده هر ابزار و فناوری جدید و ارتقا یافته‌ای که پدیدار گشته نتیجه فناوری و ابزار قبلی است؛ بنابراین در حال حاضر ما شاهد فناوری‌های بسیار پیچیده و کارآمدی نسبت به ابزارهای نخستین هستیم. ابزارهای نوین ارتباطی ترکیبی از چندین فناوری شامل وسایل ارتباط‌جمعی، انفورماتیک و ارتباطات دور است. این مثلث فناوری، یاری‌رسان به انسان‌ها در جهت ضبط، ذخیره‌سازی، پردازش، بازیابی، انتقال و دریافت اطلاعات در هر زمان و مکانی است. اثرات قابل‌ملاحظه فناوری‌های نوین ارتباطی بر جوامع انسانی در بخش‌های اجتماعی، اقتصادی، سیاسی را می‌توان به شرح زیر تشریح نمود:

- اثرات اجتماعی: بیشترین اثرات اجتماعی فناوری‌های نوین دوسویه بودن روابط در کمترین زمان ممکن است.
- اثرات اقتصادی: فناوری‌های نوین موجب انتقال و گسترش علم و دانش بین صنایع مختلف در دنیا شده است.
- اثرات سیاسی: بر اثر گسترش وسایل ارتباط‌جمعی امکان دخالت در جهت‌دهی رویدادهای سیاسی توسط صاحبان رسانه‌ها را دوچندان کرده است. کاهش اقتدار چهره‌های سیاسی و دولت‌ها، زایل شدن اسطوره مردان قدرتمند، به علت اطلاع مردم از زوایای مختلف زندگی معمولی آن‌ها، تفکرات و اندیشه‌های سیاسی‌شان، شکست‌ها و ...

۳.۴ فناوری متاورس

انسان‌ها همیشه به دنبال معنایی سازی پدیده‌های فیزیکی بوده و تلاش کرده‌اند برای هر موجودیتی نمادهای معنایی تعیین و به‌صورت جمعی بر آن توافق کنند. تداوم تلاش‌ها برای معنایی ساختن پدیده‌ها با پدیدار شدن اینترنت و شکل‌گیری شبکه‌ها و جایگاه‌های الکترونیکی با تحول جدی روبرو شده و به ظهور واقعیت‌های جدیدی با عناوین مختلف مانند واقعیت دیجیتال، واقعیت مجازی، واقعیت افزوده، واقعیت توسعه‌یافته، واقعیت ترکیبی و نظایر آن انجامیده است. رواج مفهوم متاورس هرچند با تغییر یک برند تجاری پررنگ‌تر شده، اما ابعاد ورود به یک فضای جدید مبتنی بر واقعیت مجازی بسیار گسترده‌تر و عمیق‌تر از یک برند تجاری خاص است. اولین مصداق از متاورس، فضای زندگی دوم بوده است که تلاش می‌کرد، شکل شبیه‌سازی‌شده

زندگی در جهان فیزیکی را در فضای اینترنت بازتولید کند. در یک تعریف عملیاتی، متاورس فضای حاصل از ترکیب اینترنت با واقعیت مجازی است. متاورس مفهومی است که به سال ۱۹۹۲ بازمی‌گردد، زمانی که یک نویسنده رمان علمی تخیلی، نیل استفنسون، آن را در رمان خود Crash Snow[۹] ابداع کرد. در این رمان، استفنسون متاورس را به‌عنوان دنیایی مجازی توصیف می‌کند که در آن قهرمان داستان می‌تواند از دنیای واقعی به آن فرار کند.

۱.۳.۴ ساختار جهان دیجیتالی متاورس

متاورس از بخش‌های مختلفی تشکیل می‌شود. در اینجا شاکله اساسی این اکوسیستم مطرح می‌شود: اینترنت، شبکه‌ای غیرمتمرکز از کامپیوترها که متعلق به هیچ نهاد یا دولتی نیست و برای استفاده از آن نیاز به دریافت مجوز از هیچ ارگان مرکزی نیست. استانداردهای باز برای رسانه‌ها شامل متن، تصویر، صدا، ویدئو، آیتم‌های سه‌بعدی، هندسه سه‌بعدی، بردارها و روش‌هایی برای ایجاد و ترکیب هر یک از این موارد است. سخت‌افزار واقعیت مجازی نیز شامل عینک هوشمند، فناوری هپتیک و تردمیل همه‌کاره و... هستند.

۲.۳.۴ اهمیت متاورس

متاورس حتی اگر به دنیایی که برای آینده خود تصور کرده دست نیابد، می‌تواند نحوه تعامل ما با دنیای دیجیتال را تحت‌تأثیر قرار دهد. تجربه مجازی جمعی می‌تواند فرصت‌های جدید برای تولیدکنندگان محتوا، گیمرها و هنرمندان ایجاد کند. این فناوری به‌عنوان توسعه‌ای از اینترنت توصیف نمی‌شود؛ بلکه جایگزینی برای آن است که با استفاده از فناوری بلاک‌چین و برنامه‌های غیرمتمرکز ساخته می‌شود. حتی اگر متاورس به چشم‌اندازی که برای آن متصور شده است نرسد، بازهم می‌تواند نحوه تعامل ما با دنیای دیجیتال را تغییر و دگرگون سازد؛ یک تجربه مجازی جمعی، می‌تواند فرصت‌های جدیدی را برای فعالان این حوزه، گیمرها و هنرمندان به ارمغان بیاورد؛ به همان شیوه‌ای که توکن‌های غیرقابل‌تعویض (NFT) نه‌تنها اقتصاد را تغییر داده‌اند، بلکه آن را دوباره از نو ساخته‌اند (محمودی، صادقی، ۱۴۰۱: ۳-۹).

با فراگیر شدن ویروس کرونا، بسیاری از کلاس‌های درس و جلسه‌های کاری به سمت سیستم آنلاین رفتند. بزرگ‌ترین مشکل کلاس‌های درس و جلسه‌های آنلاین کاهش تعامل افراد نسبت به شرایط حضوری است. متاورس نیز به دنبال ایجاد تعامل بیشتر میان دنیای فیزیکی و مجازی است که شما می‌توانید با استفاده از ابزارها و فضایی که ایجاد می‌شود، طی زمانی که در یک جلسه آنلاین شرکت می‌کنید تعامل بیشتری با افراد دیگر داشته باشید. حضور در دنیای متاورس فقط به جلسات کاری ختم نمی‌شود و می‌توانیم از این فرصت برای برگزاری مهمانی‌ها، دورهمی و گردهمایی نیز استفاده کنیم. برای مثال می‌توانید جشن تولد خود را در فضای متاورس برگزار کنید و دوستان شما با آواتارهای خود در این فضا حضور داشته باشند.

[۹] خرابی برفکی

۳.۳.۴ ویژگی‌ها متاورس

متاورس مجموعه‌ای از فضاهای چندبعدی شبیه‌سازی‌شده، شبه هوشمند، متصل و مبتنی بر فناوری اطلاعات است که تعاملات اجتماعی، اقتصادی، علمی و غیره به‌صورت ترکیبی توسط عامل‌های هوشمند شده و انسان‌ها انجام می‌شود. همه تعاملات موجود و جاری در جهان فیزیکی قابلیت انتقال به فضای متاورس را داراست. حضور عامل‌های هوشمند در کنار قابلیت‌های گرافیکی و شبیه‌سازی سطح بالا موجب پویایی بیشتر فضاها و جذابیت آن‌ها شده است. یک فرد حقیقی یا حقوقی با ورود به فضای متاورس در واقع بازنمونی ارتقا یافته، انعطاف‌پذیر و چابک از موجودیت فیزیکی خود را ایجاد و توسعه می‌دهد. به‌کارگیری ابزارهای الکترونیکی در متاورس موجب شده که محدودیت خاص و منحصر در جهان فیزیکی از بین رفته و جای خود را به موجودیت‌ها و ارتباطات پویا داده است.

احساس حضور واقعی: کاربران در این دنیای مجازی و در کنار باقی کاربران، احساس حضور کنند. تحقیقات نشان می‌دهد که این احساس حضور به افزایش کیفیت تعاملات در این دنیای مجازی کمک می‌کند. هرچند فناوری اینترنت در بستر برخی شبکه‌های اجتماعی این احساس را قدری فراهم آورده بود؛ اما در متاورس این احساس حضور بسیار ملموس‌تر و واقعی‌تر است. کاربران می‌توانند در دنیاهای مجازی متعددی سیر کنند و تجربه‌های مختلفی در قالب دیجیتال کسب نمایند. نکته‌ای که باید در اینجا به آن اشاره کنیم این است که این احساس حضور و نزدیکی با دیگران، از طریق هدست و نمایشگرهایی که وجود دارند انتقال پیدا می‌کند. به دلیل فضای سه‌بعدی آن، حضور واقعی را برای کاربران، تداعی می‌کند (Lee, Braud, 2021: 34-35).

تعامل و همکاری: متاورس می‌تواند همکاری جهانی را با وجود فاصله‌های جغرافیایی فراهم کند. این دنیای دیجیتال می‌تواند قابلیت دسترسی برای وقایع اجتماعی را نیز فراهم کند و همچنین می‌تواند بسیاری از وقایع اجتماعی را که به‌صورت فیزیکی ممکن نیست ایجاد نمایند و همچنین می‌توانید فعالیت‌ها از جمله خریدوفروش را انجام دهید.

فرازمانی: کاربران در متاورس می‌توانند در هر زمانی و در هرجایی بدون محدودیت فضا حضور یابند.

هم‌زمانی: ویژگی است که بر اساس آن کاربران در دنیای کشور مختلف و با فاصله زیاد می‌توانند در یک واحد ارتباط داشته باشند.

قابلیت سرعت بالا: همه چیز در متاورس به‌صورت سریع و بدون تأخیر رخ می‌دهد و لذا تجربه در آن بی‌نقص است.

پایداری: ویژگی پایداری در متاورس به منزله امکان دسترسی همیشگی و ذخیره‌سازی است. شما در متاورس می‌توانید، هر وسیله و ساختمانی را به هر شکلی که می‌خواهید، بسازید. ابزارهای جدید ذخیره‌شده

و در مراجعات و استفاده‌های بعدی شما وجود خواهند داشت. برخلاف دنیای واقعی که ممکن است اطلاعات و ابزارها روزی از بین بروند یا تخریب شوند، در متاورس اطلاعات و ابزارها به دلیل ماهیت دیجیتالی بودن از بین نمی‌روند. این به دلیل فناوری بلاک‌چین است که همه چیز در آن می‌تواند به‌صورت ثابت ذخیره شود (محمودی، صادقی، ۱۴۰۱: ۳-۹).

۴.۳.۴ مزایای متاورس

متاورس پتانسیل تغییر امور جهانی را به سمت بهتر شدن دارد. دیپلماسی بین‌المللی ممکن است به همین راحتی در سفارتخانه‌های مجازی انجام شود. کشورهای کوچک‌تر و ضعیف‌تر، ممکن است خود را در زمین‌بازی برابر تری بیابند و بهتر بتوانند در امور تصمیمات جهانی در ترکیب باقی بمانند یا شاید اتحادیه‌های جدیدی ایجاد کنند. محیط‌های مجازی نیز برای فعالانی که در برابر اقتدارگرایی دیجیتال مقاومت می‌کنند، نویدبخش بوده است. گزارشگران بدون مرز از یک کتابخانه بدون سانسور حمایت مالی کرده است که در آن کاربران می‌توانند محتوای نویسندگان مخالف را ببینند که در برخی از کشورها سانسور شده است. این احتمال وجود دارد که متاورس نوید جدیدی برای آزادی و شفافیت در فراسوی مرزها به ارمغان آورد.

۵.۳.۴ کاربردهای متاورس

توانایی‌های بالقوه زیادی وجود دارد که می‌توان در جهت ارتقا عملکرد و بهره‌وری در حوزه‌های مختلف از آن استفاده کرد. این توانایی‌ها می‌تواند ما را به دنیای مجازی جذابی برده و تجربه‌های منحصربه‌فردی را برای ما به ارمغان بیاورد. برخی کاربردهایی که می‌توان به آن اشاره کرد شامل موارد زیر است؛ متاورس پزشکی و سلامت؛ متاورس علمی و آموزشی؛ متاورس تفریحی و سرگرمی؛ متاورس تجاری و خرید؛ متاورس فرهنگی و هنری؛ متاورس گردشگری؛ متاورس نظامی. در ادامه به طور اختصار به کاربردهای متاورس در چند حوزه خواهیم پرداخت.

حفاظت متاورس از محیط‌زیست: اولین مورد در ارتباط بین متاورس و محیط‌زیست را می‌توان در کاهش نیاز به حمل‌ونقل دید. حمل‌ونقل منبع اصلی انتشار گاز کربن است و به افزایش گرمایش جهانی کمک می‌کند. به‌عبارت‌دیگر مزیت اصلی متاورس برای محیط‌زیست این است که به میزان قابل‌توجهی نیاز به سفر انسان را از بین می‌برد و در نتیجه ترافیک کمتر، تصادفات کمتر، آلودگی کمتر و در نتیجه گرمایش زمین کمتر می‌شود. این فناوری همچنین می‌تواند مکانی برای برگزاری فعالیت‌های دیگر، مانند کنفرانس‌های بین‌المللی و نمایشگاه‌ها باشد، جایی که مردم از سراسر جهان می‌توانند بدون پرواز به منطقه‌ای دیگر در آن شرکت کنند. برای افراد خوشنام سیاسی و تجاری بزرگ، برگزاری کنفرانس‌ها در دنیای مجازی آسان‌تر است، بنابراین علاوه بر هزینه‌های هنگفت امنیت و سفر، در زمان صرفه‌جویی می‌شود. با انتقال بخشی از زندگی خود به دنیای مجازی، می‌توانیم سفرهای غیرضروری را کاهش دهیم و در نتیجه انتشار کربن را کم کنیم.

متاورس و نجات جان انسان‌ها: برای اولین‌بار انسان‌ها می‌توانند موقعیت‌های خطرناک را به‌وسیله واقعیت افزوده تجربه کنند. می‌توان از VR به‌عنوان جایگزین آموزش حضوری بسیاری از مشاغل خطرناک

استفاده کرد. افرادی که شغل‌های خطرناکی دارند و بسیاری از خدمات عمومی را می‌توان تنها با کمک متاورس و ربات‌های کنترل از راه دور انجام داد. متاورس به افراد اجازه می‌دهد تا با خیال راحت یک نسخه از واقعیت مجازیِ کارهای پرخطر را قبل از اینکه در معرض خطر واقعی قرار بگیرند، تجربه کنند.

متاورس و صنعت بازی: در حال حاضر متاورس بیشتر از هر چیزی با صنعت بازی گره‌خورده است. علاقه‌مندان به این حوزه می‌توانند بیش‌ازپیش لذت و تجربه واقعی داشته باشند.

متاورس و حقوق بشر: شاید شنیدن این کلمه در اینجا کمی عجیب به نظر برسد. متاورس، مزایای بسیاری برای هر نژاد، طبقه اجتماعی و هر سطح درآمدی به ارمغان می‌آورد. فرصت‌های شغلی، گفت‌وگو بین ملت‌های مختلف و... فرصت‌های بی‌نظیری برای تمامی افراد در سرتاسر دنیا به وجود می‌آورد.

متاورس و یادگیری: بسیاری از افراد، از جلسات آموزش مجازی لذت می‌برند و در این زمینه از متاورس استفاده می‌کنند. فضای سه‌بعدی بر اساس چاشنی احساس حضور واقعی بسیار بهتر از محیط خشک و خام کتب درسی می‌تواند ذهن انسان‌ها را نسبت به آموزش و یادگیری برانگیزد (محمودی، صادقی، ۱۴۰۱: ۵-۷).

۶.۳.۴ محدودیت‌های متاورس

کاربران در حال حاضر نیاز به داشتن سخت‌افزارهای قوی و گران‌قیمت برای استفاده از متاورس دارند. زیربنای خطوط مخابراتی در حال حاضر گنجایش تأمین سرویس‌های متاورس جهت استفاده عامه کاربران را ندارد. پردازشگرهای دستگاه‌های سخت‌افزاری برای تولید گرافیک‌های سه‌بعدی پیچیده توانایی کافی را ندارند.

۷.۳.۴ متاورس در کشورهای توسعه‌یافته و درحال توسعه

همه کشورهای درحال‌توسعه به سمت متاورس پیشروی می‌کنند. بنا بر تحقیقات صورت‌گرفته، مردم کشورهای درحال‌توسعه دوبرابر بیش‌تر از کشورهای توسعه‌یافته به تأثیرگذاری متاورس بر زندگی روزمره‌شان خوش‌بین هستند. به طور مثال در کشور هند شرکت‌های بزرگ هندی شروع به استقبال از دنیای جدید جسورانه متاورس کرده‌اند و کشورهایی نظیر عربستان سعودی و امارات با تبدیل‌شدن به بازیگران اصلی خاورمیانه در دنیای مجازی آنلاین، منطقه را هدایت خواهند کرد. ایده متاورس در ایالات متحده شروع‌شده و شرکت‌های زیادی وجود دارند که درحال‌توسعه فناوری‌های موازی مانند AR و VR را نیز هستند. ازآنجایی‌که کاربران اینترنتی، همچنان متاورس را به‌عنوان یک فناوری انقلابی می‌شناسند و آن را تمجید می‌کند، کاربران اینترنت در سراسر اروپا به طور فزاینده‌ای در مورد این مفهوم کنجکاو شده‌اند. علاوه بر این روزانه بر شمار کشورهایی که علاقه‌مند به ورود و استفاده از این فناوری هستند افزوده می‌گردد (راسل، ۱۴۰۱: ۲۹-۴۸).

۵ متاورس و دگرگونی روابط سنتی میان کشورها

روابط بین‌الملل که امروزه به‌صورت یک‌رشته معتبر علمی شناخته می‌شود و دارای تحقیقات و بررسی‌ها و نظریات بسیاری است، سابقه‌ای طولانی به قدمت تشکیل دولت‌ها در روی کره زمین دارد. دولت‌ها از همان ابتدا روابط مختلف و متنوعی با یکدیگر داشته‌اند که مهم‌ترین آن‌ها تجارت و درگیری‌های نظامی بوده است. ولی در روزگار کنونی ما، ملت‌ها به‌صورت مهم‌ترین واحدهای سیاسی جهان با یکدیگر روابط متعدد و بسیار پیچیده‌ای دارند که عرصه تحقیقات روابط بین‌الملل نیز به شمار می‌رود. امروزه بی‌توجهی به قدرت فناوری و الزامات آن می‌تواند تأثیر جدی و مخربی بر موقعیت کشورها در منظومه قدرت و ثروت جهانی و نظام بین‌الملل داشته باشد.

دراین‌بین فناوری متاورس با ویژگی‌های منحصربه‌فرد خود نظیر شتاب فوق‌العاده، قاعده گریزی، بدیع بودن، واقعیت مجازی، کنترل‌ناپذیری، کاهش فاصله‌های زمانی – مکانی و افزایش کنشگران در سطح جهانی، موجب شده ابزاری سودمند و هم مخرب برای کشورها تلقی می‌شود. این فناوری باعث کاهش هزینه‌ی ارتباط و ایجاد پیوند و هماهنگی میان فضاهای اختصاصی کاربران، می‌شود. در این محیط، افراد و گروه‌ها بدون حضور فیزیکی برای اقدام و هدفی مشترک با یکدیگر مرتبط می‌شوند. این محیط، حاکمیت دولت – ملت و دولت‌های ملی را با مسائل مختلفی مواجه می‌سازد و موجب آن می‌شود مجموع حاکمیت از معنای قدرت بلامنازع و عدم پاسخگویی سنتی خود جدا شده و به سمت «مسئولیت‌پذیری» حرکت نمایند. متاورس با پررنگ‌کردن نقش افکار عمومی و همگانی کردن جریان آزاد اطلاعات، نه‌تنها سطوح ملی بلکه ساختار نظام بین‌الملل را با دگرگونی‌های اساسی مواجه می‌سازد. ساختار فعلی تحت‌تأثیر عصر اطلاعات در حال شکل‌گیری است و طبیعی است کشورهایی از بیشترین قدرت و توان تأثیرگذاری بر این ساختار برخوردارند که توجهات و برنامه‌ها و لوازم کافی را در این زمینه به کار گیرند.

ساختار نظام بین‌الملل حال حاضر ساختاری انعطاف‌پذیر است؛ بنابراین دیدگاه، نظم جدید نظمی غیرساختاری است و آنچه مشخص‌کننده‌ی رفتار کشورهاست، منافع ملی آن‌ها است که به‌صورت شناور تابع شرایط زمان و مکان است. در ساختار جدید، نقش توان نظامی رو به افول نهاده و توانمندی‌های اطلاعاتی و اقتصادی به گفتمان قدرت‌ساز مسلط تبدیل‌شده و مؤلفه‌های مهمی مثل جهانی‌شدن، گسترش و تعمیق دموکراسی، چندلایه شدن گفتمان امنیتی، منطقه‌گرایی، یک‌جانبه‌گرایی برخی واحدهای سیاسی قدرتمند بر تصمیمات و داده‌های سیاست خارجی واحدهای سیاسی تأثیرگذار و تعیین‌کننده شده‌اند.

متاورس با پراکندن اقتدار بین بازیگران متعدد، افزایش حضور و تأثیر جامعه مدنی جهانی و رهبری جریان توسعه جهانی امور مالی و تجاری، روند سنتی روابط بین‌الملل را با چالش‌های عمده و نوینی مواجه خواهد ساخت. در شرایطی که مرزهای سرزمینی اهمیت خود را به مرزهای اقتصادی و فرهنگی واگذار می‌نمایند و متاورس، فرایند جهانی‌شدن را سرعت می‌بخشد، حضور سازنده در افکار عمومی دنیا، از طریق این فناوری برای تأثیرگذاری در راستای تأمین منافع ملی در ابعاد مختلف سیاسی، اقتصادی و فرهنگی، مهم‌ترین تلاش اغلب کشورهای جهان محسوب می‌گردد. به نظر می‌رسد متاورس در سال‌های آینده به‌عنوان یکی از ارکان سیاست‌گذاری‌های کلان اقتصادی مبدل خواهد شد. هرچه میزان دسترسی شرکت‌های نوپا و کسب‌وکارهای

کوچک و متوسط به زنجیره‌های تأمین بین‌المللی افزایش یابد این موضوع جزو موارد انگیزشی در اهداف توسعه پایدار ملی خواهد بود. دیپلماسی بین‌المللی ممکن است به‌راحتی در سفارتخانه‌های مجازی انجام شود. کشورهای کوچک‌تر و کمتر قدرتمندتر ممکن است خود را در زمین‌بازی برابرتر بیابند و بهتر بتوانند در امور جهانی در ترکیب باقی بمانند یا شاید اتحادهای غیرممکن را ایجاد کنند.

متاورس در حال آمدن است. زمانی متاورس ایده‌ای فانتزی و علمی – تخیلی بود، به‌ویژه در رمان «تصادف برفی» نیل استفنسون، جهان مجازی فراگیر که در کنار جهان فیزیکی وجود داشت؛ اما پیشرفت‌های فنّاورانه این دگرگونی جامعه بشری را به‌اندازه‌ای به واقعیت نزدیک کرده است که ما را ملزم می‌کند پیامدهای آن را در نظر بگیریم. به‌هرحال ممکن است چالش‌هایی نیز با خود به همراه داشته باشد که این همان نقطه‌ای است که کشورها باید نقش سازنده خود را ایفا نمایند. به طور مثال، در این محیط مجازی، کمپین‌های اطلاعات نادرست، جاسوسی و نظارت را افزایش می‌دهد و مبارزه برای کنترل زیرساخت‌های فیزیکی متاورس به‌خوبی می‌تواند درگیری‌های جهانی را تشدید کند.

همچنین فناوری متاورس باعث تغییر روابط سنتی کشورها با محیط اطرافشان می‌شود. این نوع فناوری روند کاغذ سالارانه و بوروکراتیک انتقال اطلاعات، انجام امور و ارتباطات درون حکومتی و محیطی را متحول کرده و باعث کارآمدی اطلاع‌رسانی و خدمات‌رسانی بهینه کشورها می‌گردد. با پدیدار گشتن متاورس، انتشار سریع اطلاعات، جوامع و در نتیجه شیوه عمل حکومت‌ها نیز دگرگون می‌شود. می‌توان گفت که کشورها در مواجهه با پارادایم جهانی‌شدن و فناوری متاورس با مخدوش‌شدن استقلال ملی، حاکمیت و مرزهای آهنین روبرو می‌شوند. دیگر این کشورها نخواهند بود که با تصمیمات خود تحولات جهانی را رقم بزنند؛ بلکه در ارتباط‌های دوسویه و تعاملی با مجموعه‌ی مختلفی از مؤلفه‌های تأثیرگذار در روابط و امنیت بین‌الملل از جمله نقش فزاینده‌ی افکار عمومی است که به کارکرد خود که قدرت سازی و تأمین امنیت است، می‌توانند نقش مؤثری داشته باشند. فناوری متاورس در جهان، خواه‌ناخواه رو به گسترش است. کشورهای توسعه‌یافته، البته با سرعت بیشتری نسبت به کشورهای کمتر توسعه‌یافته، این راه را طی می‌کنند. چنین گسترشی جهان را به‌سوی یک مجموعه واحد اطلاعاتی یا به عبارتی دهکده‌ای جهانی هدایت می‌کند. در چنین جامعه‌ای مرزهای جغرافیایی، مفهوم فیزیکی خود را از دست می‌دهند و مسائل جدیدی بروز می‌کند.

در جمع‌بندی این بحث می‌توان به عمده فرصت‌ها، مسائل و چالش‌های شکل‌گرفته توسط متاورس در جوامع و در روابط بین آن‌ها اشاره نمود؛ افزایش آگاهی عمومی و تعامل آن با سیاست، گسترش آموزش الکترونیکی و امکان کاهش فقر، اعمال حقوق بشر، تأثیرات اقتصادی و اجتماعی، جنایات سایبرنتیکی، پورنوگرافی و مسائل ضد فرهنگی، کپی‌برداری غیرمجاز، بروز مشکلات جدید خانوادگی براثر حذف فاصله میان محیط کار و محیط خانه، ایجاد اختلاف دیجیتال میان جوامع و برخورد میان فرهنگ‌ها و جنگ‌های دیجیتالی و... .

بنابراین، بر اساس فرضیه مطرح گشته در این مقاله؛ با تحول و دگرگونی عرصه سیاست بین‌الملل در نتیجه ظهور متاورس و شکلگیری عرصه سیاست هنجاری، زمینه تشکیل و ساخت دوباره هویت‌ها، منافع، مفاهیم و قلمرو سیاسی فراهم می‌گردد و به تشدید تعاملات بین‌المللی، شتاب تغییرات نهادی، توسعه فرایند به همگرایی و به‌هم‌پیوستگی جهانی، اهمیت یافتن هنجارها و افزایش مؤثر نقش بازیگران غیردولتی می‌انجامد.

این فناوری همچنین تأثیرات اساسی و مهمی در ساختار و روابط بین‌الملل ایفا خواهد کرد. به‌طورکلی، تحول در «ساختار نظام بین‌الملل»، «قواعد راهبردی» و «بازیگران عرصه‌ی روابط بین‌الملل» از عمده موضوعاتی هستند که فناوری متاورس با خود به همراه خواهد داشت. بعد از دوران جنگ سرد ما شاهد مفاهیم و تحولات جدیدی در حوزه روابط بین‌الملل بوده‌ایم. مفاهیمی مانند ضربه اول، ضربه دوم، پرده آهنین، جنگ ستارگان و... از بین رفتند و مفاهیم جدیدی همانند جنگ هسته‌ای، بازدارندگی، ساختار دوقطبی، سیاست کنترل و... به حوزه روابط بین‌الملل راه پیدا نمودند، اینک بعد از چند دهه و ثبات در نظم و نبود تغییر و دگرگونی در مفاهیم، به نظر می‌رسد به دلایل و عوامل مختلف و عمدتاً تحت‌تأثیر فناوری، مجدداً شاهد دگرگونی در مفاهیم روابط بین‌الملل خواهیم بود. رشد سریع اطلاعات و ارتباطات و به‌تبع آن فناوری نوین متاورس، باعث می‌شود اغلب مفاهیم در این حوزه بازتعریف گردند. به طور مثال قدرت نظامی و سخت آن به توانایی علمی، انسانی، اطلاعاتی تغییر مفهوم می‌دهد. منافع ملی نیز از ملی‌گرایی به جهان‌گرایی و از تضاد و تعارض به تداخل و هم‌پوشی تغییر می‌یابد. علاوه بر بازتعریف مفاهیم نو ناشی از بروز فناوری متاورس، کشورها و سازمان‌های بین‌المللی نیز باید خود را با تغییرات جدید سازگار سازند و موانع، چالش‌ها، فرصت‌ها، راهکارها و دستاوردهای مختلف این حوزه را مورد تحقیق و بررسی قرار دهند.

در بخش فرهنگ، متاورس بانفوذ به قلب فرهنگ کشورها می‌تواند آن‌ها را متلاشی نماید و فرهنگ نوینی در قالب فرهنگ جهانی و البته فرهنگ برتر عرضه نماید. در حوزه اقتصاد نیز منجر به تحولات در حوزه کسب‌وکار، دگرگونی در صنایع مختلف، خلق دستگاه‌ها و کارخانه‌های هوشمند چندمنظوره و چندبعدی، تأثیر بر حوزه صنعت کشاورزی، دامداری و موارد مختلف فراوانی گردد که تمامی این موارد در بحث‌های قبلی مطرح گردیده است. متاورس همچنین هویت افراد، علم و دانش آن‌ها، مذهب، آیین، اعتقادات و مسائل مختلف را نیز تحت شعاع خود قرار می‌دهد؛ مفهوم ملی‌گرایی را در هم پاشیده و به‌سوی درهم‌تنیدگی فراملی‌گرایی حرکت می‌کند. مفهوم جهانی‌سازی و جهانی بودن نیز جان تازه‌ای خواهد گرفت.

تمامی این موارد درنهایت باعث تغییرات در روابط جاری و سنتی کشورها در نظام بین‌الملل خواهد شد و کشورها به‌ناچار، راهی جز تجدید در روابط و مناسبات برای حفظ منافع ابتدا فردی و سپس جمعی نخواهند داشت.

نتیجه‌گیری

متاورس مفهوم و تعریف گسترده‌تری نسبت به دنیای واقعی که در آن زندگی می‌کنیم دارد. باتوجه‌به اینکه دنیای متاورس به فضاهای فیزیکی محدود نیست تا بی‌نهایت امکان گسترش آن وجود دارد و حدومرزی برای آن وجود ندارد. به طور خلاصه باید گفت متاورس دنیای بی‌پایان است. متاورس جایی است که اختیار همه چیز در آن در اختیار خودمان است. می‌توان آینده متاورس را از جهات بسیاری به دنیای واقعی ما شبیه‌سازی کرد. حتی در آینده‌ای نزدیک ممکن است برخی از فعالیت‌ها در متاورس جایگزین دنیای واقعی شود. در آینده با متاورس تعاملات اجتماع به‌شدت گسترده می‌شوند. اکنون فقط می‌توانیم تصویر و ویدئو را با یکدیگر در شبکه‌های اجتماعی به اشتراک بگذاریم، در نسل سوم و آینده دنیا با متاورس می‌توانیم عواطف و احساسات

را به اشتراک بگذاریم. ممکن است احساساتی نظیر بو، مزه و حتی لامسه را از طریق فضای مجازی درک کنیم. دنیای متاورس هم‌اکنون درحال‌توسعه است و در حال حاضر نمی‌توانیم در مورد اینکه آینده جهان با متاورس چگونه است و چگونه کسب‌وکارها گسترش می‌یابند جواب قطعی بدهیم. فقط می‌توانیم برای آن سناریوهای مختلف در نظر بگیریم و برای هر چیزی در آینده آماده باشیم. هنوز استانداردی برای آن تعریف‌نشده است، اما چه قبول کنیم و چه نه آینده دنیا با متاورس تحت‌تأثیر قرار می‌گیرد. به‌هرحال، رقابت قدرت‌های بزرگ، همان‌طور که قبلاً در حوزه فناوری‌های مختلف بین ایالات متحده و چین شاهد بودیم، احتمالاً به متاورس نیز وارد خواهد شد. طبیعتاً پیش‌گام شدن و یا جاماندن از یک فضای تعاملی به‌شدت تأثیرگذار بر نسل آینده، از منظر منافع و امنیت ملی برای دولت‌ها به شکل تهدید یا فرصت تلقی می‌شود.

این فناوری با اثرگذاری و نقش راهبردی در بخش‌های مختلف جوامع باعث می‌شود که این کشورها جهت جلوگیری از نفوذپذیری منفی سایر کشورها، سیاست‌های نوینی را در دستور کار خود قرار دهند. تأثیرپذیری حوزه اقتصاد بر مبنای رونق و فعالیت کسب‌وکار در متاورس، تغییر در فرهنگ کشور به دلیل حل‌شدن فرهنگ‌ها در این محیط و تغییرات در سایر بخش‌ها، درنهایت منجر به تغییر در نظم شکل‌گرفته کنونی بین جوامع و رابطه بین آن‌ها خواهد شد که در فصل‌های قبل به طور کامل تشریح گردید که چگونه می‌توان در این شرایط، روابطی که در این دوره از مدار خود خارج خواهد شد را مجدداً در جهت صحیح خود قرارداد. پیرامون این مبحث، نتایجی که از سایر پژوهش‌ها استنباط می‌شود، تکیه آن‌ها بر مفاهیمی همچون تغییر در نظم و امنیت، دگرگونی در مفهوم قدرت، تحول در مفهوم ملی‌گرایی و رشد جهان‌وطنی و... است. علاوه بر اینکه متاورس بر چنین بخش‌ها و مفاهیمی اثرگذار است و دچار بازتعریف در کارکرد آن‌ها می‌شود، ضروری است که از نقش و ویژگی‌های خاص این فناوری نسبت به سایر فناوری‌های ارتباطی غافل نشویم. مادامی‌که افراد و گروه‌های مختلف از نقاط مختلف جهان در یک محیط، مقابل یکدیگر به فعالیت و مناظره می‌پردازند، خروجی آن ایجاد درهم کنش رفتارها، آداب، رسوم و تفکرات و شکل‌گیری فردی با آگاهی‌های ارتقاءیافته‌تر به‌واسطه این تعاملات است. در این هنگام فرد تأثیر پذیرفته، بر اطرافیان و جامعه و به عبارتی کشور خود در محیط واقعی خود اثرگذار خواهد بود و در نهایت، نتیجه آن تغییر در رویکردهای مختلف در تمامی زمینه‌ها چه در بعد داخلی و چه بعد خارجی و روابط بین‌الملل خواهد بود.

مراجع

[۱] آقایی، سید داود (۱۳۸۲)، سازمان‌های بین‌المللی، انتشارات نسل نیکان.

[۲] برجعلی‌زاده، محمد؛ جعفری، علی؛ کردی، ناهید (۱۴۰۰)، «نقش فناوری‌های نوین ارتباطی در گسترش دیپلماسی در عرصه بین‌الملل»، فصلنامه پژوهش‌های ارتباطی.

[۳] جلالی، علی‌اکبر (۱۳۷۹)، «نقش اینترنت در جهان آینده»، فصلنامه پژوهش‌های ارتباطی، شماره هفتم، ص ۲-۲۲.

[۴] حاجی یوسفی، امیرمحمد (۱۳۸۴)، «سیاست خارجی جمهوری اسلامی ایران در پرتو تحولات منطقه‌ای»، وزارت امور خارجه، چاپ دوم، ص ۲۲-۲۳.

[۵] حیدری فر، محمدرئوف (۱۳۸۹)، «نقش و جایگاه عامل سرزمین در عرصه روابط بین‌الملل»، فصلنامه سیاست خارجی، سال بیست و چهارم، شماره سوم، ص ۸۱۷-۸۴۶.

[۶] دویچ، کارل (۱۹۷۹)، نظریه‌های روابط بین‌الملل، ترجمه: وحید بزرگی (۱۳۷۵)، انتشارات جهاد دانشگاهی، جلد اول.

[۷] دهشیری، محمدرضا (۱۳۹۳)، «جهانی‌شدن و نظام بین‌الملل»، فصلنامه مطالعات راهبردی سیاست‌گذاری عمومی، دوره پنجم، شماره چهاردهم، ص ۷-۴۴.

[۸] سلطانی‌نژاد، احمد؛ اسلامی، محسن؛ راست‌گو، محمدزمان (۱۳۹۵)، «فناوری اطلاعات و ارتباطات پیشرفته و تحول مفهوم حاکمیت در روابط بین‌الملل»، جستارهای سیاسی معاصر، پژوهشگاه علوم‌انسانی و مطالعات فرهنگی، سال هفتم، شماره اول، ص ۸۵-۱۱۴.

[۹] فرجی، محمدرضا (۱۳۸۹)، تحول در ساختار سیستم بین‌الملل و استراتژی یک‌جانبه‌گرایی آمریکا، دانشگاه تربیت‌معلم تهران، دانشکده ادبیات و علوم‌انسانی، پایان‌نامه کارشناسی‌ارشد.

[۱۰] محمودی، محسن؛ صادقی، سالار (۱۴۰۱)، «متاورس و تأثیر آن بر سبک زندگی»، فصلنامه علمی مطالعات حقوقی فضای مجازی، سال اول، شماره اول.

[۱۱] مشیرزاده، حمیرا (۱۳۹۳)، «رویکردهای معنایی در روابط بین‌الملل و تأثیر آن‌ها در تحلیل سیاست خارجی»، فصلنامه رهیافت‌های سیاسی و بین‌المللی، سال پنجم، شماره سی و هشتم.

[12] Eduardo Mangada Real De Asua, Victoria Otter, Tatsuaki Tsukuda, Bastien Vivenot (2022) , “Master in Public Policy and Master in European Affairs Digital, New Technology and Public Policy stream Course“ Comparative approach to Big Tech regulation”, (F. G’sell) Spring semester.

[13] Lik-Hang LEE, Tristan Braud, Pengyuan Zhou, Lin Wang, Dianlei Xu, Zijun Lin, Abhishek Kumar, Carlos Bermejo, and Pan Hui, (2021), “All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity”, Virtual Ecosystem, and Research Agenda Journal, vol 14, no 8.

یک روش کارا جهت شناسایی حملات سیبل در شبکه‌های بین خودرویی

زهرا حر آبادی فراهانی [1]

[1] دانشجوی کارشناسی ارشد مهندسی کامپیوتر - نرم افزار، دانشکده فنی و مهندسی دانشگاه آزاد اسلامی واحد تهران شمال، تهران، ایران
zahrafarahany70@gmail.com

چکیده

محققین با معرفی شبکه‌های موردی بین خودرویی در صدد ایجاد بستر ارتباطی مناسب بین خودروها به منظور نیل به اهداف و کاربردهای مختلفی جهت رفاه حال مردم هستند. با پیشرفت تکنولوژی در قرن حاضر روز به روز بر کاربردهای این شبکه ها افزوده شده و شبکه‌های بین خودرویی بسیار مورد توجه شرکت‌های خودروسازی واقع شده‌اند. در شبکه‌های بین خودرویی، خودروها به صورت کاملاً خودمختار با یکدیگر ارتباط برقرار کرده و یک شبکه غیرساختارمند بی‌سیم ایجاد می‌کنند. در شبکه‌هاي موردی بین خودرویی هیچ ایستگاه یا گره مرکزي، مدیریت و کنترل شبکه را برعهده ندارد و شبکه از یک سري خودرو تشکیل شده که متحرک بوده و جاي ثابتي ندارند. این مساله باعث شده است که تهدیدات امنیتی فراوانی این شبکه‌ها را تهدید کند. بدین منظور در این مقاله روشی برای مقابله با حملات سیبل در شبکه‌های موردی بین خودرویی ارائه شده است. روش پیشنهادی با یارگیری گره‌ها و اثبات هویت گره‌ها بر مبنای تاییدیه گره‌های یار سعی در مقابله با نفوذ به این شبکه‌ها دارند. بدلیل پویایی بسیار بالای شبکه‌های بین خودرویی، مدت زمان همسایگی دو گره جهت یارگیری گره‌ها پارامتر بسیار مهمی است. بدین شکل که هدف انتخاب گره‌هایی است که مدت زمان زیادی مجاور یکدیگر باشند. لذا رویکرد اصلی در روش پیشنهادی این است که گره‌های یار بر مبنای جدول همسایگی گره‌ها تعیین گردند. به طوریکه روش پیشنهادی سعی می‌کند در روند یارگیری از گره‌هایی با مسیر یکسان و مدت زمان همسایگی بیشتر به عنوان گره‌های یار استفاده نماید. پس از تعیین گره‌های یار، روش پیشنهادی بر مبنای کلیدهای عمومی به واسطه گره‌های یار اقدام به تایید پیام‌های امن درون شبکه می‌نماید. به طوریکه اگر فرستنده پیام گره‌ای امن درون شبکه باشد، گره یار کلید عمومی خود را با پیام ارسالی گره فرستنده هش می‌نماید. نتایج شبیه‌سازی‌ها که با شبیه‌ساز ns-۲ پیاده‌سازی شده‌اند نشان می‌دهد که روش پیشنهادی به شکل کارایی گره‌های سیبل را درون شبکه شناسایی نموده و از انتشار بسته‌های جعلی ارسالی توسط آنها ممانعت می‌کند.

کلمات کلیدی: شبکه‌های موردی بین خودرویی، حملات سیبل، جداول همسایگی.

۱ مقدمه

پیشرفت‌ها در شبکه‌های حمل و نقل هوشمند و وسایل نقلیه بین جاده‌ای، راحتی و کارایی را برای فعالیت‌های روزانه بشر به ارمغان آورده است. در این راستا مسافران می‌توانند سریع‌تر و ایمن‌تر نسبت به سیستم حمل و نقل سنتی به مقصد مورد نظر خود برسند. در شبکه‌های بین خودرویی[۱]، وسایل نقلیه به‌واسطهٔ واحدهای کنار جاده‌ای با کابران شبکه و دیگر خودروها در ارتباط هستند تا در صورت بروز تصادف یا تراکم ترافیک، رانندگان را در مورد وضعیت جاده‌ها مطلع نمایند. ارتباطات در شبکه‌های بین خودرویی را می‌توان به ارتباطات خودرو به خودرو (V2V) و خودرو با زیرساخت‌های کنار جاده‌ای (V2I) دسته‌بندی کرد [۱]. واحدهای کنار جاده‌ای اطلاعات کافی از وسایل‌نقلیه موجود در مسیر جهت مدیریت مناسب ترافیک دارند. شبکه‌های بین خودرویی منجر به تحقق حمل و نقل ایمن شده‌اند که این مهم به معنای نجات جان افراد است. این مسأله در صورتی است که امروزه تصادفات رانندگی تلفات جانی و مالی بسیاری را به همراه داشته است [۲].

پیشرفت‌ها در زمینه شبکه‌های بین خودرویی، توسعه‌ی برنامه‌های کاربردی در صنعت خودرو را منتج شده است. شبکه-های بین خودرویی، ایمنی و سهولت سفر را افزایش داده‌اند. اینترنت خودروها[۲] یکی از تغییراتی است که در حوزه‌ی اینترنت‌اشیا رخ داده است. اینترنت خودروها از شبکه‌های بین خودرویی تکامل یافته است که یک فناوری مدرن است و برای کنترل تماس خودرو با خودرو به کار می‌رود. در شبکه‌های بین خودرویی، سرویس‌های مرتبط با ایمنی نیاز به تأخیر کم و قابلیت اطمینان بالا دارند. سرویس‌های بلادرنگ محدودیت‌های زیادی را روی سرعت و پایداری اتصال صرف می‌کنند، و سرویس‌های با تحمل تأخیر عموماً پهنای باند بیشتری مصرف می‌کنند [۳]. با این حال، بسترهای ناهمگن موجود در شبکه به سختی می‌توانند تفاوت این سرویس‌ها و شبکه‌ها را پشتیبانی کنند. یک چالش دیگر در این شبکه‌ها وجود دارد که نحوه‌ی مدیریت و کنترل خودروها بصورت مقیاس‌پذیر و انعطاف‌پذیر است. با افزایش روزافزون اندازه و تراکم شبکه‌های بین خودرویی، مدیریت و کنترل وسایل نقلیه تبدیل به یک چالش اساسی خواهد شد. لذا این مسأله می‌تواند مانع عملکرد کارای شبکه‌ی بین خودرویی گردد [۴].

شبکه‌های بین خودرویی با انواع حملات امنیتی روبرو هستند. از آن جمله مهم‌ترین حملات در این شبکه‌ها می‌توان به موارد زیر اشاره نمود:

- حمله‌ی سیاه چاله[۳]
- حمله‌ی انکار سرویس[۴]
- تغییر چهره[۵]

[1] Vehicular ad hoc networks (VANETs)
[2] Internet of Vehicles (IoV)
[3] Black Hole
[4] Denial of Service (DoS)
[5] Face Changing

- ویروس یا اسپم[۶]
- حمله‌ی سیبل[۷]

حمله سیبل به منظور کنترل شبکه با ایجاد چندین هویت جعلی توسط گره‌ی مهاجم اتفاق می‌افتد. گره‌های مهاجم در پس هویت-های جعلی، آن‌ها را کنترل می‌کند. این یک جعل هویت است که گره‌ی مهاجم برای مختل کردن عملکرد درست برنامه‌های کاربردی شبکه‌های بین خودرویی، چندین گره‌ی دیگر را جعل می‌کند. به گره‌ای که هویت گره‌های دیگر را به صورت جعلی ایجاد می‌کند، مهاجم سیبل گویند. [۵] از طرفی در این حمله برخی گره‌ها ممکن است با جعل‌شناسه‌ی دیگر گره‌ها، اقدام به خراب‌کاری در روند عملکرد شبکه نمایند. افزایش ازدحام شبکه باعث کاهش قابلیت اطمینان به دلیل افزایش تأخیر انتشار بسته و افزایش احتمال از بین رفتن بسته‌ها می‌گردد. از طرفی گره‌ی سیبل می‌تواند خود را به عنوان یک گره‌ی معتبر نشان داده و به صورت غیرواقعی تعداد خودروهای در طول یک مسیر را نشان دهد. به دلیل عملکرد بی‌درنگ شبکه‌های بین خودرویی برای انتشار وقوع رویدادهای درون شبکه، افزایش ازدحام و در نتیجه افزایش تأخیر انتشار رویدادهای درون شبکه می‌تواند به شدت بر جنبه‌های مختلف کارایی شبکه تأثیرگذار باشد. در این مقاله روشی بر مبنای افزونگی طبیعی در شبکه‌های موردی بین خودرویی برای کشف گره‌های سیبل ارائه خواهد شد. در صورت استفاده‌ی مؤثر از افزونگی طبیعی در این شبکه‌ها می‌توان تحمل‌پذیری شبکه در مقابل حملات سیبل را افزایش داد. باقی این مقاله به صورت زیر سازماندهی شده است. در بخش دوم کارهای تحقیقاتی صورت گرفته در زمینه‌ی حملات سیبل ارائه و بحث می‌شوند. بخش سوم روش پیشنهادی برای شبکه‌های موردی بین خودرویی تشریح شده است. نتایج شبیه‌سازی در بخش چهارم بیان شده و در بخش پنجم با بیان نتیجه‌گیری و ارائه‌ی کارهای آینده گزارش این مقاله به پایان رسیده است.

۲ کارهای پیشین

همان‌گونه که بیان شد مهم‌ترین کاربرد شبکه‌های موردی بین خودرویی افزایش ایمنی و سلامت رانندگان و مسافران است. اکثر برنامه‌های شبکه‌های خودرویی برای تأمین امنیت سرنشینان خودروها ایجاد شده‌اند. با توجه به حساسیت موضوع، هرگونه آسیب‌پذیری و حمله، زندگی افراد و سرنشینان خودروها را به‌طور جدی تهدید خواهد کرد [۶]. به این دلیل حمله‌ی سیبل در شبکه‌های موردی بین خودرویی می-تواند برای امنیت رانندگان و مسافران تهدید جدی محسوب شود. برخی از برنامه‌ها و پروتکل‌هایی که می‌توانند به‌وسیلهٔ حمله‌ی سیبل در شبکه‌ی موردی بین خودرویی مورد تهدید قرار گیرند، در زیر مورد بحث قرار گرفته شده‌اند [۷]، [۸]:

[6] Virus or Spam Attack
[7] Sybil

۱. مسیریابی

۲. جمع‌آوری داده‌ای

۳. تخصیص منبع عادلانه

۴. رأی‌گیری

۵. اطلاعات غلط

۶. شناسایی سوءرفتار

- مکانیزم تشخیص براساس آزمون منبع [۸]

خود این مکانیزم به دسته‌های زیر تقسیم می‌شود :

۱. آزمون هویت منبع :

این روش بدین شکل است که خودروهایی که MAC و آدرس IP آن‌ها درون لیست ثبت نیست به‌عنوان یک ورودی مشکوک یا اشتباه در نظر گرفته می‌شوند. در این روش خودروها می‌بایست‌شناسه‌ی یکتای ثبت‌نامی خود را درون شبکه انتشار دهند که این مسأله ناقض حریم شخصی راننده است [۹].

- مشکلات :

این روش برای ممانعت از حمله‌ی سیبل ناکارآمد است. بدین ترتیب که یک مهاجم ممکن است چندین هویت غیر ثبت شده در شبکه برای خود بسازد. اما بعداً این هویت‌ها می‌توانند در شبکه ثبت‌نام شوند و مهاجم قادر خواهد بود که چندین گره‌ی سیبل ثبت‌نام شده داشته باشد.

۲. آزمون محاسباتی منبع :

این روش بیان می‌کند که اگر یک خودرو در حل کردن یا تمام کردن یک مسأله یا معما ناتوان باشد به عنوان یک گره‌ی جعلی در نظر گرفته می‌شود. در حملات سیبل مهاجم، گره‌های جعلی را می‌سازد که حافظه، محاسبات و منابع ارتباطی را با هم به اشتراک می‌گذارند. بنابراین به‌وسیلهٔ دنبال‌کردن و نظارت خودروهایی که از منابع به اشتراک گذاشته شده برای پردازش ارتباط و فرستادن پاسخ‌ها استفاده می‌کنند، می‌توان خودروهای متخلف را پیدا کرد [۱۰].

- مشکلات:

این روش نیازمند نظارت شدید و دنبال کردن پیام‌ها است که این، خود نیازمند وسایل طراحی شده‌ی خاصی می‌باشد. مکانیزم‌هایی که براساس آزمون منبع هستند در

[8] Resource Testing

واقع از حمله جلوگیری نمی‌کنند، درحقیقت هدف این مکانیزم‌ها خراب کردن حملات به‌وسیلهٔ محدودکردن هویت‌های تقلبی است. اما با توجه به این نکته که مهاجم می‌تواندشناسه‌های قانونی کافی به‌دست آورد (به‌وسیلهٔ به اشتراک گذاشتن یا دزدیدن)، امکان اینکه یک حمله‌ی موفق صورت گیرد بسیار زیاد می‌باشد. بنابراین این روش‌ها ممکن است نتوانند سطح امنیتی مناسبی در مقابل مهاجمان به‌دست آورند.

- تشخیص براساس موقعیت:

این روش‌ها براین اساس استوار هستند که خودرو در یک لحظه فقط در یک نقطه می‌تواند حضور داشته باشد. این تکنیک‌ها پیشنهاد می‌کنند تا از گره‌ها و مکانیزم‌های موقعیت محورگوناگونی برای جلوگیری از حمله‌ی سیبل استفاده شود. با توجه به توسعه‌ی گسترده در زمینه‌ی شبکه‌های بین خودرویی، که به‌خاطر نیازمندی‌های مختلف نظارت بر ترافیک استفاده می‌شوند، تشخیص بر اساس موقعیت برای اجرا، بسیار آسان شده است. اما برای مؤثر واقع شدن این برنامه‌ها در دنیای واقعی، اطلاعات موقعیتی باید حفاظت شده باشند. اگر این اطلاعات حفاظت شده نباشند مهاجم قادرخواهد بود که شبکه‌ی خودرویی را به‌وسیلهٔ حمله‌ی نفوذی تخریب کند.

- مکانیزم‌های برمبنای تصدیق‌کننده:

این روش‌ها شامل رویکردی برای شناسایی و موضع‌یابی گره‌های سیبل در شبکه‌های بین خودرویی هستند. این روش از مکانیزم‌های تصدیق‌کننده برای تأیید موقعیت ادعا شده به‌وسیلهٔ خودرو استفاده می‌کند. بدین طریق که از شدت سیگنال‌های دریافت‌شده‌ای که به‌وسیلهٔ خودروهای همسایه در یک دوره‌ی زمانی گرفته می‌شود استفاده می‌کنند و بعد آن‌ها را آنالیز می‌کنند تا موقعیت خودروی مدعی را حساب کنند [۱۱].

- تشخیص براساس RSSI:

این روش تخمینی از فاصلهٔ بین دو خودرو را با استفاده از شدت سیگنال دریافتی و مدل‌های نظری پخشی رادیویی، پیشنهاد می‌کنند. این رویکرد این روش را به یک روش کم هزینه برای سیستم‌های منحصر به سخت‌افزار تبدیل می‌کند [۱۲].

- مکانیزم شناسایی براساس کلید عمومی :

حمله‌ی سیبل می‌تواند با رویکرد رمزنگاری و تعیین اعتبار شناسایی شود. مکانیزم شناسایی براساس تعیین اعتبار خودروها از زیر ساخت کلید عمومی استفاده می‌کند. شناسایی حملات سیبل بر اساس این رویکرد نقطه‌ی اصلی بسیاری از تلاش‌های محققین بوده است. این موضوع قابل درک است که استفاده از مکانیزم‌های تعیین اعتبار و کلیدها بهترین وتنها رویکردی است که قادراست حملات سیبل را از بین ببرد. اما از آن‌جایی که زیرساخت کلید عمومی سنگین است و می‌تواند منجر به یک راه‌حل پیچیده گردد، برای به اجرا درآمدن دشوار خواهد بود [۱۳].

۳ روش تجمیع پیشنهادی

به‌دلیل طبیعت بسیار پویای شبکه‌های بین خودرویی، زمان همسایگی گره‌ها با یکدیگر به شدت با سرعت حرکت آن‌ها وابسته است. در این زمینه گره‌هایی که با سرعت نزدیک به هم حرکت می‌کنند مدت زمان بیشتری با یکدیگر همسایه هستند. تمرکز بر افزونگی منحصر به فرد شبکه‌های موردی بین خودرویی می‌تواند در تدوین پروتکل‌های مختلف برای کاربردهای مختلف این شبکه‌ها از جمله مقابله با نفوذ و کشف گره‌های نفوذگر درون شبکه استفاده گردد. همچنین استفاده از الگوریتم‌های مختلف جهت رمزگذاری و رمز گشایی داده‌های ارسالی از جمله راهکارهای تأمین امنیت در این شبکه‌ها است. لذا در روش پیشنهادی، از مکانیزم یارگیری برای احراز هویت گره‌های مطمئن درون شبکه استفاده می‌گردد. پس از یارگیری توسط گره‌های درون شبکه، بسته‌های ارسالی توسط هر گره باید توسط گره‌های تصدیق‌کننده‌ی گره‌ی اصلی تأیید گردد. تأیید بسته‌های ارسالی توسط کلید عمومی گره‌ها انجام می‌شود. در این راستا بسته ارسالی توسط گره‌ها نهایتاً با استفاده از کلید عمومی گره همراه و گره اصلی هش شده و درون شبکه انتشار می‌یابد. در ادامه نحوه‌ی یارگیری گره‌ها جهت تصدیق بسته‌های ارسالی و نحوه‌ی تبادل بسته‌ی اطلاعاتی بین گره‌ی اصلی و گره‌های همراه تشریح خواهد شد.

۱.۳ یارگیری گره‌ها

با توجه به تحرک زیاد خودروها با سرعت و مسیرهای حرکتی متفاوت، انتخاب گره‌های پشتیبان (گره‌های همراه جهت یارگیری گره‌ها) در شبکه‌های موردی بین خودویی چالشی اساسی برای محققین است. از طرفی تدوین پروتکل‌های مختلف برای این شبکه‌ها باید با کمترین تبادل داده‌های افزونه صورت گیرد. برای کاهش تبادل داده‌های افزونه الگوریتم پیشنهادی از راهکارهای زیر استفاده می‌کند:

۱. گره‌هایی که دارای مسیر حرکت یکسانی هستند، نیاز به تبادل داده کمتری نسبت به گره‌هایی که به تازگی در مسیر حرکت گره‌های اصلی قرار گرفته‌اند، دارند. لذا روش پیشنهادی از خودروهایی که به احتمال زیاد دارای مسیر و سرعت یکسانی با خودروی اصلی هستند به عنوان خودروی تصدیق‌کننده‌ی خودروی اصلی استفاده می‌نماید.

۲. فرایند یارگیری درون شبکه همواره تغییر می‌کند. این مسأله به دلیل تغییر مداوم گره‌های همسایه درون شبکه‌های بین خودرویی است.

برای یارگیری خودروها، روش پیشنهادی فرض می‌کند جدولی با عنوان جدول همسایه به صورت جدول در هر کدام از خودروها وجود دارد. از این جدول برای نگهداری اطلاعات خودروهای همسایه هر خودرو استفاده می‌شود. فیلدشناسه در جدول ۱ معرف شناسهٔ گره‌ی همسایه است و فیلد زمان نیز مشخص‌کننده‌ی زمان سپری شده از همسایگی دو گره را بیان می‌کند.

جدول ۱: ساختار جداول همسایه‌ی خودروها

Node. ID	Time	State	Re-Select
10	12.54	1	1
5	0	1	0
7	22	0	0

فیلد وضعیت (State)، وضعیت فعال یا غیرفعال بودن گره‌های همسایه را مشخص می‌کند. برای به‌روزرسانی جدول پشتیبان روند دستورالعمل های زیر باید طی شود:

۱. خودروها برای آگاهی از وضعیت همسایه‌های خود در بازه‌های زمانی مشخص، اقدام به ارسال پیام سلام [۹] برای همه‌ی همسایه‌های خود می‌کنند.

۲. قبل از ارسال پیام سلام توسط گره‌ها، هر گره مقدار فیلد حالت همه‌ی سطرهای جدول را صفر می‌کند.

۳. گره‌ها به محض دریافت پیام سلام، شناسهٔ خود را به عنوان پاسخ پیام دریافت شده به گره‌ی فرستنده پیام سلام ارسال می‌کنند.

۴. پس از جستجوی شناسهٔ گره‌ها در جدول پشتیبان، یکی از حالات زیر ممکن است رخ دهد:

- در اولین حالت ممکن است که شناسهٔ گره‌ی جدید درون جدول همسایگی وجود نداشته باشد. در این حالت گره‌ی دریافت‌کننده داده‌ی، شناسهٔ گره‌ی همسایه جدید خود را درون جدول همسایگی درج کرده و واضح است که زمان سپری شده از همسایگی گره‌ها نیز باید صفر شود. همچنین مقدار فیلد وضعیت گره نیز فعال یا یک لحاظ می‌شود.
- حالت بعدی، حالتی است که شناسهٔ گره قبلاً درون جدول همسایگی وجود داشته باشد و مقدار فیلد انتخاب مجدد گره نیز صفر باشد. در این حالت واضح است که تنها زمان سپری شده از همسایگی دو گره و فیلد وضعیت همسایگی گره از غیر فعال یا صفر به حالت فعال یا یک تغییر داده می‌شود و احتیاجی به تغییر مقدار فیلد انتخاب مجدد نیست.
- آخرین حالت، حالتی است که داده‌ای از طرف گره‌هایی که از قبل درون جدول همسایگی قرار داشته‌اند، دریافت نشده باشد. این مسأله ممکن است یا به دلیل عدم همسایگی گره با گره‌ی جاری رخ دهد و یا ممکن است به دلیل وقوع خطا در داده-های ارسالی، ارسال‌های ناموفق اتفاق افتاده باشد.

۵. در انتهای هر مرحله ۵، الگوریتم پیشنهادی سطرهایی از جدول همسایگی را که دارای فیلد حالت غیرفعال یا صفر هستند را حذف می‌کند.

[9] Hello Message

۶. جدول همسایگی به‌روزرسانی شده‌ی خودروها در اختیارایستگاه‌های پایه قرار می‌گیرد.

۲.۳ اختصاص کلید به گره ها

در روش پیشنهادی‌ایستگاه‌های پایه وظیفهٔ اختصاص کلید و شناسهٔ منحصر به فرد، به گره‌ها را بر عهده دارند. در این زمینه خودروها به محض عبور از مقابل یک‌ایستگاه پایه‌ی‌شناسه و کلید عمومی دریافت شده ازایستگاه پایه‌ی قبلی را در اختیارایستگاه پایه‌ی جدید قرار می‌دهند. در صورت معتبر بودن‌شناسه و کلید عمومی خودرو، ایستگاه پایه‌ی‌شناسه و کلید عمومی قبلی، گره را غیر فعال کرده و یک‌شناسه و کلید عمومی منحصر به فرد و جدید را برای خودرو ارسال می‌کند. لذا در روش پیشنهادی‌ایستگاه‌های پایه لازم است که ازشناسه‌ها و مقادیر کلید عمومی ایجاد شده مطلع گردند. بنابراین به محض ایجادشناسه و کلید عمومی جدید توسط هرایستگاه پایه، شناسه و کلید عمومی ایجاد شده در اختیارایستگاه پایه‌ی بعدی در طول مسیر نیز قرار داده می‌شود. همچنین در روش پیشنهادی ابطال‌شناسه و کلید عمومی قبلی نیز به‌ایستگاه پایه‌ی قبلی اطلاع داده می‌شود. بنابراین در روش پیشنهادی مقادیرشناسه و کلید عمومی گره‌ها دارای تاریخ انقضا هستند وایستگاه پایه بعدی در طول مسیر وظیفه ابطال پارامترهای فوق را بر عهده دارد.

۳.۳ کشف گره‌ی سیبل

به منظور شناسایی حملات سیبل روش پیشنهادی، در دو مرحله اقدام به کشف حملات سیبل درون شبکه می‌کند:

۱. انجام فرایند یارگیری به منظور انتخاب گره‌های تصدیق‌کننده برای هر گره.

۲. رمزگذاری بسته‌ها با هش کردن مقادیر کلید عمومی گره‌های تصدیق‌کننده و گره‌ی اصلی.

در روش پیشنهادی تنها از دو گره با بیشترین و کمترین زمان همسایگی گره‌ی اصلی به عنوان گره‌های تصدیق‌کننده استفاده می‌کند. بدیهی است هر چه تعداد گره‌های تصدیق‌کننده بیشتر باشد شناسایی گره‌های سیبل نیز آسان‌تر است. در روش پیشنهادی گره‌ی مبدا ابتدا بسته‌ی مورد نظر خود را ایجاد کرده و سپس کلید عمومی خود را با شناسهٔ منحصر به فرد خود هش کرده و برای گره‌ای با کمترین زمان همسایگی، ارسال می‌نماید. البته روند فوق می‌تواند بالعکس نیز باشد و گره‌ی مبدا، بسته را برای گره‌ای با بیشترین زمان همسایگی خود ارسال نماید. اولین گره‌ی تصدیق‌کننده در صورتی که بسته‌ی ارسالی مورد تأییدش باشد، کلید عمومی خود را با فیلد کلید عمومی سرآیند بسته هش کرده و شناسهٔ خود را نیز در سرآیند بسته درج می‌کند. سپس گره‌ی تصدیق‌کننده، بسته را برای گره‌ی تصدیق‌کننده‌ی بعدی ارسال می‌کند. گره‌ی تصدیق‌کننده‌ی بعدی نیز در صورت تأیید محتوای بسته، کلید عمومی خود را با فیلد کلید عمومی سرآیند بسته هش کرده، شناسهٔ خود را درون سرآیند بسته درج کرده و سپس بسته را درون شبکه منتشر می‌کند. ایستگاه پایه با شنود بسته‌های مبادله شده قادر به شناسایی گره‌های سیبل درون شبکه هستند. به طوری که گره-هایی که بدون گره‌ی تصدیق‌کننده اقدام به انتشار بسته درون شبکه نمایند، بر چسب گره‌ی سیبل

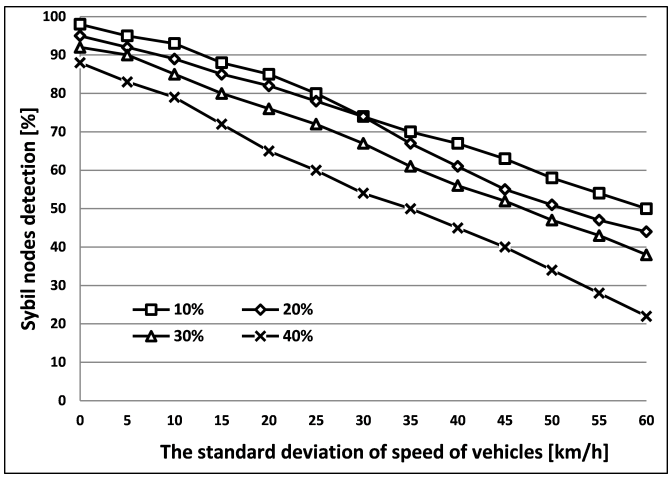
خورده می‌شوند. گره‌های برچسب خورده به عنوان گره‌ی سیبل با تحلیل جداول همسایگی توسط ایستگاه پایه، به عنوان گره‌ی سیبل تشخیص داده خواهند شد. ایستگاه‌های پایه با رصد جداول همسایگی گره‌ها نسبت به نظارت بر رفتار گره‌های بر چسب خورده، اقدام می‌نمایند. در صورتی‌که گره‌هایی که بر چسب گره‌ی سیبل خورده‌اند، دارای فعالیت مشکوک درون جداول همسایگی باشند، وجود گره‌ی سیبل درون شبکه حتمی است وایستگاه پایه گره‌ی فوق را به عنوان یک گره‌ی سیبل، درون شبکه معرفی می‌نماید.

۴ ارزیابی روش تجمیع پیشنهادی

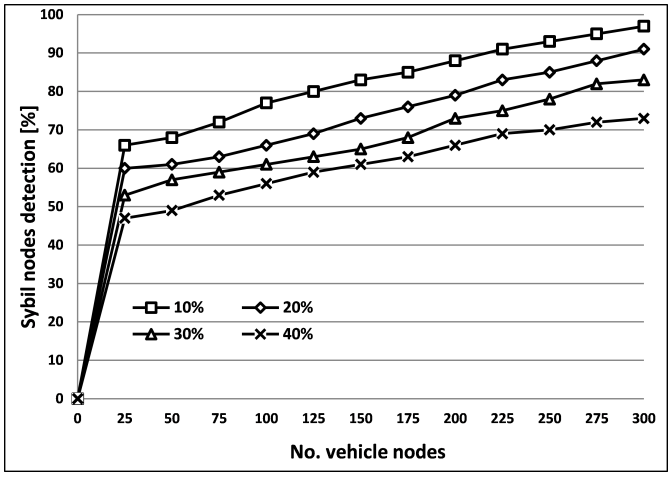
کارایی روش پیشنهادی با استفاده از شبیه‌ساز ns-۲ مورد ارزیابی قرار می‌گیرد. جهت پیاده‌سازی سناریوهای مختلف تعداد متغیری خودرو، در طول مسیری به طول ۲۰ کیلومتر در حال حرکت هستند. سرعت حرکت خودروها از ۴ متر بر ثانیه (تقریباً ۱۵ کیلومتر بر ساعت) تا ۳۳ متر بر ثانیه (تقریباً ۱۲۰ کیلومتر بر ساعت) متغیر است. سرعت حرکت خودروها برابر با حداکثر و حداقل سرعت در بیشتر کشورها است. همچنین عرض جاده‌ها نیز در سناریوهای مختلف متفاوت است.

شکل ۱ تأثیر انحراف معیار سرعت حرکت خودروها بر احتمال کشف گره‌های سیبل را نشان می‌دهد. افزایش انحراف معیار سرعت حرکت خودروها اختلاف سرعت حرکت خودروها در طول مسیر را نشان می‌دهد. مطابق با این شکل مشاهده می‌شود که با افزایش انحراف معیار سرعت حرکت خودروها، احتمال کشف گره‌های سیبل نیز کاهش می‌یابد. این مسأله بدین دلیل است که با افزایش انحراف معیار سرعت حرکت خودروها، هم‌بندی و وضعیت همسایگی گره‌ها به شدت تغییر می‌کند. تغییر مکرر وضعیت همسایگی گره‌ها منجر به کاهش صحت جداول همسایگی می‌گردد. شکل ۲ تأثیر چگالی طول مسیر حرکت خودروها بر احتمال کشف گره‌های سیبل را نشان می‌دهد. مطابق با این شکل مشاهده می‌شود که افزایش چگالی طول مسیر، احتمال کشف گره‌های سیبل را افزایش می‌دهد. این مسأله بدین دلیل است که همزمان با افزایش چگالی طول مسیر، انحراف معیار سرعت حرکت خودروها کاهش یافته و در نتیجه انتظار می‌رود که گره‌های تصدیق‌کننده تمامی بسته‌های ارسالی را تأیید یا عدم تأیید کنند. شکل ۳ تأثیر انحراف معیار سرعت حرکت خودروها بر درصد تحویل بسته به گره‌ها را نشان می‌دهد. مطابق با این شکل مشاهده می‌شود که افزایش انحراف معیار سرعت حرکت خودروها نرخ تحویل مطمئن داده به خودروها را کاهش می‌دهد. شکل ۴ تأثیر تعداد خودروهای طول مسیر بر نرخ تحویل داده به خودروها را نشان می‌دهد. مطابق با این شکل مشاهده می‌شود که با افزایش تعداد خودروهای طول مسیر نرخ تحویل بسته به گره‌ها افزایش می‌دهد. با توجه به اینکه افزایش چگالی شبکه منجر به کاهش انحراف معیار سرعت خودروها می‌گردد. لذا در این شکل مشاهده می‌شود که همزمان با افزایش تعداد خودروهای طول مسیر با افزایش مدت زمان همسایگی خودروها با یکدیگر، نرخ تحویل بسته به گره‌ها نیز افزایش می‌یابد. از طرفی مطابق با شکل ۵ افزایش چگالی یا تعداد خودروهای طول مسیر منجر به افزایش احتمال کشف گره‌های سیبل و در نتیجه بهبود کارایی روش پیشنهادی جهت ترافیک شبکه در روند ارسال بسته‌های مطمئن درون شبکه می‌گردد. بنابراین می‌توان نتیجه گرفت که روش پیشنهادی در شبکه‌های بین خودرویی چگال‌تر، کارایی مناسب‌تری دارد. شکل ۶ تأثیر انحراف معیار

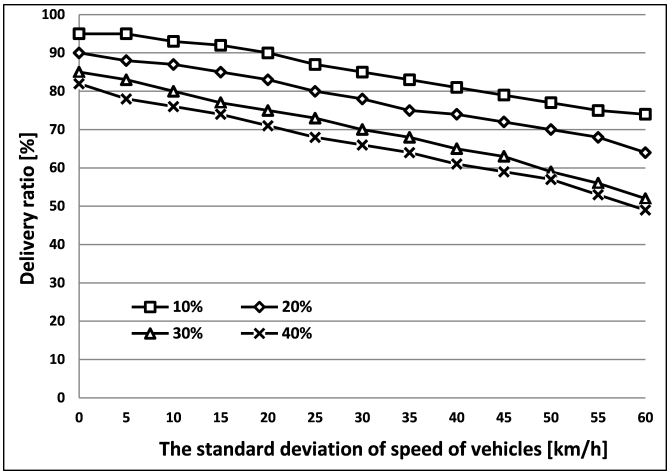
سرعت حرکت خودروها بر شناسایی مؤثر گره‌های سیبل توسط خودروها را نشان می‌دهد. کاهش صحت جدول همسایگی گره‌ها مهم‌ترین عامل کاهش پارامتر شناسایی مؤثر گره‌ها است. این مسأله بدین دلیل است که کارایی روش پیشنهادی به شدت بر عملکرد گره‌های تصدیق‌کننده و همراه گره‌ی اصلی وابسته است. لذا با تحرک بالای گره‌ها، گره‌های تصدیق‌کننده از همسایگی گره‌ی اصلی جدا شده و ممکن است برخی گره‌های سیبل داده‌ها را درون شبکه منتشر نموده و برخی گره‌های مطمئن نیز به دلیل عدم دریافت تأییدیه از گره‌های تصدیق‌کننده به عنوان گره‌ی سیبل در نظر گرفته شوند.



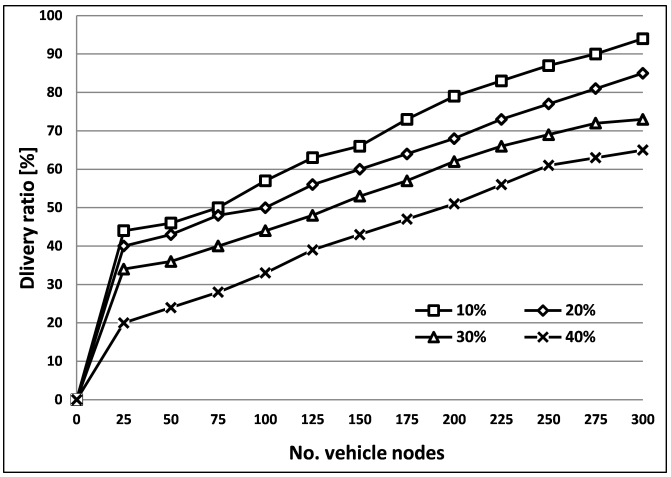
شکل ۱: تأثیر انحراف معیار سرعت حرکت خودروها بر درصد کشف گره‌های سیبل.



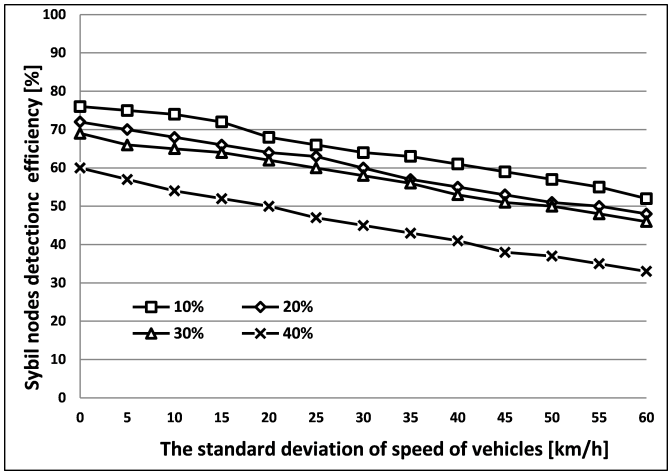
شکل ۲: تأثیر تعداد خودروهای طول مسیر بر احتمال کشف گره‌های سیبل.



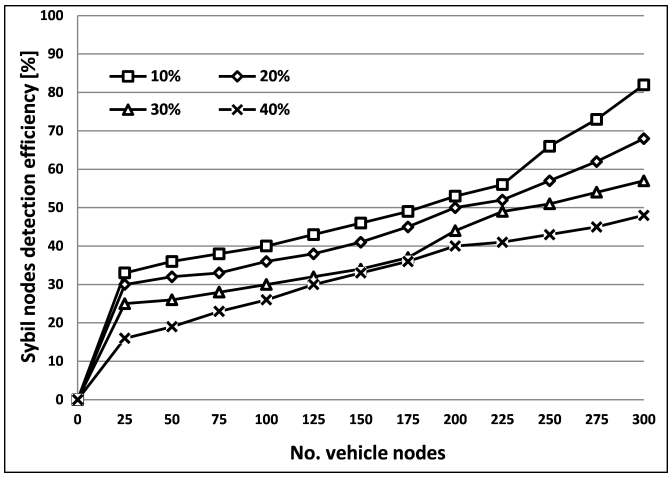
شکل ۳: تأثیر انحراف معیار سرعت حرکت خودروها بر نرخ تحویل بسته به خودروها.



شکل ۴: تأثیر تعداد خودروهای طول مسیر بر نرخ تحویل بسته به خودروها.



شکل ۵: تأثیر انحراف معیار سرعت حرکت خودروها بر شناسایی مؤثر گره‌های سیبل.



شکل ۶: تأثیر تعداد گره‌های طول مسیر بر شناسایی مؤثر گره‌های سیبل.

۵ نتیجه‌گیری

در این مقاله روشی کارا برای مقابله با حملات سیبل در شبکه‌های موردی بین خودرویی بر مبنای الگوریتم رمزنگاری کلید عمومی ارائه شد. روش پیشنهادی بر مبنای یارگیری گره‌ها جهت تصدیق هویت خود درون شبکه عمل می‌کنند. در این زمینه هر گره برای انتشار داده درون شبکه لازم است تأییدیه‌ی داده‌های فوق را از سایر گره‌های یار خود اخذ نماید. یارگیری گره‌ها بر مبنای جداولی تحت عنوان جداول همسایگی صورت می‌گیرد. در جدول همسایگی گره‌ها، اطلاعاتی همچون شناسهٔ گره و مدت زمان همسایگی گره‌ها با یکدیگر قابل حصول هستند. روش پیشنهادی، گره‌هایی با بیشترین احتمال داشتن مسیر یکسان را به عنوان گره‌های

یار انتخاب می‌نماید. لذا روش پیشنهادی یک جفت گره با کمترین زمان و بیشترین زمان همسایگی را به عنوان گره‌های یار لحاظ می‌کند. پس از یارگیری گره‌ها، هر گره برای ارسال داده لازم است که بسته را قبل از ارسال برای تأیید به گره‌های یار خود تحویل دهد. گره‌های یار در صورت تأیید بسته با هش کردن کلید عمومی خود در فیلد سرآیند بسته، اقدام به انتشار بسته درون شبکه می‌نماید. کلید عمومی هش شده در سرآیند بسته‌ها و تحلیل جداول همسایگی از جمله مهم‌ترین عوامل شناخت حملات سیبل در روش پیشنهادی هستند.

مراجع

[1] H. Yang, C. Pu, J. Wu, Y. Wu و Y. Xia, “Enhancing OLSR protocol in VANETs with multi-objective particle swarm optimization”, Physica A: Statistical Mechanics and its Applications, Volume 614, 2023.

[2] S. Monfared and S. Shokrollahi, “DARVAN: A fully decentralized anonymous and reliable routing for VANets”, Computer Networks, Volume 223, 2023.

[3] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. Mini and A. Loureiro, “Data communication in VANETs: Protocols, applications and challenges”, Ad Hoc Networks, volume 44, pp. 90-103, 2016.

[4] H. Hasrouny, A. Samhat, C. Bassil and A. Laouiti, “VANet security challenges and solutions: A survey”, Vehicular Communications, Volume 7, 2017.

[5] F. Sakiz and S. Sen, “A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV”, Ad Hoc Networks, volume 61, 2017.

[6] M. Arif, G. Wang, M. Bhuiyan, T. Wang and J. Chen, “A survey on security attacks in VANETs: Communication, applications and challenges”, Vehicular Communications, Volume 19, 2019.

[7] M. Baza, M. Nabil, M. Mahmoud and N. Bewermeier, “Detecting Sybil Attacks Using Proofs of Work and Location in VANETs”, IEEE Transactions on Dependable and Secure Computing, Volume 19, Number 1, 2022.

[8] B. Luo, X. Liu, and Q. Zhu, “Credibility Enhanced Temporal Graph Convolutional Network Based Sybil Attack Detection On Edge Computing Servers”, in IEEE Intelligent Vehicles Symposium (IV), 2021.

[9] G. Jethava and U. Rao, “User behavior-based and graph-based hybrid approach for detection of Sybil Attack in online social networks”, Computers and Electrical Engineering, volume 99, 2022.

[10] L. Xiao and L. Greenstein, “Channel-Based Detection of Sybil Attacks in Wireless Networks”, IEEE Transactions on Information Forensics and Security, Volume 4, 2009.

[11] A. Bhise and S. Kamble, “Review on Detection and Mitigation of Sybil Attack in the Network”, Procedia Computer Science, Volume 78, 2016.

[12] X. Li, Q. Lin and J. Mao, “Hybrid graph-based Sybil detection with user behavior patterns”, Procedia Computer Science, volume 178, 2021.

[13] C. Pu and K. Choo, “Lightweight Sybil Attack Detection in IoT based on Bloom Filter and Physical Unclonable Function”, Computers and Security, Volume 113, 2022.

تصویر مقصد ایران در اینستاگرام به روایت بلاگرهای غیرایرانی سفر

ندا رضوی‌زاده[۱]

[۱]استادیار جامعه‌شناسی گروه جامعه‌شناسی گردشگری، پژوهشکده گردشگری جهاد دانشگاهی، مشهد
n.razavi@gmail.com

چکیده

تحولات گسترده تکنولوژیک در زمینه اطلاعات و ارتباطات و پوشش جهانی اینترنت، دگرگونی‌های وسیعی در فناوری‌های رسانه‌ای، و در نتیجه در فنون بازاریابی محصولات و خدمات پدیده آورده است. صنعت گردشگری نیز از این تحولات برکنار نمانده است. یکی از مهم‌ترین کاربردهای رسانه‌های جدید مبتنی بر اینترنت، به‌ویژه شبکه‌های اجتماعی، شناسایی وضع موجود، تقویت، اصلاح و بهبود تصویر مقصد است. پژوهش حاضر با تحلیل محتوای پست‌های ۲۰ بلاگر سفر در پلتفرم اینستاگرام می‌کوشد به این پرسش پاسخ دهد که: وضعیت تصویر مقصد ایران در شبکه اجتماعی اینستاگرام چگونه است؟ یافته‌ها نشان داد از نظر شناختی، منابع و جامعه میزبان بیش از هر چیز توجه گردشگران را به خود جلب کرده است. از نظر عاطفی نیز همین مؤلفه‌ها واکنش مثبت گردشگران را برانگیخته است و سهم واکنش‌های عاطفی منفی و خنثی نسبت به واکنش‌های مثبت ناچیز است. همچنین از نظر رفتاری، گردشگران در بیش از نیمی از پست‌های خود، ایران را به‌عنوان مقصدی جذاب به سایرین توصیه کرده‌اند و در حدود ٪۴۰ پست‌ها به سفر مجدد به ایران تمایل نشان داده‌اند. این وضعیت تصویری مثبت از مقصد ایران را در اجتماع بلاگرهای سفر شبکه اجتماعی اینستاگرام نشان داد که تمایز واضحی با تصویر ایران در رسانه‌های جریان اصلی دارد. بنابراین بهبود تصویر ایران، مستلزم اتخاذ استراتژی‌هایی برای بازاریابی مقصد ایران است که به‌طور وسیع بر محتوای تولیدشده توسط کاربر و تبلیغات دهان به دهان الکترونیک متمرکز شود.

کلمات کلیدی: تصویر مقصد، اینستاگرام، بازاریابی مقصد، مدیریت مقصد، محتوای تولیدشده توسط کاربر و تبلیغات دهان به دهان الکترونیک.

۱ مقدمه

اگرچه پاندمی کووید-۱۹ در سال ۲۰۲۰ شوکی به این صنعت وارد کرد، اما بررسی روندها نشان می‌دهد پس از فروکش کردن کووید-۱۹ رشد گردشگری بار دیگر خیز برداشته است. طبق گزارش بارومتر گردشگری

جهانی منتشر شده توسط سازمان جهانی گردشگری [1] (۲۰۲۳) گردشگری بین‌المللی در سه ماهه اول ۲۰۲۳ نسبت به مدت مشابه سال گذشته ۸۶ درصد رشد داشته که نشان‌دهنده تداوم رشد گردشگری در ابتدای سال ۲۰۲۳ است. این رشد حاکی از آن است که ورود گردشگران بین‌المللی در سه ماهه اول سال ۲۰۲۳ به ۸۰ درصد سطوح قبل از همه‌گیری رسیده است، در حالی که در سال ۲۰۲۲، ۶۶ درصد نسبت به سال قبل بهبود یافته بود. در سال ۲۰۲۳ خاورمیانه قوی ترین عملکرد (۱۵ درصد رشد) را داشته و اولین منطقه جهانی است که اعداد پیش از همه‌گیری را در یک فصل کامل بازیابی می‌کند (همان).

افزایش گردشگران بین‌المللی بلافاصله پس از فرونشستن امواج سهمگین کووید-۱۹، نشان‌دهنده رقابت سرسخت مقاصد برای جذب گردشگران نیز هست. این رقابت در گام اول در زمینه بازاریابی محصولات گردشگری خود را نشان می‌دهد. یکی از رو به رشدترین روندهای بازاریابی که در گردشگری نیز به کار می‌رود، استفاده از اینترنت و شبکه‌های اجتماعی است. یک یافته مشترک پژوهش‌ها این است که تعامل با مصرف‌کنندگان و استفاده از رسانه اجتماعی برای بازاریابی محصولات توریستی یک راهبرد عالی اثبات شده است (چن و ژانگ [2]، ۲۰۱۵). تحلیل محتوای پژوهش‌ها همچنین آشکار کرده که رسانه اجتماعی اساساً شیوه جست‌وجو، یافتن، خواندن و اعتماد و نیز تولید همکارانه اطلاعات درباره تأمین‌کنندگان گردشگری و مقاصد گردشگری را در میان گردشگرها تغییر داده است (همان). رسانه اجتماعی در حال تغییر دادن بعضی فرایندهای موجود در صنعت گردشگری نیز هست، از جمله خدمات مصرف کنندگان، بازاریابی و ترویج در درون بخش گردشگری، تهیه روش‌های جدید سازمان‌های گردشگری و بازمهندسی و اجرای مدل‌های کسب و کار و عملیات، نظیر توسعه خدمات جدید، بازاریابی، شبکه‌سازی و مدیریت دانش (همان). طبق آمارهای موجود، در سال ۲۰۱۹ برای مثال ٪۴۷ از کل هزینه های تبلیغات جهانی سفر را تبلیغات دیجیتال تشکیل می‌دهد و ۱.۰۰۰.۰۰۰ هشتگ مرتبط با سفر به صورت هفتگی جستجو می‌شود. ٪۷۴ درصد از مسافران اظهار می‌کنند که در سفر از رسانه‌های اجتماعی استفاده می‌کنند و ٪۹۷ از گردشگران نسل هزاره گزارش می‌دهند که هنگام سفر عکس‌های خود را در رسانه‌های اجتماعی به اشتراک می‌گذارند. ٪۸۴ از این نسل می‌گویند که احتمالاً تعطیلات خود را بر اساس پست‌های اجتماعی دیگران برنامه‌ریزی می‌کنند (N.A, 2020).

ایران با وجود جاذبه‌های بسیار از جمله ۲۶ جاذبه طبیعی و فرهنگی و ۲ میراث فرهنگی ناملموس ثبت شده در میراث جهانی یونسکو و رتبه اول در رقابت قیمتی (کالدروود و ساشکین [3]، ۲۰۱۹) سهم کافی از گردشگری بین‌المللی به‌دست نیاورده است. شاهد این ادعا این است که درآمد ایران از محل گردشگری بین‌المللی به قدری است که تنها ٪۷٫۳ از تولید ناخالص داخلی از محل گردشگری ورودی تامین می شود، این در حالی است که سهم گردشگری در تولید ناخالص داخلی در ترکیه و امارات متحده عربی بیش از ٪۱۱، در خاورمیانه به‌طور میانگین نزدیک به ٪۹ و در جهان به‌طور میانگین ٪۱۰٫۳ است (نبوی و همکاران ۲۰۱۹). از این رو برای به‌دست آوردن سهم متناسب در بازار گردشگری بین‌المللی لازم است تلاش‌های فشرده و منسجم بازاریابی به‌ویژه از طریق اینترنت و شبکه‌های اجتماعی صورت گیرد. این امر پیش از هر

[1] UNWTO World Tourism Barometer
[2] Chen and Zhang
[3] Calderwood and Soshkin

چیز مستلزم شناخت وضعیت موجود تصویر ایران به‌عنوان مقصد گردشگری روی فضای آن‌لاین به‌عنوان یکی از مهم‌ترین فضاهای اطلاع‌رسانی در عصر حاضر است تا از این طریق برنامه‌ریزی برای تقویت نقاط قوت و اصلاح و بهبود نقاط ضعف تصویر ایران صورت گیرد. متاسفانه بعضی پژوهش‌ها نشان داده است که تصویر ایران، هویت رقابتی ایران و برند ایران در رسانه‌ها وضعیت مناسبی ندارد (محسنیان راد و عابدی، ۱۳۹۹، بیچرانلو، ۱۳۹۴، آنهولت، ۲۰۱۰). با توجه به اهمیت یافتن شبکه‌های اجتماعی در تصویرسازی، برندینگ و بازاریابی مقاصد، به ویژه اهمیت یافتن پلتفرم اینستاگرام در ارزیابی و اعتبارسنجی مقاصد توسط گردشگران (کاپاناکیس[۴]، ۲۰۲۰)، و اهمیت فزاینده آن در بازاریابی مقصد و محصولات گردشگری توسط کسب‌وکارهای گردشگری و سازمان‌های مدیریت مقاصد، پژوهش حاضر در صدد است تصویر ایران در شبکه اجتماعی اینستاگرام را بررسی کند. اینستاگرام از این رو انتخاب شده که چهارمین شبکه اجتماعی پرمخاطب و اولین شبکه اجتماعی پرمخاطب عکس شناخته می‌شود با نزدیک به ۳۸.۱ میلیارد کاربر در سراسر جهان (Statistica, 2023)[۵]. با این تفاصیل، پژوهش حاضر در صدد است به این پرسش پاسخ دهد که: وضعیت تصویر مقصد ایران در شبکه اجتماعی اینستاگرام چگونه است؟

۲ مرور ادبیات

۱.۲ تصویر مقصد

تصویر کشورها و مقاصد در ادبیات به صورت‌های مختلفی مفهوم‌سازی شده است. بسیاری از محققان تصویر مقصد را به عنوان بازنمایی ذهنی فرد از عقاید، احساسات و درک کلی از یک مقصد خاص تعریف می‌کنند (کرامپتون ۱۹۷۹؛ فیکیه و کرامپتون، ۱۹۹۱ به نقل از لی، لی و لی، ۲۰۰۵). بیرلی و مارتین (۲۰۰۴) در یک مطالعه تجربی کوشیدند مدلی را توسعه دهند و اعتبارسنجی کنند که عوامل تشکیل تصویر مقصد گردشگری را مشخص کند. آنها «تصویر ادراک شده مقصد» را شامل تصویر شناختی و احساسی تعریف کردند و نُه بعد برای تصویر ادراک شده در نظر گرفتند: منابع طبیعی، زیرساخت عمومی، زیرساخت توریستی، تفریحات و سرگرمی توریستی، فرهنگ، تاریخ و هنر، عامل‌های اقتصادی و سیاسی، محیط طبیعی، محیط اجتماعی و اتمسفر مکان. از نظر این محققان تصویر مقصد از دو منبع تأثیر می‌پذیرد: منابع اطلاعاتی (منابع اطلاعاتی دست دوم (القایی، بنیادین و مستقل)، منابع اطلاعاتی دست اول (تجربه قبلی، میزان بازدید)، عوامل فردی (انگیزه‌ها، تجربه سفر، خصوصیات اجتماعی-جمعیت‌شناختی).

۲.۲ محتوای تولید شده توسط کاربر(UGC) و بازاریابی دهان به دهان الکترونیکی (e-WOM)

امروزه آن چه گردشگران در رسانه‌های اجتماعی درباره یک مقصد گردشگری منتشر می‌شود، اعم از مشاهدات، تجارب و احساسات و رد و تاییدها، یکی از شکل‌دهنده‌های مهم تصویر مقصد است و به‌عنوان

[۴] Kopanakis
[۵] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users

محتوای تولید شده توسط کاربر (UGC)[۶] در بازاریابی دهان به دهان الکترونیکی (e-WOM)[۷] حائز اهمیت ویژه‌ای است (چو، دنگ و چنگ، ۲۰۲۰). رسانه‌های اجتماعی در هر مرحله سفر مورد رجوع گردشگران بالقوه و بالفعل هستند و از این رو آن چه آنها در این شبکه‌ها جست‌وجو می کنند یا نشر می‌دهند در ساخت افکار عمومی و تصویر مقصد مؤثر است. برای مثال پیکازو و مورنو گیل[۸] (۲۰۱۹) طی یک مرور نظام‌مند در می‌یابند که پیش، حین و پس از سفر مصرف‌کنندگان به چه قصدی به شبکه‌های اجتماعی رجوع می‌کنند، و تأمین‌کنندگان خدمات گردشگری نیز در بخش‌های مختلف بازاریابی محصول خود از این ابزار بهره می‌جویند. مثلاً در مرحله پیش از سفر، نیاز به تأیید، جستجوی اطلاعات و ... محرک است، حین سفر برای ارزیابی آلترناتیوها، تصمیم خرید از رسانه اجتماعی استفاده می‌کنند، تأمین کنندگان خدمات گردشگری برای ترویج[۹] محصول خود از ظرفیت رسانه‌های اجتماعی برای دسترسی به مخاطب جهانی، انتشار اطلاعات ترویجی، تقویت نیروهای بازاریابی شرکت استفاده می‌کنند، برای توزیع محصول، ارتباطات، مدیریت و تحقیقات نیز از آن بهره می‌برند.

۳.۲ نظریه بازنمایی

معنا بخشیدن به چیزها از طریق فرایند بازنمایی صورت می‌گیرد. آراء و رویکردهای مختلفی در نسبت بازنمایی و واقعیت خارجی وجود دارد: رهیافت بازتابی، نیت‌گرا و سازه‌انگار (هال، ۱۳۹۱ : ۳۲). رهیافت بازتابی زبان را وسیله‌ای می‌داند که معنای موجود در چیزها، انسان‌ها و رویدادهای جهان را منعکس می‌کند. رهیافت نیت‌گرا بر آن است که زبان فقط چیزی را منتقل می کند که مؤلف، گوینده یا تصویرگر می‌خواهد بیان کند. رهیافت سازه‌انگار معتقد است معنا در زبان و از طریق زبان برساخته می‌شود (هال، ۱۳۹۱: ۳۲).

بر مبنای آن چه گذشت، چنان که هال (۱۳۹۱) استدلال می‌کند رسانه‌ها به‌جای آن که معناهای موجود را منتقل کنند، واقعیت را گزینش، تعریف، بازتولید و مجدداً صورت‌بندی می کنند و به آن معنا می‌بخشند. این واقعیت‌های بازنمایی شده همچون عین واقعیت انگاشته می‌شوند. این دیدگاه به‌خوبی با رویکرد موضوعی این پژوهش سازگار است از این رو که مفروض ما این است که تصمیم گردشگران در خرید محصولات گردشگری تا حد زیادی متأثر از تصویری است که به واسطه رسانه‌ها در ذهن آن ها شکل می‌گیرد. این رسانه‌ها ممکن است رسانه‌های رسمی باشند یا آن چه از طریق کاربران ظاهراً عادی در صفحات شبکه‌های اجتماعی‌شان نشر می یابد (UGT) و بازتاب نگاه و تجربه ایشان است . در چارچوب رویکرد سازه‌انگار، این بیان‌ها و توصیفات از مقصد، سازنده معنای مقصد در نظر مخاطبان خواهد بود.

[6] User Generated Content
[7] Electronic word of mouth
[8] Picazo and Moreno-Gil
[9] Promotion

منابع	زیرساخت ها	محیط	مردم
• فرهنگ و منابع میراثی • منابع طبیعی • تفریحات و سرگرمی	• حمل و نقل • ICT • مبادلات مالی • ویزا و مسایل حقوقی • خدمات تجاری گردشگری	• امنیت • ایمنی • بهداشت	کارکنان صنعت گردشگری • جامعه میزبان • سن • جنسیت • ملیت

شکل ۱: مدل مفهومی پژوهش برای تصویر مقصد ایران

۴.۲ مدل مفهومی

با تلفیق شاخص‌های رقابت‌پذیری سفر و گردشگری مجمع جهانی اقتصاد (کالدروود و ساشکین، ۲۰۱۹) و مهم‌ترین ابعاد و ویژگی های به کار رفته در مقالات پیشین بر اساس مرور نظام‌مند دو دهه تحقیقات اخیر (پیکازو و مورنو-گیل، ۲۰۱۷)، تصویر مقصد در چهار بعد اصلی مطابق شکل ۱ در این پژوهش بررسی خواهد شد.

۳ روش تحقیق

این پژوهش اساساً به روش تحلیل محتوای کمی انجام شد. متون ذیلِ مدلِ مفهومیِ پیش‌گفته کدگذاری شد. روش تحلیل محتوای کمی، از آن رو انتخاب شد که استنباطی تکرارپذیر و معتبر از داده‌ها به‌دست می‌دهد.

برای تحلیل تصاویر اینستاگرام، ۲۰ اکانت (پیج) بلاگر بین‌المللی توریسم که حاوی تصاویر ایران و انگلیسی زبان باشند انتخاب شد. از هر پیج حداقل ۱۰ تصویر مرتبط با سفر به ایران (به صورت تمام‌شماری در صورتی که کمتر یا مساوی با ۱۰ تصویر در پیج بوده است، و نمونه‌گیری تصادفی از بین کل تصاویر مرتبط با سفر به ایران در صورتی که بیش از ۱۰ تصویر وجود داشته است) انتخاب و تحلیل محتوا شد. تحلیل تصاویر اینستاگرام همراه با رجوع به محتوای کپشن برای تأمین روایی بیشتر کدگذاری‌ها انجام شد. کپشن‌ها ابتدا ترجمه و سپس کد گذاری شدند.

برای تأمین روایی از راهنمای تحلیل محتوای نئوندورف (۱۳۹۵: ۱۳۷) استفاده شد. روایی صوری[10] با بررسی شاخص‌ها و تحلیل مفهومی آنها، ربط مفهومی شاخص‌ها با موضوع تحقیق مشخص شد. برای سنجش پایایی از دو کدگذار استفاده شد و توافق نسبی به روش هولستی (نئوندورف، ۱۳۹۵: ۱۵۲) محاسبه شد. در تحلیل محتوای پلتفرم اینستاگرام، ضریب پایایی ۰٫۸۳ به‌دست آمد که که میزان بالا و قابل قبولی است و نشانگر توافق بالای میان کدگذاران و به‌تبع عینیت شاخص‌بندی محتوای ثبت شده است.

[10] Face validity

جدول ۱: ویژگی‌های بلاگرهای اکانت های بررسی شده در اینستاگرام

جنسیت کاربران	رده سنی کاربران	ملیت بلاگرها
۱۶ بلاگر زن	رده سنی جوان	۱۶ مورد از کشورهای اروپایی
۲ بلاگر مرد		۳ مورد آمریکا
۲ مورد زوج		۲ مورد کشورهای آسیایی
		۱ مورد استرالیا
		۱ مورد کشورهای آفریقایی

جدول ۲: فراوانی ابعاد تصویر ایران

ابعاد	جمع	درصد
منابع	۱۵۵	۵۴
زیرساخت	۴۵	۱۶
محیط	۷	۲
جامعه میزبان	۸۰	۲۸
جمع کل	۲۸۷	۱۰۰

۴ یافته ها

در شبکه اجتماعی اینستاگرام ۲۰ صفحه متعلق به بلاگرهای گردشگری با بیشترین میزان بازدیدکننده انتخاب گردید که از این ۲۰ صفحه، ۱۸۰ پست متنی به همراه عکس آن تحلیل شده است. در جدول ۱ ویژگی‌های بلاگرهای صفحه‌های تحلیل شده از اینستاگرام گزارش شده است.

در این پژوهش تصویر مقصد گردشگری ایران در شبکه اجتماعی اینستاگرام در قالب ۳ بعد ذیل مورد بررسی و تحلیل قرار گرفت: بعد شناختی، بعد عاطفی یا احساسی و بعد رفتاری. در ادامه توصیف این ابعاد ارائه می شود.

۱.۴ بعد شناختی تصویر ایران

از آنجایی که برای هر پست بیش از یک کد ثبت شده است و برای هر کد مشخصات کاربر آن تکرار شده است، لذا در جدول ۲ تعداد فراوانی محاسبه شده بیش از تعداد کاربران اصلی است که در این بخش تحلیل شده است.

با توجه به تنوع و اهمیت منابع در جذب گردشگران، این بعد با جزییات بیشتری بررسی شد. منابع گردشگری ایران در قالب جاذبه‌های طبیعی، جاذبه‌های تاریخی، فرهنگی و مذهبی، جاذبه‌های تفریحی، رویدادهای فرهنگی – مذهبی، رسوم، جشن‌ها، موسیقی، دانش بومی (میراث ناملموس)، صنایع دستی و اقلیم و پوشش گیاهی و جانوری بررسی شد و فروانی اشاره به این منابع در پست‌های بررسی شده به شرح

جدول ۳: توزیع فراوانی مقولات منابع گردشگری در اینستاگرام

ابعاد	فراوانی	درصد
جاذبه های طبیعی	۳۲	۲۱
اقلیم و پوشش گیاهی و جانوری	۳	۲
جاذبه های تاریخی، فرهنگی و مذهبی	۱۰۸	۶۹
رویدادهای فرهنگی – مذهبی (میراث ناملموس)	۷	۵
صنایع دستی	۵	۳
تفریحات و سرگرمی	۰	۰
جمع کل	۱۵۶	۱۰۰

جدول ۳ است.

در پست‌های تحلیل شده بیش از همه (۶۹ درصد) به جاذبه‌های تاریخی، فرهنگی و مذهبی ایران اشاره شده است. در ۲ درصد از پست‌ها به جاذبه‌های طبیعی پرداخته شده است. همان‌طور که مشاهده می‌شود سهم رویدادهای فرهنگی–مذهبی، اقلیم و پوشش گیاهی و جانوری و صنایع دستی مجموعا ۱۰ درصد از کل محتوای مورد بررسی بوده است.

۲.۴ بعد عاطفی تصویر ایران

در پست‌های بررسی شده، واکنش عاطفی مؤلف نسبت به ابعاد تصویر ایران بررسی شد. برای این منظور، احساسات افراد نسبت به مقصد در قالب مطلوب، نامطلوب یا خنثی (در قالب صفاتی چون) تحریک‌کننده – کسل‌کننده؛ خوشایند – ناخوشایند؛ هیجان‌انگیز – غم‌انگیز؛ و آرامش‌بخش – ناراحت‌کننده بررسی شد.

جدول ۴ سهم هر یک از واکنش های مثبت، منفی و خنثی به این ابعاد مشاهده می شود.

اکثریت پستهای تحلیل شده همراه با بار احساسی مثبت بوده است، این موضوع به ویژه در ارتباط با منابع و جامعه میزبان بیشتر به چشم می خورد. در مجموع ۲۹ پست دارای بار احساسی منفی بوده است که عمدتا به زیرساخت های گردشگری ایران مربوط بوده است.

۳.۴ بعد رفتاری تصویر ایران

برای واکاوی واکنش مولفان پست ها در بعد رفتاری، تمایل گردشگر برای بازدید مجدد از مقصد یا توصیه آن به اطرافیانش در این پست ها بررسی شد.

داده های مندرج در جدول ۵ نشان می دهد که در ۱۷ پست، گردشگران بازدید از ایران و جاذبه‌های آن را به مخاطبان خود توصیه کردهاند (۵۹ درصد). همچنین در ۱۲ پست به این امر اذعان داشته اند که به ایران برمی‌گردد و یا تجربه گردشگری خاصی مانند بازدید از جاذبه یا صرف غذای ایرانی را دوباره تکرار خواهند کرد. اغلب گردشگران با جملاتی چون «عاشق آن شدم» و «مجذوب آن شدم»، «همیشه دلتنگ تو

جدول ۴: ابعاد تصویر ایران بر حسب جهت‌گیری عاطفی آن

ابعاد	منفی	خنثی	مثبت	جمع کل
منابع	۴ ۲٫۶۰٪	۱۶ ۱۰٫۳۰٪	۱۳۵ ۸۷٫۱۰٪	۱۵۵ ۱۰۰٫۰۰٪
زیرساخت	۱۵ ۳۳٫۳۰٪	۵ ۱۱٫۱۰٪	۲۵ ۵۵٫۶۰٪	۴۵ ۱۰۰٫۰۰٪
محیط	۵ ۷۱٫۴۰٪	۰ ۰٫۰۰٪	۲ ۲۸٫۶۰٪	۷ ۱۰۰٫۰۰٪
جامعه	۵	۱۳	۶۲	۸۰
میزبان	۶٫۳۰٪	۱۶٫۳۰٪	۷۷٫۵۰٪	۱۰۰٫۰۰٪
جمع کل	۲۹	۳۴	۲۲۴	۲۸۷

جدول ۵: توزیع فراوانی بعد رفتاری گردشگری در اینستاگرام

ابعاد	فراوانی	درصد
تمایل به بازدید مجدد	۱۲	۴۱
توصیه مقصد به دیگران	۱۷	۵۹
جمع کل	۲۹	۱۰۰

هستم» از شیفتگی خود نسبت به ایران صحبت کرده‌اند. همچنین گردشگران اظهار داشته‌اند که ایران از معدود کشورهایی است که قطعاً دوباره به آن باز خواهند گشت.

۵ نتیجه‌گیری

امروزه جهان با افزایش تقاضای گردشگری مواجه است و ایران هنوز سهم خود را قدری که لایق آن است به‌دست نیاورده است. ایران برای عقب نماندن از قافله ای که به‌سرعت در این منطقه در حال حرکت به سمت جذب گردشگر بین‌المللی بیشتر است لازم است اقدامات مختلفی را مد نظر قرار دهد، هم اقداماتی درباره توسعه محصول و هم استفاده از فرصت‌های آنلاین برای ترویج محصول خود. همچین امروزه با طیف متفاوتی از گردشگران مواجه هستیم که تحصیلات بالاتر دارند، با تجربه‌ترند و سخت‌تر راضی می‌شوند (کتر و گودال، ۱۹۹۲؛ دلیور، ۱۹۹۶ به نقل از دیلیپ، ۱۳۹۵). آن ها مجهز به مهارت‌ها، تکنولوژی و رسانه هستند و چنان که دیلیپ (۱۳۹۵) می‌گوید گردشگری جدید صرفاً تحت تأثیر عوامل اقتصادی نیست، عوامل فرهنگی و نسل جدید گردشگران موجب تغییرات ژرفی شده است. بنابراین باید بازاریابی گردشگری نیز متناسب با این مصرف‌کنندگان باید متحول شود.

در این پژوهش تصویر مقصد گردشگری ایران در شبکه‌های اجتماعی اینستاگرام در سه بعد شناختی، احساسی و رفتاری تحلیل محتوا شد. از شبکه اجتماعی اینستاگرام مجموعاً ۱۸۰ پست از ۲۰ اکانت متعلق به پرمخاطب‌ترین بلاگرهای گردشگری تحلیل گردید.

طبق یافته‌ها، از نظر شناختی، منابع و جامعه میزبان بیش از هر چیز توجه گردشگران را به خود جلب کرده است. از نظر عاطفی نیز همین مؤلفه‌ها واکنش مثبت گردشگران را برانگیخته است. همچنین از نظر رفتاری، گردشگران در بیش از نیمی از پست‌های خود، ایران را به عنوان مقصدی جذاب به سایرین توصیه کرده‌اند و در حدود ٪۴۰ پست‌ها به سفر مجدد به ایران تمایل نشان داده‌اند. این وضعیت نشان می‌دهد تمایز واضحی بین تصویر ایران، هویت رقابتی ایران و برند ایران در رسانه‌های جریان اصلی (محسنیان راد و عابدی، ۱۳۹۹، بیچرانلو، ۱۳۹۴، آنهولت، ۲۰۱۰) و محتوای تولیدشده توسط بلاگرهای سفر روی شبکه‌های اجتماعی وجود دارد و برای بهبود تصویر ایران، استراتژی‌های بازاریابی مقصد لازم است بیش از پیش بر محتوای تولید شده توسط کاربر و تبلیغات دهان به دهان متمرکز شود.

یافته های این پژوهش بار دیگر نشان داد فضای بازاریابی گردشگری جهان به‌شدت متکی بر پلتفرم‌های دیجیتال و به‌خصوص محتوای تولید شده توسط کاربر (UGC) است. بنابراین مهم‌ترین و اولین گام در دیجیتال کردن خدمات توریستی و ترویج توریسم (به‌عنوان جزئی از فرایند بازاریابی محصولات توریستی ایران، و بلکه ابزار ضروری آن در دنیای معاصر)، مستلزم دسترسی پایدار و امن و آزاد به اینترنت پرسرعت جهانی است. اینترنت کم کیفیت، بسیار کم سرعت، ناپایدار، فیلترشده و گاه فاقد دسترسی به اینترنت جهانی، هم کسب‌وکارهای گردشگری را در زمینه تبلیغات و خدمت‌رسانی با مشکلات عدیده مواجه می‌کند، هم هراس در دل گردشگران بالقوه می‌اندازد و هم تجربه‌ای بسیار منفی برای گردشگرانی که در این مقطع در ایران بوده‌اند ایجاد می‌کند. امروزه فروش محصولات گردشگری بیش از هر زمان دیگری و بیش از هر محصول

دیگری وابسته به اینترنت است، زیرا محصول گردشگری را نمی‌توان خارج از مقصد تجربه و بازدید و برانداز و ارزیابی کرد.

علاوه بر این، چنان که پژوهش نشان داد بلاگرهای مشهور و بین‌المللی سفر و گردشگری این ظرفیت را دارند که به طور فعالانه گردشگری ایران را به مخاطبان پرشمار خود معرفی کنند. استفاده از این ظرفیت با دعوت از آنها در قالب کمپین‌ها و تورهای آشناسازی (فم تریپ)، دعوت از روزنامه‌نگاران، نویسندگان زبده و سرشناس، تورگردانان برای تولید محتوا و انتشار خبر از رویدادهای فرهنگی، ورزشی و گردشگری جذاب در ایران لازم است در برنامه‌ریزی ها در نظر گرفته شود. تأمین امنیت و آزادی این چهره‌ها برای تهیه گزارش باید بخشی از برنامه بازاریابی مقصد ایران توسط سازمان مدیریت مقصد (وزارت میراث فرهنگی، گردشگری و صنایع دستی) باشد. همچنین لازم است از رسانه‌های معتبر جهانی برای بازاریابی گردشگری ایران استفاده شود. برای مثال، عربستان سعودی برای بازاریابی مقصدی به نام «العلا» نه‌تنها صفحات رسمی در شبکه‌های اجتماعی راه‌اندازی کرده بلکه ویدیوهای تبلیغاتی آن را در صفحه رسانه‌های طراز اول گردشگری چون National Geography پخش می‌کند. سیاست‌های تشویقی برای بازاریابی مشارکتی مقصد ایران توسط کسب‌وکارها نیز می‌تواند مؤثر باشد. به‌علاوه، بازاریابی ویروسی در سطح پلتفرم‌های شبکه‌های اجتماعی یک شیوه مهم ترویج یک مقصد است که لازم است وزارت میراث فرهنگی، گردشگری و صنایع دستی به‌عنوان سازمان مدیریت مقصد سرمایه‌گذاری و مشارکت فعالانه در تولید چنین محتواهایی داشته باشد.

سپاس‌گزاری

بدین‌وسیله از همکاری سرکار خانم زهرا بستان در تحلیل داده‌ها سپاسگزاری می‌شود.

مراجع

[۱] دیلیپ، ام. آر (۱۳۹۵). بازاریابی بین‌الملل در گردشگری. (ا. تاج‌زاده نمین، ز. میرزاآقا، مترجم) تهران: مهکامه.

[۲] محسنیان راد، مهدی و عابدی (۱۳۹۹). حمید بازنمایی برند ملی ایران در عکس‌های خبرگزاری آسوشیتدپرس. فصلنامه انجمن ایرانی مطالعات فرهنگی و ارتباطات. ۱۶ (۵۹): ۳۱۱-۳۵۱.

[۳] نئوندورف، کیمبرلی ای. (۱۳۹۵). راهنمای تحلیل محتوا. حامد بخشی و جیهه جلائیان بخشنده، مترجم. مشهد: انتشارات جهاد دانشگاهی واحد مشهد.

[۴] هال، استیوئرت (۱۳۹۱). معنا، فرهنگ و زندگی اجتماعی. احمد گل محمدی مترجم. تهران: نشر نی.

[5] Anholt, Simon (2010). PLACES: Identity, Image and Reputation. PALGRAVE MACMILLAN.

[6] Beerli, Asunciòn, Martín, Josefa D. (2004). Factors influencing destination image, Annals of Tourism Research, 31 (3): 657-681.

[7] Calderwood, Lauren Uppink and Soshkin, Maksim (2019).The Travel and Tourism Competitiveness Report 2019. Geneva: World Economic Forum.

[8] Chu, S. C., Deng, T., and Cheng, H. (2020). The role of social media advertising in hospitality, tourism and travel: a literature review and research agenda. International Journal of Contemporary Hospitality Management. [First Published Online.]

[9] Kopanakis, John (2020). How Social Media Analytics Impacts Travel and Tourism Industry. Accessed: https://www.mentionlytics.com/blog/how-social-media-analytics-impacts-travel-and-tourism-industry/

[10] Lee, Choong-Ki, Lee,Yong-Ki, Lee, BongKoo (2005). Korea's destination image formed by the 2002 World Cup, Annals of Tourism Research, 32(4): 839-858.

[11] N. A (2020). 25 Travel And Tourism Statistics That You Need To Know Accessed : https://www.socialtoaster.com/travel-tourism-statistics/

[12] Nabavi, S. Hossein, HOSSEINIFAR, HODA, EBRAHIMZADEH, AMIR and TORKABADI, AMIRHOSSEIN (2019). Iran Travel and Tourism Industry current status and opportunities. ILIA CORPORATON. Accessed: https://ilia-corporation.com/wp-content/uploads2022/04/Travel-and-Tourism-Industry-Iran-ILIA-CorporationWhite-Paper-c-Pub-1.pdf

[13] Picazo, P., and Moreno-Gil, S. (2019). Analysis of the projected image of tourism destinations on photographs: a literature review to prepare for the future. Journal of Vacation Marketing, 25(1), 3-24.

[14] Statistica (2023) Most popular social networks worldwide as of January 2023, ranked by number of monthly active users. Accessed: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[15] UNWTO World Tourism Barometer (2023), World Tourism Organization May 2023. Volume 21, Issue 2. Accessed:https://webunwto.s3.eu-west-1.amazonaws.com/s3fs-public/2023-05/UNWTO_Barom23_02_May_EXCERPT_final.pdf?VersionId=gGmuSXlwfM1yoemsRrBI9ZJf.Vmc9gYD

ارتقای امنیت سیستم بانکی با استفاده از فناوری بلاک‌چین و رایانش ابری

رضا مدنی [۱]

[۱] دانشجوی کارشناسی ارشد، مهندسی فناوری اطلاعات، دانشگاه پیام نور، تهران، ایران
rezamellat2005@gmail.com

چکیده

با توجه به حملات و تهدیدات امنیتی سیستم‌های بانکی و حریم خصوصی کاربران، استفاده از سرورهای متمرکز می‌تواند عاملی برای از دست دادن یا تحریف داده‌ها توسط مهاجمین باشد. بلاک‌چین یک دفتر غیرمتمرکز، توزیع‌شده و تغییرناپذیر دیجیتال است که معاملات را در یک شبکه جهانی رایانه‌ای ثبت می‌کند که اطلاعات از امنیت بالایی برخوردار هستند. از آنجا که ادغام آن با دامنه‌های دیگر مسائل مرتبط زیادی را حل کرده است، امکان حل مسائل مربوط به حریم خصوصی و امنیت در حوزه سیستم‌های بانکی وجود دارد. از بلاک‌چین به عنوان تأمین کننده‌ی امنیت و یکپارچگی فناوری‌هایی نظیر رایانش ابری استفاده می‌شود. بنابراین، استفاده از بلاک‌چین در حوزه رایانش ابری دامنه جدیدی از تحقیقات را به‌وجود می‌آورد. در این تحقیق ابتدا مفاهیم بلاک‌چین و رایانش ابری بررسی می‌شوند. سپس بلاک‌چین به‌عنوان خدماتی برای ارتقای امنیت سیستم بانکی در بستر رایانش ابری ارائه می‌شود تا نشان دهد چگونه می‌توان از ویژگی‌های مختلف فناوری بلاک‌چین و رایانش ابری به‌عنوان خدماتی برای امنیت سیستم بانکی استفاده نمود.

کلمات کلیدی: امنیت، سیستم بانکی، بلاک‌چین، رایانش ابری.

۱ مقدمه

بیشتر فناوری‌های نوظهور و پرکاربرد از سرورهای متمرکز استفاده می‌کنند که این سرورها همواره در خطر حملات مهاجمین و حتی خطرات طبیعی می‌باشند به گونه‌ای که اگر فرد مهاجم به اطلاعات سرور دست پیدا کند امکان جعل، دستکاری و حتی حذف داده‌های سرور وجود دارد و همچنین این گونه سرورها به نظارت و مدیریت شخص ثالث نیازمند هستند، اما در سال ۲۰۰۹ توسط ناکاموتو سروری غیر متمرکز برای بستر ارز دیجیتال بیت کوین، به نام بلاک‌چین معرفی گردید. این شبکه با توجه به اینکه از سرورهای توزیع شده و غیر متمرکز استفاده می‌کند امکان جعل، دستکاری و حذف داده‌ها را به حداقل می‌رساند و همچنین ماندگاری، محرمانگی و مقیاس پذیری را برای داده‌ها فراهم میکند. بلاک‌چین با توجه به اینکه در ایجاد بلوک‌های

جدید و فرآیندهای محاسباتی سرعت کمتری نسبت به رایانش ابری و اینترنت اشیا دارد، این فرضیه پیش آمد که به زودی از چرخه رقابت حذف خواهد شد، اما امتیاز ایجاد سرورهای غیر متمرکز در این شبکه و خلق امنیت داده برای کاربران، محققین را بر آن داشت تا از این شبکه جذاب برای ایجاد امنیت در فناوری‌هایی نظیر اینترنت اشیا که به دلیل داشتن دستگاه‌های متعدد و سرعت عملیاتی بسیار بالا قادر به ایجاد امنیت و حفظ حریم خصوصی نیستند استفاده شود. بلاک‌چین همانند تمامی طرح‌ها و فناوری‌های نوظهور دارای نواقصی می‌باشد از جمله فضای ذخیره سازی کم بلوک‌ها و زمان نسبتا زیاد ایجاد یک بلوک در زنجیره که باید با بررسی‌ها و ارائه الگوهای مناسب این ایراد رفع گردد و همچنین خلاهای امنیتی که در اجرا و بکارگیری بلاک‌چین در زمینه‌های مختلف مشخص می‌شود، پوشش داده شود [۱].

با گسترش فضای مجازی و ایجاد پلتفرم‌ها و شبکه‌های بانکی ارائه خدمات به کاربران و ارسال حجم انبوهی از داده‌ها به این فضا مهم‌ترین ویژگی که باید به آن توجه داشت ایجاد امنیت داده و حفاظت از حریم خصوصی کاربران است. زمانی‌که حجم گسترده‌ای از اطلاعات در یک پایگاه داده یا سرور ذخیره شود برای مهاجمین بسیار جذاب می‌باشد که به این منبع نفوذ کرده و با استفاده از داده‌های شخصی کاربران، منفعتی را کسب نمایند یا موجب اختلال در سرویس‌دهی سیستم به کاربران شوند. با توجه به اینکه استفاده از الگوریتم‌های رمزنگاری برای ورود به سرورهای اطلاعاتی، راهی کاملا امن برای حفاظت از داده‌ها نبود و معرفی سرور غیر متمرکز بلاک‌چین برای ذخیره سازی اطلاعات مهم در سال های اخیر انجام شد بایستی روش‌هایی ایجاد شود که به جای استفاده از سرورهای سنتی از سرورهای توزیع‌پذیر بهره برده شود تا با حمله یا نفوذ به یک منبع، اطلاعات به کلی از بین نرود [۲]. برای درک بهتر این موضوع مثالی مطرح میشود که اگر عکسی در یک تلفن همراه ذخیره گردد و این عکس به هر دلیلی از دستگاه حذف شود دیگر امکان دسترسی به آن وجود ندارد اما اگر همین عکس در چند تلفن همراه دیگر ذخیره شده باشد میتوان آن را بازیابی کرد [۳].

در این بخش از مطالعات در پی طرح‌ها و روش‌هایی هستیم که بتوان با استفاده از آنها خلا امنیت و حفاظت از حریم خصوصی را پوشش داد. مهمترین عامل برای استفاده‌ی گسترده کاربران از فناوری‌های جدید و پیشرفت این فناوری‌ها ارائه سطح بالایی از امنیت در کنار کارایی می‌باشد. از این رو سوالاتی مطرح است که چگونه و با چه روش‌هایی میتوان این امنیت را برقرار نمود؟ برخی از محققین با استفاده از تلفیق طرح‌های ارائه شده با هم و ایجاد یک سازکار جدید روش‌هایی را ارائه میدهند که از لحاظ امنیت سطح بالاتری را در برمی‌گیرند در نتیجه می‌توان الگوریتم‌ها و طرح‌هایی که حتی در یک زمینه‌ی ساده امنیت مناسبی را ارائه دادند را به طور کامل بررسی نمود و با ایجاد تغییرات و افزودن الزامات امنیتی جدید و ترکیب با دیگر طرحهای موفق موجود، طرحی با امنیت بالا را طراحی کرد. برای این منظور می‌بایست ابتدا به طورکامل نقاط ضعف و قوت فناوری‌ها و پلتفرم‌های مورد استفاده را بررسی نمود و سپس طرح‌هایی را که میتوانند با این فناوری‌ها همگام شوند انتخاب کرد و برای استفاده در آنها بررسی نمود.

۲ بلاک‌چین

بلاک‌چین یک فناوری نوظهور است که نخستین بار در سال ۲۰۰۹ توسط ناکاموتو به عنوان بستر معاملات ارز دیجیتال بیتکوین بکار گرفته شد. این فناوری بر اساس دفتر کل توزیع شده طراحی شده است که عدم تمرکز، شفافیت، در دسترس بودن و عدم شکست از ویژگی‌های بارز این فناوری می‌باشد. بلاک‌چین بعد از عملکرد موفق در بستر معاملات بیت‌کوین و حذف واسطه‌ها در معاملات، برای سایر بخشها نیز مورد توجه محققین قرار گرفت تا از آن در زمینه‌های دیگری چون توزیع دارو، احراز هویت، تجارت الکترونیکی، اینترنت اشیا وزمینه‌هایی که هر روز در حال افزایش هستند به کار گرفته‌شود. شبکه بلاک‌چین سرور متمرکز ندارد و اطلاعات به صورت زنجیره‌ای در تمام شبکه توزیع می‌شود و هر بلوکی بعد از تایید بلوک رهبر و با هماهنگی سایر بلوکها به زنجیره اضافه می‌شود، به بلوک جدید یک جفت جدید تخصیص داده می‌شود که شامل کلید عمومی و کلید خصوصی می‌باشد. کلید عمومی نمایشگر آدرس هر بلوک در شبکه می‌باشد و برای ارسال داده از آن استفاده می‌شود و کلید خصوصی نیز به منظور امضای تراکنش‌ها و رمزگشایی از پیام‌های دریافتی استفاده می‌شود [۴].

۱.۲ انواع بلاک‌چین

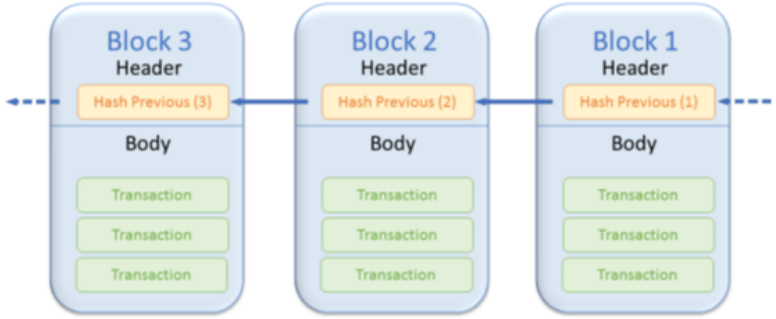
بلاک‌چین‌ها بر اساس کاربردی که دارند در سه نوع طبقه بندی می‌شوند که هر کدام دارای الزامات امنیتی و شرایط خاصی می‌باشند و کاربردهای مختلفی دارند. در این بخش به معرفی انواع بلاک‌چین می‌پردازیم [۵].

۱.۱.۲ بلاک‌چین عمومی

بلاک‌چین عمومی یا بدون مجوز، این نوع از بلاک‌چین برای افزودن بلوک جدید نیاز به مجوز خاصی ندارد و هر گره‌ای در این زنجیره میتواند آزادانه به شبکه بپیوندد یا از آن خارج شود. داده‌ها در یک شبکه بلاک‌چین عمومی کاملا باز و شفاف هستند. بلاک‌چین عمومی امنیت و حریم خصوصی داده‌های بلاک‌چین را با استفاده از یک الگوریتم رمزگذاری و الگوریتم اجماع تضمین می‌کند. نمونه‌هایی از این نوع بلاک‌چین عبارت است از بیت کوین و اتریوم.

۲.۱.۲ بلاک‌چین خصوصی

در یک بلاک‌چین خصوصی، حقوق نوشتن بلاک‌چین توسط یک موسسه کنترل می‌شود در حالیکه حقوق خواندن بر اساس وضعیت واقعی تنظیم می‌شود. بلاک‌چین خصوصی نسبت به نوع عمومی آن معمولا دارای بلوک‌های کمتری می‌باشد و امنیت در این نوع دارای اهمیت بیشتری است. از بلاک‌چین خصوصی در مدیریت زنجیره تامین و حسابرسی استفاده می‌شود. نمونه پر کاربرد از بلاک‌چین خصوصی، پلتفرم مالتی‌چین می‌باشد که عمدتا محیط زنجیره خصوصی را برای حفاظت از حریم خصوصی سازمانی و کنترل مجوزها به کار می‌گیرد.



شکل ۱: نمایش ساختار بلاک‌چین

۳.۱.۲ بلاک‌چین کنسرسیومی

محدودترین و امنیتی‌ترین نوع بلاک‌چین که در شرکت‌های حقوقی و تجاری خاص کاربرد دارد. در این نوع برای اضافه شدن یک بلوک باید تمامی بلوک‌ها آن بلوک را تایید کنند. نمونه‌های این نوع بلاک‌چین را لینوکس و اتحاد بلاک‌چین R3 ارائه می‌دهند. بلاک‌چین خصوصی و کنسرسیومی برای اضافه شدن بلوک‌های جدید به تایید تمامی یا بخشی از بلوک‌ها نیاز دارند که به آنها بلاک‌چین‌های مجاز گفته می‌شود.

۲.۲ ساختار بلاک‌چین

بلاک‌چین از زنجیره بلوکی تشکیل شده است که حاوی جزئیات معاملات ذخیره شده درون شبکه است (شکل ۱). هر بلوک از زنجیره شامل یک سرآیند و یک بدنه است، جایی که سربرگ شامل شناسه بلوک قبلی است و بدنه شامل معاملات ذخیره شده در یک درخت مرکل است [۶]. بلوک‌ها به صورت زنجیرهای به هم متصل شده‌اند و می‌توان آنها را به عنوان یک لیست پیوندی تصور کرد. سربرگ بلوک شامل شماره آن، مقدار هش بلوک قبلی و مهر زمانی است و در بدنه بلوک نیز داده‌های تراکنش ثبت می‌شود.

۱.۲.۲ الگوریتم هش

یک الگوریتم رمزنگاری است که اطلاعات اصلی را با هر طولی به مقدار هش با طول ثابت تبدیل می‌کند، به این شکل که اگر بیست کاراکتر و عدد به عنوان داده وارد بلوک شود طبق این الگوریتم با طول ثابتی مثلا ده کاراکتر به یک رشته تبدیل می‌شود و امنیت این الگوریتم باید به گونه‌ای باشد که مهاجم نتواند از روی رشته هش به داده اصلی دستیابی پیدا کند. معمولا از الگوریتم SHA-256 برای هش کردن داده‌ها استفاده می‌شود.

۲.۲.۲ درخت مرکل

درخت مرکل یک اثر انگشت دیجیتالی از مجموعه تراکنش ایجاد می‌کند تا تراکنش‌ها را به سرعت شناسایی و موقعیت‌یابی کند. مقدار هش هر تراکنش را به عنوان یک گره در نظر می‌گیرد و به صورت بازگشتی دو مقدار

هش مجاور را دوباره هش می‌کند تا زمانی که فقط یک مقدار هش باقی بماند یعنی به ریشه درخت برسد.

۳.۲.۲ قرارداد هوشمند

بلوکی است که قوانین و الزامات امنیتی بلاک‌چین مورد نظر در آن وارد می‌شود و به شکل رمزگذاری شده نگه‌داری می‌گردد تمامی محاسبات و الزامات امنیتی بلاک‌چین یعنی دسترسی‌ها توسط قرارداد هوشمند انجام می‌شود. باید توجه داشت که فقط بلوک‌های مجاز می‌توانند از محتوای قرارداد هوشمند مطلع باشند. قرارداد هوشمند باید به طور ایمن نگه‌داری شود و مهاجمین نباید به آن دسترسی پیدا کنند.

۳.۲ فناوری‌های کلیدی و چارچوب‌های پیاده سازی بلاک‌چین

طیف گستردهای از فناوری‌ها و چارچوب‌ها جهت برنامه‌نویسی بلاک‌چین در دسترس است، که در این بخش به معرفی تعدادی از این چارچوب‌ها خواهیم پرداخت. اصلی ترین نکات در انتخاب بستر بلاک‌چین عبارت است از : نوع شبکه، زبان برنامه نویسی، پروتکل اجماع، میزان اهمیت کار و شیوه کار می‌باشد [۷].

۱.۳.۲ اریس

از چارچوب‌های برنامه‌نویسی کارآمد و چند منظوره است. برنامه‌نویسان بلاک‌چین معمولا از این نرم افزار برای ساده سازی قراردادهای هوشمند استفاده می‌کنند.

۲.۳.۲ هیدراچین

ویژگی اصلی هیدراچین سازگاری کامل با پروتکل اتریوم است. بخش اصلی آن پیکربندی بلاک‌چین‌های خصوصی و کنسرسیومی را تحت پوشش قرار می‌دهد.

۳.۳.۲ اوپن‌چین

شبکه متن‌باز و آزاد جهت اشتراک‌گذاری دفترکل است. در مقایسه با سایر بسترها از سرعت بیشتری برخوردار است و در برنامه‌های سطح بالا از آن استفاده می‌شود، از این پلتفرم اغلب در بلاک‌چین عمومی استفاده می‌شود.

۴.۳.۲ اتریوم

محیطی متن باز جهت برنامه‌نویسی بلاک‌چین می‌باشد که می‌تواند از آن برای تمامی برنامه‌های غیرمتمرکز استفاده کرد. اتریوم از سطح امنیت و انعطاف بالایی در بسترهای مختلف برخوردار است. معمولاً در بلاک‌چین‌های عمومی از آن استفاده می‌شود و از زبان های C++ و پایتون پشتیبانی می‌کند.

۵.۳.۲ هایپر لجر

چارچوب متن باز برای نرم افزارهای پیشرو در حوزه بلاک‌چین است که معمولا در برنامه‌های تجاری و شبکه‌های خصوصی استفاده می‌شود.

۳ رایانش ابری

رایانش ابری یک سیستم است که در آن منابع یک مرکز داده با استفاده از فنّاوری مجازی‌سازی به اشتراک گذاشته شده است و دارای صفات کشسان ، مبتنی بر تقاضا و فیش هزینه بر اساس میزان استفاده کاربر است [۸]. صفت کشسان بودن به این معنا است که منابع در کمترین زمان و در هر میزان که کاربر درخواست کرده باشد در اختیار او قرار می‌گیرد و با سرعت در پایان سرویس پس گرفته می‌شود. به‌عبارت‌دیگر به معنای بزرگ و کوچک شدن پویایی سیستم با توجه به نیاز کاربر است. در واقع ابر برای سهولت استفاده از منابع اطلاعاتی، سخت‌افزاری، برنامه‌های کاربردی، شبکه‌ها و زیرساخت‌ها اختراع شده است. رویکرد آن بدین گونه است که شما دیگر احتیاج نیست دستگاه‌های کامپیوتری با قدرت پردازش بالا داشته باشید و برای این امر هزینه زیادی بپردازید، بلکه تنها کافی است سیستم کامپیوتری داشته باشید که قابلیت اتصال به شبکه جهانی اینترنت را داشته باشد. درنتیجه ابر می‌تواند باعث کاهش هزینه و افزایش سرعت برای کاربران شود.

معماری رایانش ابری، در حالت کلی، از سه لایه نرم‌افزار به‌عنوان سرویس (SaaS) ، بستر به‌عنوان سرویس (PaaS) و زیرساخت به‌عنوان سرویس (IaaS) تشکیل‌شده است [۹]. با وجود تمام این امکانات، کاربران برای پیوستن به ابر دچار تردید هستند و علت این تردید عدم اعتماد به امنیت ابر است. ابر دارای ویژگی‌های منحصربه‌فردی است که باعث بروز مسائل امنیتی جدیدی شده است. از جمله این مشکلات می‌توان عدم اعتماد کاربران به فراهم‌کننده ابر را نام برد. درنتیجه ابر باید محرمانگی داده را تضمین کند [۱۰]. محرمانگی در محیط ابر به این معنا است که داده‌ها و اطلاعات افراد باید از هر دو فرد فراهم‌کننده ابر و همچنین دیگر مشتری‌ها محرمانه نگه‌داری شود. همچنین ابر باید حفظ حریم خصوصی کاربران را تضمین کند. این موضوع بدین معنا است که ابر باید تضمین کند اطلاعات برون‌سپاری شده توسط کاربر به‌وسیله هیچ فرد تائید نشده‌ای که اجازه دسترسی ندارد، قابل‌دسترسی نیست. پس کنترل دسترسی یکی از نیازمندی‌های اساسی به‌منظور ممانعت از دسترسی افراد غیرمجاز به سیستم و محافظت از دارایی‌های سازمان است. امروزه ابر برای ذخیره‌سازی اطلاعات حساسی به کار گرفته می‌شود، درنتیجه اطمینان از اینکه این اطلاعات توسط افرادی که اجازه دسترسی به آن را ندارند دیده نمی‌شود حائز اهمیت است. به‌عبارت‌دیگر یک روش کنترل دسترسی کارا می‌تواند این اطمینان را برای کاربران ایجاد کند که اطلاعات آن‌ها توسط افراد تائید نشده قابل‌دسترسی نیست.

با ظهور رایانش ابری، نگرانی‌های تازه‌ای به امنیت اضافه‌شده است. ازجمله این نگرانی‌ها می‌توان به ذخیره‌سازی منابع و داده‌ها در ابر با احتمال اینکه در کشور دیگری با قوانین امنیتی متفاوتی ذخیره شود اشاره کرد. علاوه بر این ابر یک محیط اشتراک گذاشته‌شده است که از مکانیسم به اشتراک‌گذاری زیرساخت‌ها استفاده می‌کند. درنتیجه درباره داده‌ها ممکن است با مسائلی مانند دسترسی‌های غیرمجاز روبرو شویم. از آنجا که اطلاعات در محاسبات ابری در میان بخش‌های مختلفی به اشتراک گذاشته می‌شود، درنتیجه درجه‌های حساسیت مختلفی را باید بتوان تعریف کرد. پس در ابر وجود مکانیسم کنترل دسترسی قوی یک نیاز اصلی و اساسی است.

ابر دارای ویژگی‌هایی مانند ماهیت پویا، ناهماهنگی و تنوع در خدمات، سیاست‌های کنترل دسترسی

مختلف و گاه متضاد و برخورد با تعداد زیادی از کاربران است. این ویژگی‌ها باعث می‌شود تا روش‌های موجود کنترل دسترسی، در ابر کارایی نداشته باشد. به‌طور قطع ارائه یک مدل کنترل دسترسی جدید نیز انتخاب مناسبی نیست؛ زیرا ارائه یک روش جدید نیاز به زمان دارد تا آزمایش‌شده و مشکلات آن برطرف شود [۱۱] با توجه به نکات ذکرشده می‌توان نتیجه گرفت که راه‌حل صحیح برای ایجاد یک مدل کنترل دسترسی متناسب با ویژگی‌های ابر این است که مدل‌های موجود را به‌گونه‌ای تغییر دهیم تا بتواند نیازمندی‌های موجود در ابر را به‌خوبی برآورده سازد. مدل کنترل دسترسی مبتنی بر ویژگی در واقع بسط یافته مدل کنترل دسترسی مبتنی بر نقش است که برای برطرف کردن مشکلات روش‌های قبلی و متناسب با ویژگی‌های ابر ایجادشده است.

یک سیستم کنترل دسترسی در واقع مجموعه‌ای از اجزا و روش‌ها است که سطح دسترسی صحیح برای کاربران قانونی را براساس اجازه‌های دسترسی از پیش تعیین‌شده در سیاست دسترسی تعیین می‌کند. هدف اصلی هر سیستم کنترل دسترسی این است که دقیقاً مشخص کند هر کاربر چه‌کارهایی را می‌تواند انجام دهد تا از اطلاعات در برابر دسترسی‌های غیرمجاز محافظت کند. محاسبات ابری یک محیط اشتراک‌گذاری شده است که کاربران نه‌تنها به دیگر کاربران ابر اعتماد ندارند بلکه به فراهم‌کننده ابر نیز اعتماد ندارند. این ویژگی‌ها و خصوصیات ابر باعث می‌شود تا نیاز به یک سیستم کنترل دسترسی نیرومند وجود داشته باشد تا بتواند منابعش را کنترل کند. درنتیجه علاوه بر اینکه ما به علت عدم اعتماد به فراهم‌کننده ابر باید داده‌ها را قبل از برون‌سپاری به ابر رمز کنیم، لازم است بتوانیم برای داده‌ها یک سیاست دسترسی تعریف کنیم تا دسترسی افراد به داده‌ها نظارت و کنترل شود.

از طرف دیگر، در محاسبات ابری کاربران می‌توانند افراد و یا دستگاه‌های هوشمند باشند. این کاربران باید بتوانند به‌راحتی اطلاعات خود را به ابر ارسال و یا از ابر دریافت کنند. هنگامی‌که از دستگاه‌های هوشمند صحبت می‌شود، محدودیت‌های این دستگاه‌ها باید در نظر گرفته شوند. این محدودیت‌ها شامل میزان انرژی دستگاه، محدودیت فضای ذخیره‌سازی و قدرت پردازش می‌شود. با افزایش حجم تبادلات بین سرور ابر و کاربر، مصرف انرژی این دستگاه‌ها افزایش می‌یابد و درنتیجه نمی‌توانند برای مدت طولانی در ابر فعالیت کنند. پس باید با ایجاد روش‌هایی علاوه بر اینکه نیازمندی‌های کنترل دسترسی در ابر را برآورده می‌کنیم، بتوانیم حجم تبادلات را کاهش دهیم. همچنین باید تعداد کلیدهای خصوصی ویژگی که هر کاربر باید ذخیره کند را نیز کاهش دهیم. در ادامه، امنیت و حریم خصوصی ابر از دیدگاه پنج ویژگی اصلی بررسی می‌شود که این پنج ویژگی شامل محرمانگی، یکپارچگی، در دسترس بودن، مسئولیت‌پذیری و حفظ حریم خصوصی می‌شود [۱۲].

۱. **محرمانگی.** محرمانگی به معنای جلوگیری از افشای اطلاعات به افراد غیرمجاز است. اطمینان از اینکه اطلاعات تنها در دسترس کاربرانی است که مجاز به دسترسی هستند. این اصل به اعتقاد بسیاری از صاحب‌نظران از مهم‌ترین جنبه‌های امنیتی برای سازمان‌های نظامی و دولتی است. محرمانگی در محاسبات ابری به این معنی است که محاسبات و داده‌های مشتری در مقابل ارائه‌دهنده ابر و همچنین سایر مشتری‌های ابر محرمانه نگهداری شود. برون‌سپاری در این زمینه در واقع باعث

می‌شود تا کنترل و مدیریت داده به‌صورت بالقوه و غیرقابل‌اعتمادی به فراهم‌کننده ابر داده شود.

۲. **یکپارچگی.** حفاظت از داده‌ها و اطلاعات در مقابل تغییرات غیرمجاز سهوی و عمدی را یکپارچگی و یا جامعیت اطلاعات گویند. در محاسبات ابری یکپارچگی داده نشان‌دهنده این است که داده باید صادقانه روی سرور ذخیره‌شده باشد و هیچ‌گونه نقضی ایجاد نشود. همچنین تمامیت محاسبات یعنی برنامه‌ها بدون تحریف توسط نرم‌افزارهای مخرب، فراهم‌کننده ابر و یا کاربران مخرب اجرا شوند.

۳. **در دسترس بودن.** قابلیت استفاده همیشگی و مداوم دستگاه‌های کامپیوتری توسط کاربران مجاز را در دسترس بودن گویند. در دسترس بودن از ویژگی‌های ضروری محاسبات ابری است، زیرا درصورتی‌که در دسترس بودن و یا کیفیت خدمات از یک سطح پایین‌تر باشد مشتریان اعتماد خود را به سیستم ابر از دست می‌دهند.

۴. **مسئولیت‌پذیری.** در ابر به این معنا است که در صورت بروز مشکل و یا عدم رعایت هرکدام از چهار ویژگی ذکرشده، ابر باید بتواند به‌صورت غیر قابله انکاری فرد خاطی یا مسئول وقایع را شناسایی کند. پس مسئولیت‌پذیری به این معنا است که بتوان دستگاه و یا برنامه معیوب یا مخرب را شناسایی کنیم.

۵. **حفظ حریم خصوصی.** اطلاعات کاربران برای افراد تائید نشده قابل‌دسترسی نباشد. خطرات بالقوه‌ای وجود دارد که داده‌های محرمانه و یا اطلاعات شخصی برای عموم و یا رقبای کسب وکار افشا شود. برخی از ویژگی‌های ذکرشده باعث افزایش حریم خصوصی کاربران می‌شود و برخی در تضاد با حریم خصوصی کاربران هست. با ایجاد یک روش کنترل دسترسی مناسب می‌توانیم محرمانگی و حفظ حریم خصوصی کاربران را تضمین کنیم.

محققان متعددی از طرح‌های رمزنگاری مختلف برای دستیابی به امنیت داده‌ها در ذخیره‌سازی ابری استفاده کرده‌اند. در ادامه، به مقایسه عملکرد تکنیک‌های به اشتراک‌گذاری داده‌ها در فضای محاسبات ابری پرداخته و نتایج به‌دست‌آمده از تحقیقات انجام‌شده در این زمینه را در قالب جدول ۱ بیان می‌کنیم.

۴ طرح پیشنهادی مبتنی بر بلاک‌چین و رایانش ابری

در طول این سال‌ها، اهمیت رایانش ابری بسیار قابل توجه بوده‌است. بسیاری از کاربران و شرکت‌ها برای خدمات مختلف به ابر متصل می‌شوند، با انتقال داده‌های خود به فضای ذخیره سازی ابری صاحبان داده‌ها از صرفه‌جویی در هزینه، مقیاس پذیری و در دسترس بودن داده‌ها برخوردار می‌شوند. علاوه بر این صاحبان داده‌ها را می‌توان از بروزرسانی سیستم‌های بانکی، نگهداری دورهای و حفظ زیرساخت ذخیره‌سازی آزاد کرد. با وجود مزایای فوق العاده، امنیت و حفظ حریم خصوصی همچنان مانعی در استفاده گسترده از رایانش ابری هستند. به عنوان مثال کاربر نمی‌داند چگونه داده‌های او در فضای ابری سازماندهی می‌شود، داده‌های او را در قالب متمرکز ذخیره می‌کنند و کنترل محدودی از ابر به آنها اعطا می‌شود، علاوه بر این بسیاری از طرح‌های موجود از در دسترس بودن داده‌ها و ذخیره‌سازی متمرکز آن رنج می‌برند. سوالی که مطرح است

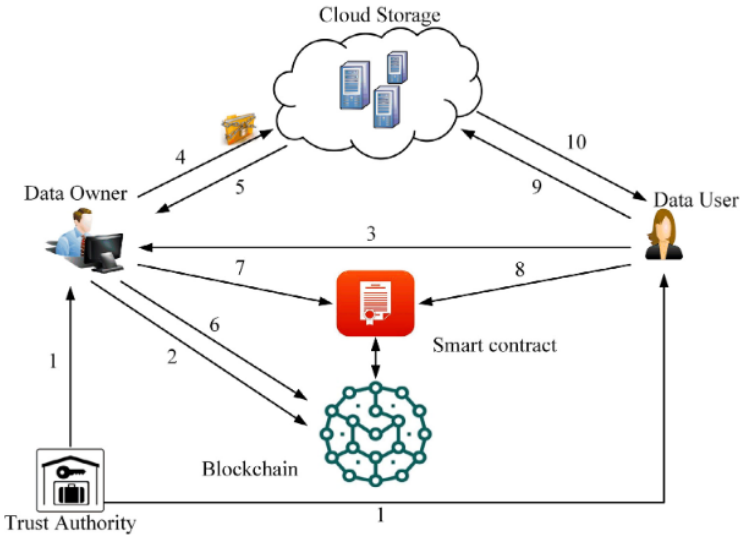
جدول ۱: نتایج مقایسه روش‌های به اشتراک‌گذاری داده‌های فضای محاسبات ابری

عنوان تکنیک	نحوه عملکرد	تضمین امنیت داده‌ها	رعایت حریم خصوصی
رمزنگاری مبتنی بر ویژگی (ABE) [۱۳]	استفاده از سیاست‌های دسترسی و ویژگی‌های نسبت داده‌شده در میان کلیدهای رمزگشایی و متون رمزنگاری‌شده.	دارد	دارد
رمزنگاری مبتنی بر هویت (IBBE) [۱۴]	داده‌های رمزگذاری شده با چندین گیرنده در یک‌زمان به اشتراک گذاشته شده و کلید عمومی گیرنده می‌تواند به‌عنوان هر رشته معتبری مانند هویت منحصربه‌فرد و ایمیل در نظر گرفته شود.	دارد	دارد
تائید از راه دور [۱۵]	تفویض یک کلید رمزگذاری مجدد مرتبط با گیرنده‌های جدید به ارائه دهنده خدمات ابری استفاده می‌شود. با این حال، پخش‌کننده داده‌ها می‌تواند تمام داده‌های مالک داده را با این کلید رمزگذاری مجدد در اختیار دیگران قرار دهد.	دارد	دارد
شارون [۱۶]	رابط برای دسترسی به اکوسیستمی از چندین سرویس ابری و امکان انتقال داده بین مشتریان را فراهم می‌کند.	دارد	دارد

این می‌باشد که چه ضمانتی وجود دارد که به داده‌های حساس بانکی فقط کابران مجاز دسترسی داشته باشند و مهاجمین برای جعل و سو استفاده به آنها دسترسی پیدا نکنند، از این رو محققین طرح به اشتراک گذاری داده ایمن مبتنی بر بلاک‌چین و رمز گذاری مبتنی بر ویژگی (ABSC) [۱۷] را پیشنهاد نمودند که در این طرح رمزگذاری با استفاده از یک امضا و یک طرح رمزگذاری بطور جداگانه انجام می‌شوند که راه کارآمدتری نسبت به روش‌های مشابه می‌باشد.

در واقع رمزگذاری با استفاده از یک امضا و یک طرح رمزگذاری به طور جداگانه روش کارآمدتری را ارائه می‌دهند که این طرح را BABSC [۱۸] نامگذاری کردند. باتوجه به بررسی انجام شده و مقایسه این طرح با سایر طرح های موجود، BABSC امنیت بالاتر و سربار کمتری را ارائه می‌دهد. الگوریتم ABSC ترکیب منطقی از ABE [۱۹] و ABS [۲۰] می‌باشد که بسیاری از ویژگی‌های امنیتی مانند محرمانگی، جعل ناپذیری، احراز هویت و کنترل دسترسی ایمن را فراهم می‌کند. اجزای تشکیل دهنده طرح BABSC، سرور ابری(CS)، مالک داده (DO)، کاربر داده (DU)، مرجع اعتماد (TA) و بلاک‌چین می‌باشند. در شکل ۲ نمای طرح پیشنهادی BABSC را مشاهده می‌کنیم.

در ابتدا مرجع اعتماد کاربران را احراز هویت کرده و به آن ها جفت کلید را اختصاص می‌دهد، سپس مالک داده الزامات خود را به شکل رمزنگاری شده در قرارداد هوشمند مستقر شده در بلاک‌چین بارگذاری می‌کند که سطح دسترسی به داده‌ها چگونه باشد. مالک داده، داده‌های رمزگذاری شده را که قصد اشتراک‌گذاریشان را دارد به سرور ابری ارسال می‌کند. کاربر داده به منظور استفاده از داده‌های مالک، یک درخواست مجوز به مالک ارسال می‌کند تا دسترسی لازم برای او ایجاد شود. سرور، مکان ذخیره سازی داده‌های مالک را به مالک داده ارسال می‌کند و مالک داده، اطلاعات مکانی داده‌ها را در بلاک‌چین قرار می‌دهد و بلاک‌چین، هش بلوک ذخیره شده را در اختیار او قرار می‌دهد و آن را در قرارداد هوشمند ذخیره می‌کند تا کاربران مجاز قادر به دسترسی به داده‌ها باشند. کاربر داده به هش مکان ذخیره سازی در قرارداد هوشمند دسترسی پیدا



شکل ۲: طرح BABSC

می‌کند و برای بازیابی داده‌های مالک، یک درخواست به مالک ارسال می‌کند و داده‌ها را از ابر دانلود می‌کند و با استفاده از کلید خصوصی خود داده‌ها را رمزگشایی می‌کند و مورد استفاده قرار می‌دهد.

در این طرح سه مورد امنیتی مهم برای کاربران ارائه می‌گردد که عبارت اند از: محرمانگی که بزرگترین چالش در رایانش ابری می‌باشد، برای اعمال محرمانگی داده‌ها بهترین مکانیزم موجود BABSC می‌باشد. دیگر مورد ارائه شده کنترل دسترسی می‌باشد که باتوجه به محدودیت‌هایی که مالک داده ایجاد می‌کند هر شخصی به هر دادهای دسترسی نخواهد داشت و مورد آخر جعل ناپذیری هست که بارزترین ویژگی بلاک‌چین می‌باشد و با قرار گرفتن در این مدل امکان جعل داده‌ها را به حداقل می‌رساند.

۱.۴ قرارداد هوشمند در BABSC

قرارداد هوشمند یک پروتکل کامپیوتری است که در داخل بلاک‌چین قرار دارد تا از مقیاس پذیری و کنترل دسترسی اطمینان حاصل کند. در این طرح، قرارداد هوشمند برای به اشتراک گذاری امن داده‌ها بین صاحبان مختلف داده و کاربران استفاده می‌شود. قرارداد هوشمند به منظور اجرای توافقات بروی گره‌ها استفاده می‌شود. طرح BABSC از قرارداد هوشمند پیشنهاد شده توسط Watanabe و همکاران [۲۱] استفاده می‌کند. بدلیل اینکه بلاک‌چین بکار برده شده عمومی است و تمامی کاربران می‌توانند آن را مشاهده کنند، داده‌های موجود در قرارداد باید رمزگذاری شود و در بلاک‌چین ذخیره شوند. سوال این است که چگونه و چه کسی قرارداد هوشمند را ایجاد می‌کند؟ مالک داده قرارداد را ایجاد می‌کند و آن را به کاربر یک ارسال می‌کند، کاربر یک با داشتن کلید رمزگشایی پیام را باز می‌کند و پیام رمزشده را به کاربر دو ارسال می‌کند و او نیز پیام را رمزگشایی می‌کند و در صورت تایید، پیام را به مالک داده باز می‌گرداند. در شبکه فقط مالک،

جدول ۲: مزایا و معایب طرح‌های پیشنهادی

نام روش	ایده اصلی روش	مزایا	معایب
BABSC	تلفیق الگوریتم‌های رمزنگار و بلاک چین برای امنیت داده	سربارکم–ذخیره‌سازی غیرمتمرکز - امنیت چند لایه	
SCDSA	رمزگذاری پیچیده و کوتاه شده برای تبادلات قرارداد هوشمند	امنیت عالی - سربار بسیار کم	این روش در سطح تئوری می‌باشد
ECDSA	رمزگذاری دیجیتال	سربار کم و نیاز به حافظه کم	در تئوری از SCDSA ضعیف تر است اما کاربردی‌تر می‌باشد
MediBchain	تلفیق بلاک‌چین وEHR	ارائه حریم خصوصی و امنیت داده در EHR	در انتقال از فرد به بلاک چین امکان حمله می‌باشد
Best	امنیت و یکپارچگی حمل و نقل هوشمند	شناسایی دستگاه ها– استفاده بهینه از انرژی	تشویق افراد به شرکت درطرح دشوار است
PHSS	تشخیص به لحظه بیماری	امنیت داده بیماران - تشخیص سریع – یکپارچگی	برای موارد خاص و نادر توصیه نمی‌شود.
MixCoin	جلوگیری از حملات خودی به شبکه بلاک‌چین	ردیابی داده - حفظ امنیت و سرمایه	می‌تواند در شبکه های مالی منجر به پول‌شویی شود.

جدول ۳: طرح‌های انتخابی

رویکرد	ایده اصلی	مزایا	معایب
BABSC [18]	ارائه بلاک چین عمومی با استفاده از الزامات چند مرحله ای برای اشتراک داده در فضای ابر	با رمزنگاری دو لایه و ارائه ذخیره – سازی غیرمتمرکز امنیت اشتراک داده را تضمین می‌کند	کاربران سیستم بایستی کلید رمزگشایی خود را با دقت نگهداری کنند.
MediBchain [22]	ارائه سیستم مراقبت بهداشتی با استفاده از بلاک چین برای حفظ حریم خصوصی	در زمینه مراقبت‌های بهداشتی امن ترین و کارآمدترین روش برای کاربر است	در فاصله ارتباط بین کاربر و بلاک چین امکان حمله وجود دارد

کاربر یک و کاربر دو بدلیل داشتن کلید رمزگشایی قادر به مشاهده پیام‌ها هستند.

۵ ارزیابی طرح پیشنهادی

در این بخش طرح‌هایی بررسی شد که در آن ها بلاک‌چین در کنار سایر فناوری‌ها قرار گرفت تا امنیت و کارآیی آن ها را بهبود ببخشد، بعضی از این پروتکل‌ها و طرح‌ها مزایای ویژه‌ای را به فناوری مورد نظر افزودند در جدول زیر به بررسی کارآیی و معایب این طرح‌ها خواهیم پرداخت. ابتدا در جدول ۲ مزایا و معایب طرح‌های پیشنهادی را بررسی می‌کنیم.

با بررسی انجام شده در جدول ۲ و مطالب مورد مطالعه قرار گرفته طرح‌های مشابه را باهم مورد مقایسه قرار دادیم تا بهترین روش و طرح ارائه شده برای حفظ امنیت در سیستم بانکی را شناسایی کنیم. در جدول ۳ دو طرحی که در امنیت اشتراک داده‌ها پیشگام هستند و برای سیستم بانکی توصیه می‌گردد را بررسی می‌کنیم.

در میان مطالعات، بررسی‌ها و مقایسه بین طرح‌های موجود این نتیجه استنباط می‌شود که طرح BABSC تمامی معیارهای یک طرح مناسب برای ایجاد امنیت سیستم بانکی و کارآیی مناسب بلاک‌چین در کنار سایر فناوری‌های روز نظیر رایانش ابری را دارا می‌باشد. طرح BABSC باتوجه به اینکه هم الگوریتم رمزگذاری دیجیتال منحنی بیضوی و هم رمزنگاری مبتنی بر ویژگی را دارا می‌باشد و مهم تر از همه اینکه از دفترکل توزیع شده مورد اعتمادی نظیر بلاک‌چین استفاده می‌کند می‌توان از آن در رایانش ابری، اینترنت اشیاء، سیستم بانکی و ... استفاده نمود. یکی از مواردی که تعدادی از محققین از آن بعنوان امتیاز شاخص این طرح یاد می‌کنند، عدم دسترسی مستقیم به سرور اصلی می‌باشد و کاربری جز با ارتباط با بلاک‌چین قابلیت ارتباط با سرور اصلی را ندارد و مهم‌تر از همه اینکه تمامی افراد در ابتدا احراز هویت می‌شوند و شخص غیرقابل اعتماد نمی‌تواند وارد شبکه شود. در طرح پیشنهادی کاربری که تمایل دارد تا اطلاعات خود را در سرور ابری ذخیره کند می‌تواند با طراحی خط مشی مورد نظر خود به افراد دیگر نیز اجازه بهره برداری از اطلاعات را بدهد. نکته مهمی که در مورد طرح BABSC باید به آن توجه کرد ارائه امنیت بالای این سیستم می‌باشد که سخت گیری این طرح را برای امور ساده‌تر نمی‌توان مناسب دانست.

۶ نتیجه‌گیری و پیشنهادها

با بررسی‌ها و مطالعات انجام شده بر روی شبکه بلاک‌چین و فناوری‌های نوظهور دیگر نظیر رایانش ابری این نتیجه حاصل شد که شبکه‌ی بلاک‌چین اگرچه از نظر محاسبات و سرعت تراکنش‌ها از سایر فناوری‌های پرکاربرد حال حاضر پیشی نگرفته است اما در ارائه امنیت و ایجاد حریم خصوصی جزء شاخص‌ترین فناوری‌های روز دنیا می‌باشد. با توجه به اهمیت مقوله امنیت در سیستم بانکی، طرحی جهت ارتقای امنیت سیستم بانکی با استفاده از فن آوری بلاک‌چین و رایانش ابری پیشنهاد شد. در طرح پیشنهادی از بلاک‌چین عمومی استفاده شد اما می‌توان برای داده‌های شخصی‌تر و دارای امنیت بالا از انواع دیگر بلاک‌چین یعنی خصوصی و کنسرسیومی استفاده نمود تا سطح ایمنی ارائه شده توسط این سیستم ارتقا یابد. در صورت بکارگیری BABSC در بحث احراز هویت و ثبت اطلاعات مهم کاربران در سیستم‌های مهم اطلاعاتی نظیر سیستم بانکی ذخیره اطلاعات در بلوک‌های بلاک‌چین می‌توان داده‌های مهم کاربران را در مقابل نفوذ مهاجمین، جعل، حذف و دستکاری حفاظت نمود.

باتوجه به اینکه بلاک‌چین یک شبکه ذخیره سازی غیرمتمرکز، شفاف و جعل ناپذیر است و ABSC یک الگوریتم رمزنگاری مستحکم و با سربار کم می‌باشد روش پیشنهادی در این تحقیق این است که طرح BABSC را با تغییرات مثبت و در جهت افزایش کارایی خود طرح و فناوری رایانش ابری به عنوان فناوری مکمل بتوان به طور گسترده در افزایش کاربرد و پیشرفت بلاک‌چین استفاده نمود.

ما این طرح را برای استفاده در سیستم بانکی پیشنهاد می‌کنیم به این ترتیب که مالک داده (شخص حقیقی یا حقوقی) پس از احراز هویت وارد شبکه می‌شود، خط مشی مورد نظر خود را در قرارداد هوشمند برای نحوه دسترسی سایرین به اطلاعات بارگذاری نموده تعیین می‌کند که چه کسی و در چه سطحی بتواند به این داده‌ها دسترسی پیدا کنند. کاربر پس از احراز وارد شبکه می‌شود درخواست دسترسی به اطلاعات را

به مالک داده ارسال می‌کند، مالک در صورت تایید به او مجوز خواهد داد و کلید رمزگشایی را با او به اشتراک خواهد گذاشت. این طرح را می‌توان با یک سرور متمرکز اجرا نمود که فقط وظیفه ذخیره داده‌ها را داشته باشد یا برای افزایش امنیت در سیستم‌های که حجم داده خیلی زیادی ندارند برای ذخیره‌سازی نیز از شبکه بلاک‌چین استفاده نمود تا امنیت را به شدت افزایش دهیم و راه نفوذ مهاجمین به داده‌ها را مسدود کنیم.

با استفاده از فن آوری بلاک‌چین و رایانش ابری با وجود تهدیدات امنیت شبکه که طبق آمار، همیشه تهدیدات از الزامات امنیتی یک قدم جلوتر هستند باید از بهترین و کارآمدترین فناوری‌ها در جهت حفظ داده‌ها و ایجاد امنیت برای کاربران استفاده نمود. بر اساس مطالعات انجام شده فناوری بلاک‌چین با استفاده از الگوریتم رمزنگاری دیجیتال مبتنی بر ویژگی، روشی کارآمد و امن برای ایجاد امنیت در سیستم بانکی می‌باشد. همان طور که پیش تر ذکر شد نباید به این روش‌ها بسنده کرد زیرا تهدیدات شبکه هر روزه در حال تغییر و پیشرفت هستند در نتیجه باید این روش های کارآمد را کامل‌تر و یا با سایر روش‌های جدید تلفیق نمود.

مراجع

[1] Guo H, Yu X. A Survey on Blockchain Technology and its security. Blockchain: research and applications. 2022 Jun 1;3(2):100067.

[2] Chowdhury MU, Suchana K, Alam SM, Khan MM. Blockchain application in banking system. Journal of Software Engineering and Applications. 2021 Jul 8;14(7):298-311..

[3] Dhanda N. Cryptocurrency and Blockchain: The Future of a Global Banking System. InRegulatory Aspects of Artificial Intelligence on Blockchain 2022 (pp. 181-204). IGI Global.

[4] Leng J, Zhou M, Zhao JL, Huang Y, Bian Y. Blockchain security: A survey of techniques and research directions. IEEE Transactions on Services Computing. 2020 Nov 25;15(4):2490-510.

[5] Sabry SS, Kaittan NM, Majeed I. The road to the blockchain technology: Concept and types. Periodicals of Engineering and Natural Sciences. 2019 Dec 24;7(4):1821-32.

[6] Ugli Jurayev DU. Security in the Internet of Things: A Review. Texas Journal of Engineering and Technology. 2022 Aug 4;11:15-7.

[7] Shrivas MK, Yeboah T. The disruptive blockchain: types, platforms and applications. Texila International Journal of Academic Research. 2019 Apr;2019:17-39.

[8] Toosi AN, Son J, Chi Q, Buyya R. ElasticSFC: Auto-scaling techniques for elastic service function chaining in network functions virtualization-based clouds. Journal of Systems and Software. 2019 Jun 1;152:108-19

[9] Tari Z, Yi X, Premarathne US, Bertok P, Khalil I. Security and privacy in cloud computing: vision, trends, and challenges. IEEE Cloud Computing. 2015 Jun 2;2(2):30-8.

[10] Tabrizchi H, Kuchaki Rafsanjani M. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing. 2020 Dec;76(12):9493-532.

[11] Younis YA, Kifayat K, Merabti M. An access control model for cloud computing. Journal of Information Security and Applications. 2014 Feb 1;19(1):45-60.

[12] Tang J, Cui Y, Li Q, Ren K, Liu J, Buyya R. Ensuring security and privacy preservation for cloud data services. ACM Computing Surveys (CSUR). 2016 Jun 6;49(1):1-39.

[13] Xue K, Chen W, Li W, Hong J, Hong P. Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Transactions on Information Forensics and Security. 2018 Feb 26;13(8):2062-74.

[14] Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys. InAdvances in Cryptology–ASIACRYPT 2007: 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, December 2-6, 2007. Proceedings 13 2007 (pp. 200-215). Springer Berlin Heidelberg.

[15] Paladi N, Gehrmann C, Michalas A. Providing user security guarantees in public infrastructure clouds. IEEE Transactions on Cloud Computing. 2016 Feb 3;5(3):405-19.

[16] Zhou Y, Deng H, Wu Q, Qin B, Liu J, Ding Y. Identity-based proxy re-encryption version 2: Making mobile access easy in cloud. Future Generation Computer Systems. 2016 Sep 1;62:128-39.

[17] Eltayieb N, Elhabob R, Hassan A, Li F. A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud. Journal of Systems Architecture. 2020 Jan 1;102:101653.

[18] Li X, Ge L, Chen J, Peng Z. Comments on "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud". Journal of Systems Architecture. 2022 Oct 1;131:102702.

[19] Guo R, Shi H, Zheng D, Jing C, Zhuang C, Wang Z. Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system. IEEE Access. 2019 Jun 28;7:88012-25.

[20] Pan W, Qiu M. Application of blockchain in asset-backed securitization. In2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) 2020 May 25 (pp. 71-76). IEEE.

[21] Watanabe H, Fujimura S, Nakadaira A, Miyazaki Y, Akutsu A, Kishigami J. Blockchain contract: Securing a blockchain applied to smart contracts. In2016 IEEE international conference on consumer electronics (ICCE) 2016 Jan 7 (pp. 467-468). IEEE.

[22] Al Omar A, Rahman MS, Basu A, Kiyomoto S. Medibchain: A blockchain based privacy preserving platform for healthcare data. InSecurity, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10 2017 (pp. 534-543). Springer International Publishing.

تبیین حکمرانی فضای سایبر، با تکیه بر جایگاه قوای شناختی و مسئله معرفت

محسن ابراهیمی [۱]

[۱] دانش آموخته حوزهٔ علمیه قم، دکتری فلسفه دانشگاه اصفهان
mhnebr@gmail.com

چکیده

در تحلیلی فلسفی، فضای سایبر را می‌توان فضای شناختی دانست که در آن، دو قوای وهم و متخیله به شکل عمده به فعالیت‌های شناختی می‌پردازد و حاصل آن، آگاهی‌هایی جزئی است که ایجاد ویا انتقال داده می‌شود. تفاوت این فضا با جهان خارج، نشان از تفاوت حکمرانی آن می‌دهد؛ به این صورت که حکمرانی در این فضا، مبتنی بر جایگاه قوای شناختی است و بر همین اساس، سه صورت از حکمرانی، امکان تحقق دارد: حکمرانی اول، مبتنی بر مؤلفه‌های غیرشناختی است که با توجه به شناختی بودن آن، حکمرانیِ ضعیف است. صورت دوم، بر اساس حاکمیت قوای وهم و متخیله و ویژگی‌های آن است. این صورت از حکمرانی، نامطلوب است؛ زیرا حاصل آن، با توجه به ویژگی کثرت‌طلبی قوهٔ واهمه و متخیله، تفرقه و تشتت است. اما صورتی دیگر از حکمرانی، بر اساس مرتبه عقل است. مولفهٔ اصلی این حکمرانی در این است که آگاهی موجود در فضای سایبر، با توجه به توانایی‌های قوهٔ عقل، می‌تواند متعلق آگاهی درجهٔ دومی برای ارزیابی قرار بگیرد و با یافتن شرایط صدق و توجیه، به معرفت تبدیل بشود. بنابراین پایه حکمرانی مطلوب بر فضای سایبر –که ناظر به اعمال قدرت، جعل قوانین و نظارت است– مبتنی بر حاکمیت و تفوق قوهٔ عاقله است.

کلمات کلیدی: حکمرانی فضای سایبر، قوای شناختی، متخیله و واهمه، قوه عاقله، معرفت.

۱ مقدمه

با گسترش فضای سایبر و نفوذ آن در شئونات مختلف اجتماعی افراد، سخن از حکمرانی فضای سایبر امری ضروری و حیاتی به نظر می‌رسد. با این حال، آنچه در فضای مجازی به شکل غالب مشاهده می‌شود، نوعی رهاشدگی و ولنگاری است که آثار و صدمات فراوانی را نسبت به جامعه‌ی انقلاب اسلامی ایران داشته است.

بررسی و تأمل در ماهیت فضای سایبر مشخص می‌کند که فضای سایبر، اساساً فضای متفاوت از فضای فیزیکی و مادی است و لذا، مؤلفه‌هایی که برای حکمرانی در فضای سایبر نیز مطرح می‌شود، باید متفاوت از فضای فیزیکی باشد و نمی‌توان آن را صرفاً برپایه اموری مانند حکمرانی بر اساس قلمرو و جغرافیا تبیین کرد.

حکمرانی بر فضای سایبر، بحث جدیدی است که مورد توجه اندیشمندان حوزه ارتباطات قرار گرفته است و آثار گوناگونی در این زمینه تألیف شده است که از جمله آن‌ها می‌توان به کتاب «درآمدی بر حکمرانی فضای مجازی»، نوشته سید ابوالحسن فیروزآبادی و کتاب «الگوی حکمرانی دو فضایی»، نوشته‌ی سید سعیدرضا عاملی اشاره کرد. با این حال از نگاه نگارنده، تبیین حکمرانی در فضای سایبر نیازمند توجه به مبانی فلسفی حکمرانی بر فضای سایبر است؛ زیرا آن‌چنان که بیان شد، بحث از حکمرانی فضای سایبر، نیازمند طرح مبانی فلسفی است که خاستگاه اعمال قدرت و ملاک مشروعیت جعل قوانین را برای نظارت بر فضای سایبر به ما بدهد؛ بر همین اساس، چیستی فضای سایبر باید مورد تحلیل دقیق فلسفی قرار بگیرد و این مسئله تبیین بشود که حکمرانی بر فضای سایبر، صرفاً نمی‌تواند بر اساس مؤلفه‌های بیرون از فضای سایبر صورت بگیرد. بنابراین هرچند مقالاتی مانند «مدینه فاضله مجازی، چهارچوب نظری حکمرانی فضای مجازی»، تألیف آقایان عزیز نجف پور، حمید پارسانیا و علی اصغر اسلامی، و همچنین مقاله دیگری با عنوان «چالش‌های فضای مجازی و ارائه راهکار برای جمهوری اسلامی»، تألیف حافظ محمدی به این مسئله پرداخته‌اند، اما، در این مقالات به شناختی بودن فضای سایبر توجهی نشده است. بر همین اساس با توجه به اینکه بحث از حکمرانی فضای سایبر، به شکل غالب ناظر به رشته‌هایی همچون ارتباطات، رسانه و علوم اجتماعی است، مقالات متعددی با این رویکرد به بحثِ از مذکور پرداخته است؛ با این حال، رویکرد فلسفی به بحث حکمرانی به معنای نفی رویکردهای دیگر بحث نیست و می‌تواند مکمل آن باشد.

مسئله دیگر این است که اساساً با توجه به جایگاه تمدنی انقلاب اسلامی و طرح نگاه متعالی و حیات برتر برای انسان، طرح مسئله حکمرانی بر فضای مجازی، نیازمند به کار گرفتن اصول و مبانی مجزا و برتر از تمدن فرهنگ غرب است؛ از همین رو نمی‌توان اساسا الگوی برخاسته از تمدن و فرهنگ غرب را اساسی برای تبیین مسئله حکمرانی فضای مجازی در نسبت با جامعه‌ی انقلاب اسلامی دانست. واضح‌ترین شاهد بر این مدعا، این مسئله است که فضای سایبر در حال حاضر، عرصه و میدانی برای تقابل شناخت انقلاب اسلامی با تمدن غرب است که موجب شکل‌گیری نوعی جنگ شناختی، میان این دو نگاه در این فضا شده است. بنابراین به کار گرفتن اصول حکمرانی برخاسته از تمدن غرب، نمی‌تواند در این جنگ شناختی جامعه‌ی انقلاب اسلامی را یاری کند؛ زیرا که اساس مبانی این حکمرانی، هماهنگ با نگاه تمدن غربی است و در نسبت با انقلاب اسلامی مثمر ثمر نیست.

براین اساس پرسش اصلی مقاله، یافتن مبانی فلسفی مناسب و مطلوب برای حکمرانی فضای سایبر است و نوآوری مقاله حاضر، در این جهت است که اولاً فضای سایبر را اساساً فضای شناختی معرفی می‌کند و بر اساس آن به مسئله حکمرانی ورود پیدا می‌کند، ثانیا سعی می‌کند که بر این اساس، مبانی ارائه شده در جهت حکمرانی، متناسب با جایگاه تمدن‌سازی حرکت انقلاب اسلامی باشد.

۲ مطالب اصلی

۱.۲ تعریف فضای سایبر

فضای سایبر، در واقع نامی است که تعداد زیادی از کاربردهای امروز فناوری‌های جدید ارتباطی را دربر می‌گیرد. این نام نخستین بار به وسیله ویلیام گیبسون، در رمان «نورومانسر» در سال ۱۹۸۴ ابداع شد. او فضایی تخیلی را فرض می‌کند که در آن تمامی انسان‌ها، ماشین‌ها و منابع اطلاعاتی، از طریق رایانه‌هایی به یکدیگر متصل هستند [۱۲] . تعریف‌های متعددی از فضای سایبر شده است که به عنوان نمونه چند مورد از آن‌ها ذکر می‌شود:

الف) فضای سایبر، فضای فناوری پایه مبتنی بر فناوری اطلاعات و ارتباطات است که در آن، تولید محتوا، پالایش داده، ذخیره سازی داده، پردازش داده و توزیع داده صورت می‌گیرد. فضای سایبر در تعامل با انسان فضای شبکه‌ای را می‌سازد؛ این فضا، خصوصیات مختلف و حتی منحصر به فردی از فضاهای پیشین دارد [۶] ؛ برخی از این خصوصیت‌ها عبارتند از: فرازمانی بودن، بی‌مکانی، وابستگی به فناوری، همه‌جایی بودن و امنیت دسترسی برای همه افراد [۵] .

ب) فضای سایبر، مجموعه‌ای از تعاریف نمادین است که شبکه‌ای از عقاید و باورها را در قالب بیت (bit) رد و بدل می‌کند؛ همچنین نامی است که امروزه تعداد زیادی از کاربردهای فناوری‌های ارتباطی جدید را دربر می‌گیرد [۱۴] .

ج) بهم پیوستگی اطلاعات دیجیتالی و ادراکی بشر، چهارچوبی از شهرنشینی می‌باشد در جایی که جویندگان اطلاعات، لایه‌های اطلاعاتی ذخیره‌شده را هدایت و ارائه می‌کنند .(Ibid)

د) فضای سایبر به عنوان نوعی فرافضا، بیانگر وجود جهانی است که در پی منابع ارتباطی، اطلاعاتی متعدد از طریق شبکه‌های بهم پیوسته رایانه‌ای به وجود آمده است [۱۳] .

با دقت در تعریف‌های ذکر شده، مشخص می‌شود که ویژگی بارز فضای سایبر، شناختی بودن آن است؛ به این معنا که این فضا، اساساً ناظر به قوه شناخت انسان و متفاوت از فضای فیزیکی و مادی است که جسم انسان در آن حضور دارد؛ از همین رو مسئله شناخت در این فضا مسئله اول و اساسی است. این امر از آن جهت مهم است که داده‌های اطلاعاتی بر فرد در فضای سایبر، جنبه معرفتی و آگاهی افزایی دارد؛ همچنین می‌توان آن‌ها را به یک معنای برابر، با صورت‌های ذهنی دانست که حضور آن‌ها برای فرد به معنای داشتن آگاهی به آن است. در اینجا نیز حضور در فضای سایبر و دسترسی داشتن به داده‌های اطلاعاتی، به معنای آگاهی داشتن به آن‌ها است؛ بنابراین مشخص می‌شود که در تحلیل فلسفی، آنچه که در این فضا مورد توجه است، جایگاه شناختی این فضا است. به این معنا که در نسبت با این فضا بحث از شناخت، مسئله اول و اساسی بوده و اساساً تبیین جنبه‌های فضای سایبر، باید با در نظر گرفتن این امر صورت بگیرد. از همین رو در فلسفه اسلامی، فضای سایبر را می‌توان به نوعی از سنخ عالم مثال دانست که برخی از ویژگی‌های غیرمادی،

مانند نبود محدودیت‌های زمانی و مکانی در آن مشهود است [۷]. همان‌طور که ذکر شد، از جمله ویژگی‌های قابل تبیین در این چهارچوب، داده‌های اطلاعاتی است که در این فضا جنبه معرفتی دارد و از این لحاظ باید مورد بررسی قرار بگیرد. این سخن مقدمه‌ای می‌شود برای طرح این پرسش: «با توجه به تعدد قوای شناختی انسان، کدام یک از آن‌ها به شکل عمده در این فضا درگیر هستند؟» که در ادامه به این سؤال پرداخته می‌شود.

۲.۲ تبیین قوای شناختی و نسبت آن با فضای سایبر

برای انسان چهار شکل از ادراک و بالتَّبع، چهار قوه ادراکی ذکر شده است:

الف) ادراک حسی: ادراک صورت‌های اشیای خارجی مقید به ماده و آثار ماده، مانند وضع، کم، کیف و...است و توسط حواس پنجگانه درک می‌شود.

ب) ادراک تخیلی: ادراک صورت اشیای بدون ماده، ولی همراه با آثار ماده است. مانند تصور شی توسط قوه متخیله محسوس بعد از غیبتش.

ج) ادراک وهمی: ادراک معانی جزئی است. مانند حب و بغض جزئی که توسط قوه واهمه درک می‌شود.

د) ادراک عقلی و یا نطق: ادراک معانی کلی است [۱].

اقسام مختلف ادراک بیانگر مراحل مختلف ادراک نیز است؛ به این صورت که انسان با مشاهده شی محسوس، صورتی از آن را به ذهن می‌سپارد که این صورت خیالی، پس از مشاهده شی محسوس و قطع ارتباط با آن در نفس نیز حضور پیدا می‌کند و نفس با عمل تجرید و انتزاع، آن را تبدیل به مفهوم کلی عقلی می‌کند که مجرد از ماده و آثار آن است.

اما نقش نفس در عمل ادراک، محدود به دریافت صورت‌ها نمی‌شود؛ بلکه علاوه بر آن نفس انسان با قوایی که دارد، قدرت بر تجزیه و ترکیب صورت‌ها دارد. هر فردی قادر است در ذهن خود با ترکیب صورت‌های ذهنی، صورت‌های جدیدی خلق کند. مانند آنکه سر انسانی با بدن اسب، کوهی از طلا و یا دریایی از طلای روان و مایع را تصور کند. فیلسوفان اسلامی، استعداد مخصوص ذهن را برای تجزیه و ترکیب ذهنی، قوه متصرفه می‌خوانند و هنگامی که در عمل خود، به منظور تحقیق واقع محسوسات جزئی یا صور خیالیه عمل کند، به نام مخصوص قوه متخیله می‌خوانند. قوه متخیله آزاد است که هر صورتی را که بخواهد و تمایلات نفسانی ایجاب کند، تجزیه، ترکیب، فصل و وصل کند [۱].

با شرحی که داده شد، می‌توان به بحث فضای سایبر پرداخت و این مسئله را مطرح کرد که در فضای سایبر، کدام یک از قوای شناختی انسان درگیر است.

در ابتدا می‌توان نبود شک در به کارگیری قوای حسی انسان (به خصوص قوه بینایی و شنوایی و گاه لامسه به هنگام استفاده از فضای سایبر) را مطرح کرد. بنابراین مرتبه قوای حسی، در حصول آگاهی برای انسان نقش پررنگی دارند. با این حال، نمی‌توان این مرتبه از قوای حسی را مرتبه اصلی در قوه شناختی مرتبط با فضای سایبر دانست؛ زیرا قوای شناخت در این مرتبه، صرفاً حالت انفعالی دارد که از آن به انطباعات

حسی تعبیر می‌شود. اما با دقت در این فضا، درمی‌یابیم که در فضای سایبر نیز نوعی حالت فعال و ایجابی، نسبت با قوای شناختی، وجود دارد؛ زیرا که یکی از کارکردهای اصلی فضای مجازی، دخالت و تغییر واقعیت است. در حقیقت، برخلاف ادراک حسی که انسان با آن واقعیت خارجی را درک می‌کند، این دخل و تصرف برعهده قوای متخیله است و به نحوی در واقعیت تصرف می‌کند؛ زیرا قوای حسی در دریافت و درک واقعیت خارجی، صرفاً جنبه انفعال دارند، اما انسان در فضای مجازی نسبت به واقعیت خارجی نوعی جنبه فعال دارد و می‌تواند در این فضا، واقعیت خارجی را تغییر داده و در آن دخل و تصرف بکند [۱۱].

بنابراین مشخص می‌شود که صرفاً در فضای سایبر، قوای حسی به کار گرفته نمی‌شود. بلکه یکی از کارکردهای اصلی متناسب با این فضا، قوه متخیله است که بر اساس آن می‌تواند داده‌های اطلاعاتی را تولید و ایجاد و در آن‌ها تصرف کند و با توجه به ماهیت غیرفیزیکی و غیرمادی، آن‌ها را به هر شکلی که می‌خواهد تبدیل کند. بنابراین فضای سایبر را می‌توان همانند عالم ذهنی خیال دانست که در آن محدودیت‌های فیزیکی و مادی وجود ندارد و البته با توجه به پیشرفت فناوری مرتبط با فضای سایبر برخلاف عالم ذهن، این عالم خیال به شکل مستقیم قابل اشتراک و انتقال به دیگران است.

قوه دیگری که در کنار قوه متخیله در فضای سایبر دخالت و تأثیر مستقیم دارد، قوه واهمه است؛ زیرا که در این فضا علاوه بر صورت‌های جزئی، معانی جزئی نیز رد و بدل می‌شود. از آنجا که قوه مدرک معانی جزئی قوه واهمه است، بنابراین علاوه بر قوه متخیله، قوه واهمه نیز قوه دیگری است که با ورود کاربر به این فضا مشغول می‌شود.

۳.۲ تمایز میان آگاهی و معرفت در فضای سایبر

مسئله دیگری که در تبیین فضای سایبر به ما کمک شایان توجهی می‌کند، تمایز قائل شدن بین آگاهی و معرفت است. شرح این تمایز به این صورت است که بیان می‌شود: آگاهی اعمّ از معرفت است و هر آگاهی، برابر با معرفت نیست؛ بلکه آگاهی زمانی معرفت به شمار می‌آید که همراه با دو شرط صدق و توجیه باشد.

هرچند که در معرفت‌شناسی معاصر، معرفت گزاره‌ای تنها به عنوان «باور صادق موجه» تعریف شده است، اما در اینجا این معرفت به هرگونه شناختی که در فضای سایبر ایجاد و یا انتقال داده می‌شود، قابل تسری است.

تقسیم‌بندی دیگری که برای آگاهی قابل ذکر است، تقسیم آن به آگاهی بسیط و مرکب است؛ این تقسیم‌بندی را می‌توان از عبارت صدرالمتالهین به دست آورد: «إن العلم کالجهل قد یکون بسیطا و هو عبارة عن ادراک شیئی مع الذهول عن ذلک الادراک و عن التصدیق بان المدرک ماذا و قد یکون مرکبا و هو عبارة عن ادراک شیئ مع الشعور بهذا الادراک و بان المدرک هو ذلک الشیئ» [۴]. بر طبق این عبارت، برای آگاهی دو حالت کلی می‌توان فرض کرد:

الف) حالت اول، حالت بسیط است که صرفاً چیزی برای فرد حاضر است، بدون آنکه فرد به این حضور آگاهی داشته باشد.

ب) حالت دوم که مرتبه قوی‌تر آگاهی است، در جایی است که فرد به حضور آن شی آگاهی داشته باشد.

در حقیقت در آگاهی مرکب دو مرتبه از آگاهی وجود دارد؛ آگاهی دوم را می‌توان آگاهی درجه دوم و یا آگاهی بالاتر نامید. با ذکر این تقسیم‌بندی، این مسئله مطرح می‌شود که: «آگاهی شکل گرفته در مرتبه قوای متخیله، واهمه و یا عاقله، در کدام یک از دو مرتبه آگاهی قرار دارد و آیا هر کدام از آن آگاهی‌ها، بسیط است و یا مرکب؟»

از آنجا که آگاهی متعلق قوای واهمه و یا متخیله مرتبه ضعیفی از آگاهی است، پس این آگاهی از سنخ آگاهی بسیط بوده و لازم نیست که در این گونه موارد، فرد آگاهی مرکب و یا درجه دوم داشته باشد. نمونه‌ی این آگاهی را در کودکان، افراد ساده لوح و یا حتی حیوانات می‌توان مشاهده کرد. برای آن‌ها با دیدن یک تصویر و یا تصور معانی جزئی، این آگاهی حاصل می‌شود، بدون آنکه بخواهند آن را متعلق آگاهی دیگری قرار بدهند و یا مانند خیالاتی که بدون اختیار به ذهن انسان خطور می‌کند، ذهن او را مشغول می‌کند. همگی این امور شواهدی هستند که نشان می‌دهند آگاهی در این سطح، سطح پایینی از آگاهی، و برابر با آگاهی بسیط می‌باشد.

شاهد دیگری که نشان می‌دهد آگاهی در حد قوه متخیله و واهمه، در حد مرتبه آگاهی بسیط است، ذکر نکته‌ای در منطق است که می‌گوید: «قضایای متخیله مفید تصدیق نیستند.» همان‌طور که در صناعت شعر بیان می‌شود، این تصویرسازی‌ها نوعی تصویرسازی خیالی هستند که تصدیقی را به دنبال نداشته و صرفاً در نفس تأثیر می‌گذارد: «هی قضایا لیس من شأنها ان توجب تصدیقا الا آنها توقع فی النفس تخییلات تؤدی الی انفعالات نفسیة من انبساط فی النفس او انقباض و من استهانة بالامر الخطیر او تهویل او تعظیم للشیء الیسیر و من سرور و انشراح او حزن و تألم ...» [۹]. بر همین اساس بیان می‌شود که آگاهی مطرح در حد این دو قوه، آگاهی بسیط است؛ زیرا فرد لازم نیست به آگاهی خود، آگاهی داشته باشد. اما آگاهی قوه عاقله، بر اساس آگاهی درجه دوم و آگاهی مرکب قابل تبیین است؛ زیرا همان‌طور که بیان شد، جایگاه عقل ادراک حقایق کلی است. در بحث ما، ادراک حقایق کلی به این شکل است که قوه عاقله با توجه به اصول و مبانی کلی که دارد، متعلق آگاهی –که از طریق قوای ادراک حسی و همچنین قوه متخیله یا وهم به دست آمده است– و دلیل موجه بودن آن را مورد بررسی و ارزیابی قرار داده و در نهایت به صدق و یا کذب بودن آن آگاهی حکم می‌کند. این سطح از آگاهی، آگاهی مطلوب برای مرتبه انسانیت است. همان‌طور که حکما این مسئله را مطرح می‌کنند، پذیرش و تصدیق امری بدون دلیل و عادت کردن بر آن، به معنای خروج از حدود انسانی است [۸]. بر این اساس، این سخن مطرح می‌شود که در فضای سایبر، ما با دو شکل از آگاهی مواجه هستیم:

الف) آگاهی بسیط: آگاهی‌ای که متعلق آگاهی دیگر نیست و صرفاً در حد قوای شناختی متخیله و یا واهمه شکل می‌گیرد. این شکل از آگاهی، مرتبه پایینی از آگاهی است که هنوز معرفت به شمار نمی‌آید و از لحاظ معرفتی فاقد ارزش است.

ب) آگاهی مرکب: فرد بر اساس دخالت قوه عاقله، با کسب آگاهی درجه دوم، آگاهی اولش را مورد سنجش و ارزیابی قرار می‌دهد. به عنوان مثال انسان با دیدن تصویری در فضای مجازی از فرود آمدن سفینه بر روی کره ماه، به این آگاهی می‌رسد که فضانوردان، کره ماه را فتح کرده‌اند.

در مقام معرفت مرکب، فرد به بررسی این آگاهی می‌پردازد و با متعلق قرار دادن آن با معرفتی دیگر، بررسی می‌کند که: «با توجه به دلایل توجیه‌گر، آیا صرفاً با دیدن یک یا چند تصویر، می‌توان این آگاهی را به عنوان یک معرفت صادق و موجه پذیرفت؟ ارزش معرفتی آگاهی چه میزان است؟»

با توجه به طرح دو شکل از آگاهی، یعنی آگاهی بسیط و آگاهی مرکب، و سنجش آن با قوای شناختی، در اینجا ذکر این نکته ضروری است که آگاهی مطلوب برای انسان، آگاهی درجه دوم، و در مرتبه قوه عاقله است. زیرا آگاهی بسیط، آگاهی‌ای است که در حد حیوانات و یا هوش مصنوعی –بنا بر پذیرش آن به عنوان ابزار هوشمند– قابل تعریف است؛ اما فصل ممیز انسان از سایر موجودات، این است که انسان می‌تواند به آگاهی خود، آگاه بوده و آن را مورد ارزیابی و بررسی قرار بدهد.

مسئله دیگر، برتری و شرافت قوه عاقله بر سایر قوای شناختی انسان، مانند متخیله، وهم و یا حواس پنجگانه است. در فضلیت برتری قوه عاقله بر سایر قوای شناختی، در فلسفه می‌توان مطالب متعددی ذکر کرد؛ زیرا قوه عقل، قوه‌ای الهی است که برای تشخیص خیر از شر به انسان داده شده است؛ عقل نامیدن آن از آن جهت است که مانع از انحراف سایر قوای دیگر انسان می‌شود. همچنین از دلیل عقلی به عنوان «سلطان» یاد می‌شود؛ زیرا سلطنت و برتری قوه عاقله بر سایر قوا، موجب می‌شود که آن‌ها تحت تدبیر و فرمان عقل قرار گرفته [۲] و فرد با استناد به دلیل عقلی و استفاده از سلطنت او، توانایی احتجاج به آن را در مقام نظر، و اخذ آن را به عنوان ملاک حقانیت به آن، در مقام عمل، پیدا کند.

۴.۲ تبیین مسئله حکمرانی فضای سایبر بر اساس قوای شناختی

حکمرانی، در یک تعبیر، به معنای داشتن قدرت برای اعمال اراده بر چیز یا موضوعی است. حکمرانی به مجموعه‌ای از فرآیندها اشاره دارد که با قدرت، اقتدار و نفوذ، سیاست‌ها و رویه‌هایی را برای حکومت کردن در دست گرفته و با آن‌ها هدایت و کنترل می‌کند. حکمرانی همچنین با خلق و بازتولید قوانین، هنجارهای اجتماعی و اقدامات ساختاریافته در ارتباط است. مسئله حکمرانی دربردارنده نهادها، فرایندها و قواعدی است که برنامه‌ریزی، سازمان‌دهی، بسیج منابع و امکانات، هدایت، اجرای تصمیمات و کنترل نتایج یا به عبارتی مدیریت جامعه در حوزه‌های سیاسی، اقتصادی، اجتماعی و فرهنگی را برعهده دارد؛ علاوه بر آن، مشخص می‌کند که قدرت چگونه اعمال می‌شود، چگونه تصمیم‌هایِ تأثیرگذار بر جامعه اتخاذ می‌شوند و چگونه منافع مختلف با چنین تصمیم‌هایی هماهنگ می‌شوند [۳]. با نگاهی به مبانی فلسفی ذکر شده، می‌توان از لحاظ فلسفی، سه شکل از حکمرانی را برای فضای سایبر ترسیم کرد. هرچند که بحث از حکمرانی، بحثی عامی و در علوم مختلف قابل بررسی است و متعاقبا تقسیم‌بندی‌های مختلفی برای آن ذکر می‌شود، اما در اینجا رویکردی فلسفی بیان می‌شود که تحقق اموری مانند اعمال قدرت، نظارت و جعل قوانین بر اساس مؤلفه‌های گوناگون در فضای سایبر را ممکن می‌سازد. بر همین اساس، سه شکل از حکمرانی بر فضای سایبر قابل تحقق است:

الف) حکمرانی بر اساس مؤلفه‌های بیرونی و غیر شناختی. با توجه به تبیینی که از فضای سایبر در این مقاله مطرح شد، مشخص می‌شود که فضای سایبر اساساً یک فضای شناختی است؛ بنابراین می‌توان

یک شکل از حکمرانی را بر طبق مؤلفه‌های غیر شناختی، مطرح کرد و موارد متعددی از آن را مثال زد؛ مانند فیلتر کردن، محدود کردن ترافیک شبکه، از دسترس خارج کردن نرم‌افزار خاص و همچنین وضع قوانین کیفری برای نقض قوانین، مانند جزای نقدی، ضربه شلاق، حبس، و یا در جنبه‌های ایجابی، طراحی سخت افزار مناسب، سرویس‌های اجتماعی و یا پلتفرم‌ها، برای اعمال اراده و نظارت بر این فضا.

ب) شکل دوم از حکمرانی، بر اساس مؤلفه‌های متناسب با قوه متخیله و واهمه است. تفاوت اصلی این شکل از حکمرانی با شکل اول، در این است که مؤلفه‌های حکمرانی در این قسم، مؤلفه‌های شناختی و متناسب با فضای سایبر در حد قوه متخیله و واهمه است. در این شکل از حکمرانی، اموری مانند اعمال قدرت، نظارت و هدایت، جنبه شناختی دارند؛ به این صورت که با تولید محتوای خاص و انتشار آن در فضای سایبر، نوعی جهت‌دهی و نظارت بر فضای سایبر صورت می‌گیرد. مانند آنکه یک کنش‌گر بیگانه توسط رسانه‌ها و شبکه‌های اجتماعی متنوع، اخبار و حوادث منفی یک کشور را برای ایجاد یأس و ناامیدی در یک جامعه مدام تولید و القا بکند و یا آنکه با در دسترس قراردادن سرویس‌های اجتماعی، که متناسب با ترویج مسائل جنسی است، در هدایت جامعه به سوی شهوت‌رانی و فساد تأثیر بگذارد.

در تبیین این شکل از حکمرانی، توجه به این نکته ضروری است که ویژگی اصلی‌ای که برای قوه متخیله و واهمه ذکر شده است، کثرت‌گرایی و تنوع‌طلبی است؛ به گونه‌ای که این دو قوه، تشبیه به دیگ جوشانی شده است که مدام زیر و رو می‌شود [۱۰] و یا همانند گنجشکی می‌ماند که مدام از یک شاخه به شاخه دیگر می‌پرد [۸]. بنابراین حکمرانی برپایه این دو قوه، براساس ارضاکردن ویژگی تنوع‌طلبی و کثرت‌گرایی وهم و متخیله، با تولید هرچه بیشتر محتوا و یا در دسترس قراردادن امکانات بیشتر، برای تولید صورت‌های خیالی و وهمی از سوی کاربران است؛ امری که در فضای سایبر تحت تسلط تمدن غرب کاملاً مشهود است. کاربران با ورود به این فضا، اساساً با حجم عظیمی از اطلاعات و داده‌ها مشغول می‌شوند که تا زمانی طولانی، ذهن کاربر را درگیر خود می‌کند.

ج) شکل سوم از حکمرانی، بر اساس حکمرانی قوه عاقله است. ترسیم این شکل از حکمرانی به این صورت است که مصحح و ملاک مشروعیت اعمال قدرت، نظارت و جعل قوانین برتری و شرافت قوه عاقله بر سایر قوای شناختی است. در این شکل از حکمرانی، محتوای شناختی گوناگون که نقل و انتقال داده می‌شود، تحت نظارت و ارزیابی قوه عاقله در آگاهی درجه دوم قرار می‌گیرد و عقل، با توجه به سنجش، ارزیابی، تأیید و یا رد آن به عنوان معرفت، حکمرانی خود را نسبت به آن آگاهی اعمال می‌کند که در بخش بعدی توضیح بیشتری در رابطه با آن ذکر خواهد شد.

۵.۲ تبیین حکمرانی مطلوب بر فضای سایبر

با تبیین اقسام سه‌گانه حکمرانی، باید به این نکته اصلی توجه داشت که اقسام سه‌گانه حکمرانی، در حقیقت مراحل مختلف حکمرانی هستند که از حکمرانی ضعیف به سوی حکمرانی قوی‌تر مطرح می‌شوند؛ بنابراین دو مرحله بالاتر با مرحله پایین‌تر قابل جمع هستند. با این توضیح می‌توان به توضیح حکمرانی مطلوب بر فضای سایبر پرداخت.

واضح است که شکل اول از حکمرانی، به تنهایی حکمرانی ضعیف است؛ زیرا که مؤلفه‌های دخیل در حکمرانی، امور غیرشناختی و بنابراین بیگانه نسبت به فضای سایبر هستند. هرچند که این امر، به معنای اشتباه و یا ناصحیح بودن این شکل از حکمرانی نیست، اما ابتنا به اعمال قدرت، صرفاً بر مؤلفه‌های غیرشناختی، منجر به ضعف در حکمرانی می‌شود. واضح‌ترین دلیل بر ضعف، این است که در فضای سایبر محدودیت‌های زمانی و مکانی، کم‌رنگ و یا برداشته می‌شوند و در نتیجه، تکیه بر ایجاد محدودیت‌های فیزیکی و یا مادی در دسترسی داشتن به فضای سایبر، نمی‌تواند ثمره چندانی در تحقق حکمرانی مطلوب داشته باشد؛ نمونه واضح آن را در سیاست اعمال فیلترینگ شبکه‌های اجتماعی بیگانه مانند تلگرام و یا اینستاگرام مشاهده می‌کنیم.

شکل دوم از حکمرانی، مرتبه کامل‌تری از حکمرانی است؛ زیرا که مؤلفه‌های دخیل در آن، امور شناختی هستند. بنابراین این شکل از حکمرانی، نسبت به حکمرانی شکل اول، قوی‌تر بوده و از آنجا که نسبت به آن برتر است، بر عوامل آن تأثیر می‌گذارد. به عنوان مثال، از آنجا که کثرت‌گرایی و تنوع‌طلبی ویژگی بارز شکل دوم است، اقتضای این حکمرانی، رهاشدگی در فضای سایبر است، به گونه‌ای که هیچ محدودیتی در تولید و یا محتوای مناسب با قوای متخیله و واهمه وجود نداشته باشد؛ بنابراین نبود فیلترینگ، نبود هیچ‌گونه قانون کیفری یا جزایی در انتقال مطالب، دسترسی بدون محدودیت به اینترنت، طراحی و در دسترس قرار دادن شبکه‌های اجتماعی‌ای که در نقل مطالب غیر اخلاقی و غیر انسانی و مانند آن بدون هیچ قیدی آزاد باشند، اقتضای این حکمرانی می‌باشد.

اما در تبیین نامطلوب بودن حکمرانی بر اساس قوای شناختی متخیله و واهمه، می‌توان به دلایل مختلفی اشاره کرد. شاید یکی از اصلی‌ترین آن‌ها این باشد که تنوع‌طلبی و کثرت‌گرایی، ویژگی ذاتی قوه متخیله و واهمه است؛ بنابراین ابتنای حکمرانی بر پایه آن دو قوه، در نهایت موجب تشتت، اختلاف و از بین رفتن اجتماع انسانی و شئون آن می‌شود. اهمیت این مطلب، از آن جهت است که فضای سایبر، به شکل غیر قابل انکاری تمام شئون اجتماعی انسان را تحت تأثیر خود قرار داده و در آن‌ها نفوذ کرده است؛ بنابراین حاکم شدن کثرت و تنوع در شئون مختلف، در نهایت موجب فساد اجتماع بشری می‌شود. زیرا که پایه اساسی اجتماع و حاکمیت، وجود اصول و مبانی وحدت بخش است که موجب یکپارچگی افراد یک اجتماع می‌شود. در حالی که حکمرانی مرتبه دوم، به سوی سست‌کردن پایه‌های این اصول وحدت‌بخش حرکت می‌کند. نمونه واضح این امر در از بین رفتن نهاد خانواده، تحریک قومیت‌ها و طرح مسائل نژادپرستی، آشوب‌ها و نافرمانی‌های اجتماعی و دعوت به هرج و مرج و خشونت توسط فضای سایبر، در تمدن غرب مشاهده می‌شود.

دلیل دیگری که در نامطلوب بودن این شکل از حکمرانی، قابل ذکر است، این است که این شکل از حکمرانی، ناسازگار با جایگاه حقیقی انسان است؛ زیرا آن‌چنان که بیان شد، قوه وهم و متخیله، قوای حیوانی

هستند و آگاهی‌ای که از این طریق برای انسان حاصل می‌شود، آگاهی مطلوبی برای انسان نیست. در حقیقت حکمرانی بر این اساس، به معنای فرو کاستن انسان به مرتبه حیوانی و یا یک ماشین هوشمند است، که صرفاً داده‌های اطلاعاتی را دریافت و پردازش کرده و بر طبق آن عمل می‌کند؛ بدون آنکه بخواهد ارزش معرفتی آن‌ها را مورد ارزیابی قرار بدهد و آن‌ها را تبدیل به معرفت بکند.

اما در تبیین قسم سوم، بیان می‌شود که مؤلفه‌های حکمرانی مطلوب بر اساس برتری و شرافت قوه عقل است. در حقیقت با توجه به جایگاهی که این قوه در معرفت دارد، این شکل از حکمرانی، صورتی مطلوب برای حکمرانی بر فضای سایبر است. مقتضای این شکل از حکمرانی این است که آگاهی‌ای که در این فضا ایجاد و یا انتقال داده می‌شود، مبتنی بر ارزیابی و بررسی قوه عاقله باشد.

در تبیین اصول و مبانی این شکل از حکمرانی، به این مسئله می‌توان اشاره کرد که شرط لازم این شکل از حکمرانی، نوعی فرهیختگی مبتنی بر سواد رسانه‌ای است. در تشبیهی می توان گفت آن‌چنان که استفاده از خودرو به عنوان وسیله حمل و نقل، مستلزم وجود قوانینی برای جلوگیری از هرج و مرج و بی نظمی است و نمی‌توان به شکل رها و بدون قانون از آن استفاده کرد، استفاده از فضای مجازی نیز نیازمند وجود قوانینی است که توسط مرتبه بالای شناخت یعنی قوه عاقله جعل و اعتبار شده باشد؛ شرط استفاده از آن در انتقال محتوای شناختی و یا ایجاد آن است. در این نگاه، کارکرد سواد رسانه‌ای در این است که برای کاربران، این امکان را فراهم می‌کند که آگاهی ابتدایی و بسیط خود را که در فضای سایبر کسب می‌کنند، تبدیل به آگاهی درجه دوم کرده و آن را متعلق آگاهی‌ای قرار بدهند که مناسب با قوه عاقله باشد. بنابراین سواد رسانه‌ای، پایه و زمینه حکمرانی قوه عاقله بر فضای سایبر است و تحقق آن، منوط به گذراندن آموزش‌ها و فرهیختگی لازم، برای کسب مهارت‌های سواد رسانه‌ای از سوی آحاد افراد یک جامعه است.

دومین مسئله در تبیین چنین حکمرانی، این است که این حکمرانی، دو حکمرانی دیگر را تحت تأثیر خود قرار می‌دهد؛ به این صورت که در بحث تولید محتوای متناسب با وهم و متخیله، و همچنین به کارگرفتن مؤلفه‌های غیرشناختی، در ذیل این قسم از حکمرانی تعریف می‌شود. در حقیقت قوه عاقله، تولید و ایجاد محتوای هماهنگ با قوه وهم و متخیله را تحت نظارت و تسلط خود در می‌آورد، و تنوع و کثرت‌طلبی این دو قوه را در ذیل اصول عقلی خود تعریف می‌کند؛ سپس بر این اساس، بر کثرت و تنوع گرایی قوه وهم و متخیله نظارت می‌کند.

همچنین این شکل از حکمرانی، مؤلفه‌های غیر شناختی حکمرانی را نیز تحت تأثیر خود قرار می‌دهد؛ به عنوان مثال بر اساس حاکمیت قوه عاقله، می‌توان فیلتر کردن و یا وضع قوانین جزایی کیفری را پذیرفت. زیرا سلطنت و تسلط قوه عاقله این اقتضا را فراهم می‌کند که در امور غیر شناختی مرتبط با فضای سایبر نیز دخالت بکند و آن‌ها را با هماهنگ با اصول مبانی خود بیاورد.

اما نکته سوم که به نوبه خود، نکته مهم و شایسته توجهی می‌باشد، این است که تحقق حکمرانی مطلوب بر فضای سایبر، تنها زمانی امکان‌پذیر است که ارتباط و تعامل حکومت و مردم با یکدیگر، به شکل عام و کلی بر اساس قوه عقل و هماهنگ با آن باشد. به عنوان مثال زمانی که مؤلفه‌های حکمرانی در یک جامعه بر اساس سودگرایی و لذت‌طلبی تنظیم می‌شود، این سودگرایی و لذت‌طلبی که هماهنگ با قوه واهمه و متخیله است، در فضای سایبر خودش را به صورت محتوای متناسب با رهاشدگی، بی‌بندوباری، محتواهای فریبنده و

شیادی نشان می‌دهد؛ از آنجا که اساس این اجتماع هماهنگ با ارزش‌های عقلی نیست، نمی‌توان به شکل مطلوبی از مؤلفه‌های قوه عاقله و قدرت و سلطنت آن در بحث حکمرانی استفاده کرد.

۳ نتیجه‌گیری

با توجه به آنچه گذشت، مشخص می‌شود که در بحث از حکمرانی بر فضای سایبر، فرهنگ و تمدن غربی داعیه‌دار حکمرانی بر اساس ویژگی‌های وهم و متخیله است. هرچند که ممکن است برخی از حکومت‌ها، در نسبت با محدوده جغرافیای خود موفق عمل کرده و این فضا را به خوبی کنترل کرده باشند، اما این نسخه برای جمهوری اسلامی ایران که در تقابل با تمدن غرب در یک جنگ شناختی حرکت می‌کند، مفید و سودمند نیست؛ آن‌چنان که به کار گرفتن مؤلفه‌های حکمرانی مبتنی بر امور غیر شناختی نیز در این تقابل نمی‌تواند به شکل موثری مفید باشد. بنابراین مسئله اصلی و مهم برای خروج از حکمرانی منفعل و تبدیل آن به حکمرانی فعال، توجه به حکمرانی بر اساس مرتبه عقل، و در اختیار گرفتن فضای شناختی سایبر بر اساس سلطنتی است که مستند به این قوه است. واضح است که سواد رسانه‌ای که در این سطح مطرح می‌شود، نوعی به فعلیت رساندن و آگاه کردن افراد به جایگاه و مرتبه‌ی مطلوب آگاهی برای انسان است؛ بنابراین باید غایت و هدف از سواد رسانه‌ای تحقق این مهم و تربیت و پروش افراد جامعه، برای واجد شدن این توانایی باشد که بتوانند آگاهی خود را در مرتبه‌ی قوه عاقله، مطرح و مورد بررسی قرار بدهند؛ از همین رو، در بحث از سواد رسانه‌ای نیازمند الگوی بومی هستیم که بر طبق مؤلفه‌های فوق تنظیم و تدوین بشود. همچنین در بحث از پیام‌رسان‌ها، شبکه‌های اجتماعی و مانند آن، اصل قرار دادن آگاهی درجه دوم و مطرح در حد مرتبه قوه عاقله، این اقتضا را دارد که این ابزارها به گونه‌ای طراحی بشوند که امکان ارزیابی و بررسی آگاهی انتقال داده شده را برای افراد فراهم بیاورند و صرفاً در جهت نقل و انتقال آگاهی بدون هیچ ضابطه نباشند.

مراجع

[۱] ابن سینا، **شرح الاشارت و التّنبیهات**، خواجه نصیر الدین طوسی، قم، نشر البلاغه، ۱۳۷۵.

[۲] جوادی آملی، عبدالله، **تفسیر تسنیم**، قم، نشر اسراء، ۱۳۸۹.

[۳] دباغ، سروش و نفری، ندا، **تبیین مفهوم خوبی در حکمرانی خوب**، نشریه مدیریت دولتی، پاییز و زمستان، صص۳-۱۸، ۱۳۸۸.

[۴] صدر الدین شیرازی، محمد بن ابراهیم، **الحکمة المتعالیة في الاسفار العقلیه**، سوم، بیروت، دار احیاء التراث العربي، ۱۹۸۱.

[۵] عباسی قادی، مجتبی و خلیلی کاشانی، مرتضی، **تأثیر اینترنت بر هویت ملی**، تهران پژوهشکده مطالعات راهبردی، ۱۳۹۰.

[۶] فیروز آبادی، سید ابوالحسن، **فضای مجازی و تحولات آن**، مشهد ، انتشارات آستان قدس رضوی، ۱۳۹۸.

[۷] گنجور، مهدی، **واقع انگاری فضای مجازی (تحلیلی فلسفی از واقعیت مجازی با تاکید بر مبانی حکمت متعالیه)**، خردنامه صدرا ، ش ۱۰۵، ۴۱-۵۴، ۱۴۰۰.

[۸] مطهری، مرتضی، **مجموعه آثار شهید مطهری**، قم، صدرا، ۱۳۷۸.

[۹] مظفر، محمدرضا، **المنطق**، قم، جامعه مدرسین قم، بی‌تا.

[۱۰] نراقی، احمد، **معراج السعاده**، اول، تهران، پیام آزادی، ۱۳۷۸.

[۱۱] هایم، مایکل، **متافیزیک واقعیت مجازی**، سروناز تربتی، تهران، رخ داد نو، ۱۳۹۰.

[12] Watson, James, Hill, Anne, ***Dictionary of Media and communication Studies***, Oxford University Press, 2012.

[13] Saha, T. K. ***War on Words in cyberspace-Legal constraints and conflicts between rights of privacy and freedom of speech***. Journal of intellectual properly Rights14(6): 489-500, 2009.

[14] Heim, Michael, ***The Metaphysics of Virtual Reality***, New York, Oxford, 1993.

اهمیت و کاربرد تحلیل کلان‌داده‌های زیرساخت ارتباطی-مخابراتی در کشور

احسان ترکمان منش [۱]

[۱] کارشناسی ارشد هوش‌مصنوعی و پژوهشگر دانشگاه جامع امام حسین(ع)، تهران
ehsan.tr@email.com

چکیده

رشد فزاینده صنعت ارتباطات خصوصاً در دهه اخیر منجربه فراگیر شدن خدمات الکترونیک و افزایش ضریب نفوذ اینترنت گشته، که در نتیجه آن تولید انبوه داده‌هایی ارزشمند از فعالیت کاربران در صنعت مخابرات است. در حال حاضر روزانه صدها میلیون رکورد داده مخابراتی در کشور تولید می‌گردد، از دیگر سو با فراگیری نسل پنجم ارتباطی (5G) با تمرکز بر اینترنت اشیا و همچنین ادغام فناوری‌های ارتباطی با هوش‌مصنوعی در نسل ششم ارتباطی (6G) تحلیل کلان داده‌های مخابراتی در آینده‌ای نزدیک اهمیتی مضاعف خواهد یافت. لذا توجه جدی به تحلیل داده در سطح مدیریت راهبردی جامعه بسیار مهم می‌نماید. در حال حاضر داده‌های مخابراتی به چهار دسته داده‌های جزئیات تماس، داده‌های ثبت آی‌پی، داده‌های شبکه و داده مشتریان تقسیم می‌شوند که با بهره‌برداری صحیح از الگوریتم‌های داده‌کاوی نه تنها می‌توان گامی مهم در راستای تحقق حکمرانی سایبری کشور برداشت، بلکه با تطبیق سایر داده‌ها امکان بسط تحلیل‌ها به حوزه‌های کلان فرهنگی، سیاسی، امنیتی و اقتصادی وجود دارد.

کلمات کلیدی: تحلیل‌داده، حاکمیت داده، کلان داده، مخابرات، هوش‌مصنوعی، فضای سایبر، حاکمیت سایبری.

۱ مقدمه

توسعه چشمگیر فناوری‌های ارتباطی در دهه اخیر، موجب افزایش ضریب نفوذ اینترنت شده، به‌نحوی‌که در حال حاضر شرکت‌های مخابراتی در جهان، تولیدکننده حجم عظیمی از داده‌ها هستند. حجم داده‌ها به‌قدری زیاد است که تجزیه‌وتحلیل دستی آن، اگر غیرممکن نباشد بسیار دشوار است. طبق اعلام سازمان تنظیم مقررات و ارتباطات رادیویی، در حال حاضر تعداد مشترکین اینترنت پهن باند بیش از ۱۱۶ میلیون نفر و ضریب نفوذ اینترنت بیش از ۱۳۸ درصد است. این موضوع سبب تولید حجم انبوهی از کلان‌داده‌های ارتباطی در زیرساخت‌های مخابراتی کشور شده است. تحلیل داده مخابراتی، از روش‌هایی است که با استفاده از داده‌های

جمع‌آوری شده از سیستم‌ها و شبکه‌های ارتباطی، می‌توان به بهبود عملکرد، افزایش امنیت و کشف بینش‌های مفید در این حوزه پرداخت. در حال حاضر کاربران اینترنت طیف وسیعی از افراد با نیازهای متفاوت را تشکیل می‌دهند؛ لذا تحلیل صحیح و به‌موقع این داده‌ها، می‌تواند منجر به تصمیم‌سازی‌های کلان و ارائه روندهای آینده‌پژوهانه در گستره سرزمینی کشور را در پی داشته باشد. طی بررسی‌هایی که در این پژوهش صورت گرفت، مشخص شد که موضوع تحلیل کلان‌داده‌های مخابراتی در ایران، توسط مجامع دانشگاهی آن‌طور که باید موردتوجه قرار نگرفته و امید است که این پژوهش، بتواند ابعاد کلان اهمیت پرداختن به این موضوع را بیان نماید؛ چراکه یکی از مراحل تحقق حکمرانی سایبری در کشور، تحقق مبحث حاکمیت داده بوده و از ابزارهای این موضوع نیز بهره‌برداری از فناوری‌های تحلیل کلان‌داده و الگوریتم‌های هوش مصنوعی در راستای کمک به اتخاذ راهبردهای کلان در ابعاد اجتماعی، فرهنگی، سیاسی، اقتصادی و امنیتی در کشور است.

۲ پیشینه پژوهش

مفهوم تحلیل داده و کاربردهای آن در صنعت مخابرات در کشورهای پیش‌گام صنعت ارتباطات موضوعی جاافتاده است، اما علی‌رغم اینکه کلان‌داده‌های صنعت مخابرات شامل میلیاردها رکورد اطلاعات می‌شوند، متأسفانه به‌صورت جدی توسط مراکز علمی و دانشگاهی در ایران به آن توجه نشده است.

در صنعت ارتباطات مخابراتی، در طول دوره نسل اول شبکه‌های تلفن همراه 1G، تجزیه‌وتحلیل داده‌ها عمدتاً بر روی کارایی تجاری و عملیاتی متمرکز بود. داده‌های تولید شده مربوط به تراکنش‌های ساده مانند پیامک و تماس‌های صوتی بود. نفوذ دستگاهی که باعث ایجاد بسترهای داده برای استفاده از تجزیه‌وتحلیل می‌شود، بسیار محدود بود. در نتیجه، توسعه نرم‌افزارهای تحلیلی، شامل ابتکارات داخلی و اختصاصی بود. در اوایل دهه ۹۰ میلادی، شبکه‌های نسل دوم 2G از ارتباطات دیجیتال با استفاده از دسترسی چندگانه بخش زمانی[1] و دسترسی چندگانه تقسیم کدی[2]، خدمات جدیدی مانند پیام‌های متنی، پیام‌های تصویری، پیام‌های چندرسانه‌ای[3]، فکس و پست صوتی را به ارمغان آوردند. دستگاه‌های نسل دوم با قابلیت ذخیره‌سازی و پردازش محدود طراحی شدند. با ترکیب همه‌ی اینها، ارائه‌دهندگان ارتباطات از راه دور، قادر به انجام برخی از عملیات‌های فشرده داده، مانند خودکارسازی گزارش‌ها و داشبوردهای سازمانی بودند. راه‌حل‌های فنی، بر پایه‌ی پایگاه‌های داده مرسوم و انبارهای داده ساخته شدند که از روش‌های متمایز فناوری‌های انباشت، استخراج و تحلیل اطلاعات استفاده می‌نمودند. از سال ۲۰۰۰، دستگاه‌های تلفن همراه 2G به‌تدریج با محصولات 3G جایگزین گشتند؛ شبکه 3G و گوشی به‌گونه‌ای طراحی شد که دارای سرعت ۲ مگابیت بر ثانیه، برای پاسخگویی به تقاضای چندرسانه‌ای از طریق سیستم تلفن همراه باشد. در طول این مرحله، اپراتورهای مخابراتی از تحلیل رفتار دارایی متمرکز به تحلیل رفتار مشتری متمرکز روی آوردند. انواع داده‌های جدیدی از قبیل محتواهای گرافیکی در دسترس قرار گرفتند و به اپراتورهای مخابراتی قابلیت‌های تحلیل

[1] Time Division Multiple Access (TDMA)
[2] Code division multiple Access (CDMA)
[3] MMS

پیچیده‌ای را ارائه کردند. نسل چهارم شبکه‌های تلفن همراه موسوم به LTE 4G در سال ۲۰۰۹ در شهر استکهلم سوئد راه‌اندازی شد که امکان دانلود ۱۰۰ مگابیت بر ثانیه و آپلود ۵۰ مگابیت در ثانیه را فراهم کرد [۳]. نسل پنجم ارتباطات سیّار سلولی یا 5G که از سال ۲۰۱۲ موردتوجه جامعه جهانی قرار گرفته، و پیشرفتی در ارتباطات بین‌فردی ایجاد کرده است. 5G می‌تواند ارتباط بین افراد و اشیا، و ارتباط فی‌مابین اشیا را درک کند. سرعت انتقال آن می‌تواند به 10Gps برسد که ۱۰۰ برابر بیشتر از 4G بوده و از نظر ظرفیت ذخیره‌سازی، ۱۰۰۰ برابر بیشتر از 4G ظرفیت دارد. علاوه بر این، نسل جدیدی از فناوری ارتباطات است [۴]. البته در حال حاضر این نسل از فناوری ارتباطی هنوز در ایران فراگیر نشده و به‌صورت محدود توسط اپراتورهایی مانند ایرانسل، به‌صورت آزمایشی مورداستفاده قرار گرفته است. اما نسل بعدی ارتباطی که هنوز به‌صورت آزمایشگاهی در مراکز پژوهشی دنیا در حال ارزیابی و توسعه بوده، 6G است. این فناوری با هوش مصنوعی عجین شده و در آینده‌ای نه‌چندان دور موجب تحول جدی در صنعت ارتباطات خواهد شد [۵]. محققان بسیار در حال ارزیابی کارایی و نقاط اثرگذاری این فناوری هستند و خیلی از ابعاد آن هنوز به‌درستی احصا نشده است.

بررسی این موضوع که هر نسل از فناوری‌هایی که در بالا اشاره شد چه نوع داده‌هایی تولید می‌کند، بسیار حائز اهمیت است. متأسفانه جنبه‌های تحلیل داده‌های مخابراتی در ایران، اغلب بر روی مدیریت مشتریان و داده‌های مبتنی بر شبکه‌های 2G متمرکز شده است. ولایتی و همکاران (۱۳۹۶) رویکردهای داده‌کاوی در تقسیم‌بندی مشتریان با تمرکز بر صنعت مخابرات را بررسی کردند. آنان دریافتند، با واکاوی رفتار مشتریان می‌توان سیاست‌های خاص هر مشتری را احصاء نمود. داده‌های مورد بررسی آنان، صرفاً مبتنی بر پرداخت‌های مشتریان متمرکز بوده و از داده‌های ارتباطی بهره‌برداری نکردند [۱]. کاهانی و بهکمال (۱۳۹۶) نسبت به دیگر پژوهش‌های صورت‌گرفته در ایران بیشترین بهره را از کلان‌داده‌های مخابراتی کشور برده‌اند. با توجه به ماهیت گراف پایه داده‌های مخابراتی، ایشان از پایگاه‌داده Neo4j به‌منظور نیل به هدف خود در حوزه دسته‌بندی و شناسایی مشترکین استفاده کرده‌اند. باید بیان نمود که بهره‌برداری از حجم قابل‌ملاحظه داده (بیش از ۱ میلیارد و ۲۰۰ میلیون رکورد) و تنوع در استفاده از اپراتورهای همراه و ثابت (مخابرات، همراه اول و ایرانسل) نقطه قوت پژوهش مذکور است [۲]. تقریباً تمامی پژوهشگران در ایران صرفاً موضوع مدیریت مشتریان را در نظر گرفته و به سایر ابعاد کاربرد کلان‌داده‌های مخابراتی که می‌تواند در حوزه تحقق حکمرانی سایبری کشور نقشی مؤثر را ایفا نماید، نپرداخته‌اند.

۳ انواع داده‌های مخابراتی

شرکت‌های مخابراتی عموماً بر حسب نوع کارکرد، به سه دسته‌ی ارائه‌دهنده اینترنت ثابت[۴]، اپراتور تلفن همراه[۵] و اپراتور شبکه مجازی موبایل[۶] تقسیم‌بندی می‌شوند [۶]. وجود چندین اپراتور و ارائه‌دهنده اینترنت در کشور، به همراه افزایش چشمگیر کاربران تلفن‌های هوشمند و ظهور فناوری‌های جدید ارتباطی، موجب

[4] Fixed Communication Provider (FCP)
[5] Mobile Network Operators (MNO)
[6] Mobile Virtual Network Operator (MVNO

تولید انبوهی از داده‌ها گشته است. اما باید گفت که ساختار تولید داده‌های مبتنی بر لاگ و مشتریان در تمامی اپراتورها، به چهار دسته تقسیم‌بندی شده که در ادامه مورد بررسی قرار خواهد گرفت.

۱.۳ داده‌های ثبت تماس

برای هر تماس که توسط یک کاربر در اپراتورهای تلفن انجام می‌گیرد، یک رکورد داده تماس[۷] تولید می‌شود. آن‌ها به طور سنتی برای مقاصد صورت‌حساب و مهندسی شبکه استفاده می‌شوند. با توجه به اینکه تلفن‌های همراه به بخشی جدایی‌ناپذیر از زندگی روزمره بخش بزرگی از جمعیت کره زمین تبدیل شده‌اند، اگر داده‌های ثبت تماس به‌صورت هدفمند جمع‌آوری شود، تلفن همراه و شبکه‌های سلولی در ترکیب با داده‌های دیگر از جمله تحلیل شبکه‌های اجتماعی برخط، زمینه تحلیل ارزشمندی را ایجاد می‌کنند [۷].

۲.۳ داده‌های ثبت جزئیات پروتکل اینترنت(آی‌پی)

داده‌های ثبت آی‌پی، برای جمع‌آوری و ثبت آمار ترافیک داده تولید شده در یک شبکه، استفاده می‌شود. جمع‌آوری داده‌های آی‌پی[۸]، بینش شبکه را در مورد ظرفیت، استفاده مشترک و نگهداری فعال شبکه ارائه می‌کند و می‌تواند جریان‌های درآمد جدیدی را ایجاد کند. داده‌های مذکور همچنین از تحلیل ترافیک برای شناسایی تراکم شبکه و برنامه‌ریزی برای سرمایه‌گذاری در ظرفیت شبکه، مانند گسترش و تقسیم شبکه پشتیبانی می‌کند. تحلیل استفاده از مشترکین، بخش‌های بازاریابی و فروش را قادر می‌سازد تا کمپین‌هایی را بر اساس استفاده از شبکه مشترک و الگوهای مصرف، راه‌اندازی کنند تا درآمد را افزایش دهند و مدیریت تجربه مشتری را هدایت کنند. علاوه بر این، می‌توان برای پشتیبانی از تیم‌های عملیاتی در تقویت مدیریت خطا و عملکرد استفاده کرد [۸].

۳.۳ داده‌های شبکه

داده‌های شبکه، وضعیت اجزای سخت‌افزار و نرم‌افزار در شبکه را توصیف می‌کند. شبکه‌های مخابراتی پیکربندی بسیار پیچیده‌ای از تجهیزات هستند که از هزاران جزء به‌هم‌پیوسته تشکیل شده‌اند. هر عنصر شبکه، قادر به تولید پیام‌های خطا و وضعیت است که منجر به تولید حجم عظیمی از داده‌های شبکه می‌شود. این داده‌ها باید ذخیره و تحلیل شوند تا از عملکردهای مدیریت شبکه پشتیبانی کنند. این داده‌ها حداقل شامل یک مهر زمان، رشته‌ای که به طور منحصربه‌فرد بخش سخت‌افزار یا نرم‌افزار تولیدکننده پیام را شناسایی می‌کند و کدی که توضیح می‌دهد چرا پیام تولید می‌شود، خواهد بود [۹].

۴.۳ داده‌های مشتریان

شرکت‌های مخابراتی، مانند سایر کسب‌وکارهای بزرگ، ممکن است میلیون‌ها مشتری داشته باشند. این به معنای نگهداری پایگاه‌داده از اطلاعات این مشتریان است. این اطلاعات، شامل اطلاعات نام، آدرس و هرگونه

[7] Call Data Record (CDR)
[8] Internet Protocol Detail Record (IPDR)

اطلاعات تکمیلی از قبیل جنسیت، میزان تحصیلات، شغل و داده‌هایی ازاین‌قبیل است. داده‌های مشتری اغلب همراه با داده‌های دیگر، به‌منظور بهبود نتایج استفاده می‌شود. برای مثال، داده‌های مشتری معمولاً برای تکمیل اطلاعات جزئیات تماس، هنگام تلاش برای شناسایی کلاهبرداری تلفنی استفاده می‌شود [۹].

۴ چالش‌های اساسی تحلیل داده‌های ارتباطی

پیش از پرداختن به کاربردهای تحلیل کلان‌داده‌های مخابراتی، شناسایی چالش‌ها بسیار مهم است. در این بخش، چالش‌ها و مزایای اجرای کلان‌داده در بخش مخابرات را معرفی کرده‌ایم. اپراتورهای مخابراتی در مواجهه با انبوه داده‌های تولید شده توسط دستگاه‌های متصل، رفتارهای مشتریان، شبکه‌های رسانه‌های اجتماعی، سوابق داده‌های تماس، پورتال‌های دولتی و اطلاعات صورت‌حساب با مشکلاتی مواجه هستند.

مالکا و براون (۲۰۱۵) بر اساس مطالعه خود در رابطه با تحلیل کلان‌داده‌ها در آفریقای جنوبی، چالش‌ها را به سه بخش فناورانه، سازمانی و محیطی دسته‌بندی نموده‌اند [۱۰]. در این پژوهش ما به دو چالش می‌پردازیم که به نظر نگارندگان تأثیر بیشتری در ایران دارند.

۱.۴ چالش‌های فناورانه

الف) عدم وجود معماری مرجع برای پیاده‌سازی تحلیل داده‌های مخابراتی: معماری تحلیل کلان‌داده، نیاز به ادغام بسیاری از منابع داده‌های مختلف دارد. در واقع، یکپارچه‌سازی داده‌ها چالش بزرگی محسوب می‌شود. گردآوری قطعات داده در یک بستر متمرکز می‌تواند یک کار چالش‌برانگیز باشد [۱۰].

ب) کیفیت داده بد: بر اساس نظرسنجی مکنزی که بر روی ۲۷۳ بازیکن مخابراتی در سراسر جهان انجام شد، مشخص شد که دلیل اصلی شکست پروژه‌های تحلیل کلان‌داده، به دلیل کیفیت بد داده است. این موضوع را می‌توان با تعداد زیادی از سیستم‌ها و عملکردهای موجود در مجموعه راه‌حل‌های اپراتورهای مخابراتی و با حجم داده‌های مدیریت شده توضیح داد [۱۱].

ج) عملکرد و ذخیره‌سازی: تقاضای فزایندهٔ ترافیک داده که توسط رسانه‌های اجتماعی و برنامه‌های کاربردی تلفن همراه[۹] هدایت می‌شود، اپراتورها را مجبور به یافتن راه‌های جدیدی برای مدیریت و استفاده از داده‌های خود می‌کند. در واقع راه‌حل‌های سنتی مبتنی بر پایگاه‌های داده مرسوم[۱۰]، محدودیت‌های خود را از نظر عملکرد، ذخیره‌سازی و مدیریت انواع مختلف داده‌ها، در قیاس با پایگاه‌داده‌های بدون ساختار نشان داده‌اند. البته در چند سال اخیر و با پیشرفت‌های تجهیزات ذخیره‌ساز و همچنین توسعه پایگاه‌داده‌هایی مانند الستیک سرچ[۱۱]، این موضوع تا میزانی مرتفع شده است [۱۱].

[9] Over-The-Top (OTT)
[10] RDBMS
[11] Elasticsearch

۲.۴ چالش‌های سازمانی

الف) مالکیت و کنترل: از رایج‌ترین راه‌حل‌های تحلیل کلان‌داده، ایجاد تیم هوش تجاری است. چراکه اکثر سازمان‌ها، تاحدامکان عملکردهای هوش تجاری و انبار داده را از طریق یک تیم فنی واحد کنترل می‌کنند. در واقع، طبق نظر، پروژه‌های تحلیل کلان‌داده را به‌عنوان یک ابتکار فناوری در نظر نمی‌گیرند، آنها را بیشتر به‌عنوان یک برنامه ی تجاری که نیاز به دانش فنی دارد، می‌دانند.

ب) کمبود مهارت: در واقع، چالش‌برانگیزترین موضوعات پروژه‌های تحلیل کلان‌داده، یافتن یک تیم توانمند است. پروژه‌های تحلیل کلان‌داده، در قیاس با پروژه‌های هوش تجاری که بیشتر سازمان‌ها در طول چندین دهه آن را ساخته‌اند، همیشه به‌عنوان فناوری جدید در نظر گرفته می‌شود. تجزیه‌وتحلیل پیشرفته به کارکنانی با دانش عمیق در حوزه‌های مختلف، از علم داده گرفته تا قوانین حفظ حریم خصوصی در سراسر جهان، همراه با درک کسب‌وکار مخابراتی نیاز دارد [۱۲].

البته در کنار دو چالش مذکور، عدم وجود پایگاه‌داده آزمایشی مناسب و منابع علمی در کشور، موجب شده که توجه پژوهشگران نسبت به این حوزه منعطف نشود. در واقع یکی از چالش‌های جدی در ایران محسوب می‌گردد.

۵ کاربردهای تحلیل کلان‌داده‌های ارتباطی

در صنعت ارتباطات، تحلیل کلان‌داده یک تغییردهنده بازی است، زیرا به اپراتورها این فرصت را می‌دهد تا از مجموعه‌داده‌های جدید بهره‌برداری کنند و اطلاعات ارزشمندی را برای درک بهتر رفتار مشتری استخراج کنند. اپراتورها پیشنهادهای هدفمندتری را ارائه می‌دهند، در نتیجه درآمدها را بهبود می‌بخشند و هزینه‌ها را کاهش می‌دهند. اما نباید به این موضوع در حد بهره‌برداری اپراتورهای ثابت و همراه در کشور نگاه نمود.

شکل ۱: آمار کلان وضعیت اینترنت در کشور طبق اعلام سازمان تنظیم مقررات و ارتباطات رادیویی وزارت ارتباطات و فناوری اطلاعات در سال ۱۴۰۱

آنچه از شکل ۱ برمی‌آید، در حال حاضر بیش از ۱۱۶ میلیون کاربر اینترنت پهن باند در کشور وجود دارد. یعنی اغلب کاربران بیش از یک حساب اینترنت پهن باند دارند. این موضوع اهمیت تحلیل داده‌های مخابراتی – ارتباطی را در بحث راهبری جامعه دوچندان می‌کند. در ادامه به برخی از کاربردهای تحلیل کلان‌داده‌های مخابراتی اشاره خواهد شد.

جدول ۱: کاربردهای تحلیل کلان داده‌های مخابراتی

کاربرد	نوع داده	مثال
شناسایی الگوی رفتاری جامعه	CDR+IPDR	با بهره‌گیری از کلان‌داده‌های مخابراتی می‌توان الگوهای رفتاری جامعه را مورد مطالعه علمی قرار داد و از آن به‌منظور تصمیم‌سازی‌های راهبردی بهره جست. به‌عنوان مثال احصاء الگوی سفر مردم در ایام تعطیلات نمونه‌ای از این دست است.
امنیت سایبری	CDR+IPDR+Network	بهره‌برداری صحیح از داده‌های مخابراتی، می‌تواند به کشف سوابق داده‌های غیرعادی و رویدادهایی که ممکن است نشان‌دهنده یک حادثه امنیتی باشد، کمک نماید.
تحلیل ترافیک شبکه	IPDR	تشخیص فعالیت باج‌افزار، نظارت بر استخراج غیرقانونی داده‌ها و فعالیت اینترنت، ارائه داشبوردهای بلادرنگ متمرکز بر فعالیت کاربر و شبکه، از طریق بهره‌برداری از فناوری سامانه بررسی و تحلیل شبکه میسر می‌شود. تشخیص بدافزارها، تشخیص نفوذ، تشخیص تقلب، شناسایی و پیش‌بینی تهدیدات داخلی از جمله این موارد است [۱۳].
شناسایی ناهنجاری	CDR+IPDR	نظارت بر سوابق داده تماس در زمان واقعی برای تشخیص رفتارهای غیرعادی و مراقبت پیشگیرانه شبکه و تشخیص ناهنجاری [۱۴]. با نگاه راهبردی‌تر، توانایی تشخیص ناهنجاری‌های اجتماعی مانند: اعتراضات و راهپیمایی‌ها، با بهره‌گیری از داده‌های مذکور امکان‌پذیر است.
ارتقای کیفیت خدمات	CDR+IPDR	اپراتورها می‌توانند بینش عملی در مورد شبکه‌های خود به دست آورند تا آنها را پایدار، بهینه و مقیاس‌پذیر کنند [۱۵].

۶ نتیجه‌گیری

در ابتدای این پژوهش، به معرفی نسل‌های ۱ تا ۶ فناوری‌های ارتباطی پرداخته شد. بعد از آن، به بررسی تاریخچه تحلیل داده‌های مخابراتی در ایران پرداخته شد و مشخص گردید که این موضوع، در میان پژوهشگران کشور موردتوجه واقع نشده است. داده‌های مخابراتی کشور به چهار دسته تقسیم‌بندی شدند و بر مبنای آن، کاربردهای کلان در حوزه‌های مختلف مورد بررسی واقع شد. بهره‌برداری صحیح از انبوه کلان‌داده‌ها، نه‌تنها می‌تواند در راستای تحقق حکمرانی سایبری مؤثر باشد، بلکه با بهره‌برداری از سایر داده‌ها از قبیل شبکه‌های اجتماعی برخط، می‌توان به تحلیل‌های راهبردی در حوزه اقتصادی، اجتماعی، سیاسی و امنیتی رسید که این

موضوع، در نهایت، منجر به تصمیم‌سازی‌های استراتژیک خواهد شد که از برنامه‌های آتی نگارنده، به‌منظور ارتقای سطح کیفی تحلیل داده‌های مذکور است. وزارت ارتباطات به‌عنوان متولی اصلی صنعت ارتباطات، می‌تواند نقشی مؤثر در توجه جامعه علمی کشور به کاربردهای کلان‌داده‌های مخابراتی ایفا کند. یکی از موضوعاتی که در این حوزه مغفول مانده، عدم توجه به پویایی داده‌های مذکور است. چراکه داده‌های مخابراتی، مبتنی بر زمان هستند و می‌توان با الگوریتم‌های سری زمانی، اقدام به پیش‌بینی روندها نمود، درصورتی‌که اغلب به‌عنوان داده‌های ایستا، در پایگاه‌داده‌های مبتنی بر گراف تحلیل می‌شوند.

مراجع

[۱] م. ولایتی، ف. سین‌زاده لطفی و م. شهریاری، «رویکرد داده کاوی در بخشبندی بازار مشتریان به منظور اتخاذ استراتژی‌های کارا»، اقتصاد مالی، جلد ۴۱، صص ۲۴۳-۲۶۶، ۱۳۹۶.

[۲] م. کاهانی و ب. بهکمال، «شناسایی شبکه ارتباطی مشترکین تلفن ثابت شرکت مخابرات با استفاده از پایگاه داده گرافی»، کنفرانس بین المللی وب پژوهی، ۱۳۹۶.

[3] "World's first 4G/LTE network goes live today in Stockholm", 2009. [Online]. Available: https://www.tmcnet.com.

[4] R. Gai, X. Du and S. Ma, "A Summary of 5G applications and prosprcts of 5G in the Internet of Things", International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), pp. 858-863, 2021.

[5] T. B. Ahammed, R. Patgiri and S. Nayak, "A vision on the artificial intelligence for 6G communication", ICT Express, vol. 9(2), pp. 197-210, 2023.

[6] A. Aniruddha and C. M. Dippon, "Voluntary relationships among mobile network operators and mobile virtual network operators: An economic explanation", Information Economics and Policy , pp. 21.1 (2009): 72-84., 2009.

[7] M. N. Mouchili, J. William Atwood and S. Aljawarneh, "Call data record based big data analytics for smart cities", in Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems, 2019.

[8] "FAQ on IPDR: Its Value Beyond Bandwidth Usage", 2022. [Online]. Available: https://www.incognito.com/tutorials/faq-bandwidth-monitoring-with-ipdr/.

[9] G. M. Weiss, "Data mining in telecommunications", Data Mining and Knowledge Discovery Handbook, pp. 1189-1201, 2005.

[10] I. Malaka and I. Brown, "Challenges to the Organisational Adoption of Big Data Analytics: A Case Study in the South African Telecommunications Industry", in annual research conference on South African institute of computer scientists and information technologist, 2015.

[11] J. Bughin, "Reaping the benefits of big data in telecom", Journal of Big Data, vol. 3.1, pp. 1-17, 2016.

[12] T. Pearson and R. Wegener, "Big data: the organizational challenge", Bain Co, 2013.

[13] "Using Data Mining Techniques in Cybersecurity Solutions", 2022. [Online]. Available: https://www.apriorit.com/dev-blog/527-data-mining-cyber-security.

[14] M. S. Parwez, D. B. Rawat and M. Garuba, "Big Data Analytics for User-Activity Analysis and User-Anomaly Detection in Mobile Wireless Network", Transactions on Industrial Informatics, vol. 13, p. 2058–2065, 2017.

[15] S. Jain, M. Khandelwal, A. Katkar and J. Nygate, "Applying big data technologies to manage QoS in an SDN", in International Conference on Network and Service Management (CNSM), 2016.

راهبردهای مواجهه با فناوری‌های نوظهور از منظر امنیت سایبری

محمدحسن فرخی[۱]، خداداد هلیلی[۲]

[۱]دانشجوی دکتری امنیت سایبر، دانشگاه عالی دفاع ملی
mhf1364@gmail.com
[۲]استادیار، عضو هیات علمی دانشکده کامپیوتر، دانشگاه شهید ستاری، تهران
kh.halili@ssau.ac.ir

چکیده

همزمان با گسترش فضای سایبر و فناوری‌های مرتبط با آن، حملات و تهدیدات سایبری نیز مدام درحال‌توسعه هستند. در بسیاری از کشورها، امنیت سایبری به یکی از اولویت‌های اساسی در دستیابی به امنیت ملی تبدیل شده است. به‌منظور پیشگیری از آثار مخرب این حملات و جلوگیری از ایجاد خدشه در امنیت ملی، لازم است علاوه بر تمهیدات فنی، راهبردهای مناسبی در سطح ملی، تدوین و اجرا شود. هدف اصلی این مقاله بررسی راهکارهای مؤثر برای بهبود امنیت سایبری و ارائه راهبردهایی برای مواجهه هوشمند با فناوری‌های مورداستفاده در فضای سایبر، است. بدین منظور پس از بررسی فناوری‌های هوش مصنوعی، زنجیره‌بلوکی، اینترنت اشیا، رایانش ابری، بیومتریک و رباتیک و کاربردهای آن‌ها، راهبردهای پیشنهادی مطرح شده است. نتایج این تحقیق نشان می‌دهد توسعه فناوری‌های امنیتی، آموزش و افزایش آگاهی کاربران، توسعه قوانین و سیاست‌های امنیتی، همکاری بین کشورها، و توسعه فرهنگ امنیت سایبری موجب بهبود امنیت سایبری می‌شود بدین منظور راهبردهایی مانند توسعه فناوری‌های امنیتی، آموزش و افزایش آگاهی کاربران، توسعه قوانین و سیاست‌های امنیتی، همکاری بین کشورها، و توسعه فرهنگ امنیت سایبری در این مقاله موردتوجه و بررسی قرار گرفته است.

کلمات کلیدی: فضای سایبر، فناوری‌های نوظهور، امنیت سایبری، هوش مصنوعی.

۱ مقدمه

فناوری‌های نوظهور به سرعت درحال توسعه و استفاده در همه جای جهان هستند. با پیشرفت فناوری، فضای سایبر نیز به یکی از مهم‌ترین بخش‌های زندگی انسان تبدیل شده است. با افزایش استفاده از این فناوری‌ها، حملات سایبری نیز درحال گسترش بوده و برای مقابله با آنها، نیاز به راهبردهای مناسب و هوشمند داریم. حمله بدافزار استاکس‌نت – ساخت مشترک دولت متخاصم آمریکا و رژیم جعلی اسرائیل - که در سال ۱۳۸۹

تأسیسات هسته‌ای ایران از جمله نیروگاه بوشهر را هدف قرار داد، از جمله رخدادهای سایبری مورد توجه در سال‌های گذشته است که زیرساخت‌های حیاتی ملی کشور را مورد هدف قرار داده است.

امنیت سایبری به‌عنوان یکی از مهم‌ترین اولویت‌های امنیت ملی در جهان مطرح است و سرمایه‌گذاری وسیعی در این زمینه انجام شده است. برای درک اهمیت موضوع، در انگلیس در سال ۲۰۲۲، شرکت‌های کوچک ۱۸۷ میلیون پوند در بخش امنیت سایبری سرمایه‌گذاری کردند که درآمد تولید شده توسط این شرکت‌ها با ۱۴ درصد افزایش به ۱.۱۰ میلیارد پوند رسیده است[1]؛ بنابراین، برای جلوگیری از حملات سایبری و حفاظت از اطلاعات حساس و مهم کشور، لازم است تا راهبردهای مناسبی در این زمینه تدوین و اجرا شود. در این مقاله، ابزارها و راهکارهایی برای بهبود امنیت سایبری مورد توجه قرار گرفته است.

برای بهبود امنیت سایبری، مقوله‌هایی مانند توسعه فناوری‌های امنیتی، آموزش و افزایش آگاهی کاربران، توسعه قوانین و سیاست‌های امنیتی، همکاری بین کشورها و توسعه فرهنگ امنیت سایبری، حائز اهمیت است. در این تحقیق، ضمن معرفی برخی از فناوری‌های نوظهور در عرصه فضای سایبر، راهبردهایی به‌صورت تجویزی برای بهبود امنیت سایبری و مواجهه با این فناوری‌ها ارائه شده است.

۲ پیشینه تحقیق

در مقاله شکری و موسوی (۱۳۹۸) هوش مصنوعی به‌عنوان یکی از ابزارهای مفید برای تشخیص و پیشگیری از حملات سایبری مطرح شده است. در این مقاله به استفاده از الگوریتم‌های هوش مصنوعی و تحلیل داده‌های سایبری، برای شناسایی الگوهای غیرعادی در رفتار کاربران، دستگاه‌ها و شبکه‌ها پرداخته شده است. محمدی و همکاران (۱۳۹۹) نیز کاربردهای هوش مصنوعی را در امنیت سایبری بررسی کرده‌اند.

کراسبی و همکاران (۲۰۱۶) و ناریامن (۲۰۱۶) با بررسی کاربردهای بلاک‌چین، آنها را به‌عنوان یک راه‌حل امنیتی برای محافظت از داده‌های حساس و ارائه خدمات امن به کاربران در فضای سایبر، مورد بررسی قرار داده‌اند.

رومن و همکاران (۲۰۱۳)، در مقاله‌ای با عنوان قابلیت‌ها و چالش‌های امنیت و حریم خصوصی در اینترنت اشیا، راهکارهای امنیتی برای محافظت از اطلاعات و کاربران را ارائه داده‌اند. لی و همکاران (۲۰۱۸) نیز در مقاله‌ای با عنوان امنیت و حریم خصوصی در اینترنت اشیا به این مسئله پرداخته‌اند.

در مقاله خسروی و عرفانی (۲۰۲۱) با اشاره به تهدیدات امنیتی در فناوری رباتیک، مدیریت دسترسی به ربات‌ها و اطمینان از دسترسی افراد مجاز، به‌عنوان راه‌حل‌های امنیتی در این حوزه مطرح شده است.

۳ فناوری‌های نوظهور درفضای سایبر و چالش‌های امنیتی آنها

در این بخش به معرفی برخی از پرکاربردترین فناوری‌های مرتبط با فضای سایبر اعم از هوش مصنوعی و الگوریتم‌های آن، فناوری بلاک‌چین، اینترنت اشیا، رایانش ابری، فناوری رباتیک و کاربردهای آنها و برخی مکانیسم‌های امن‌سازی آنها پرداخته شده است.

[1] https://www.gov.uk

۱.۳ هوش مصنوعی

در حوزه امنیت سایبری، هوش مصنوعی می‌تواند به‌عنوان یکی از ابزارهای مفید برای تشخیص و پیشگیری از حملات سایبری استفاده شود. هوش مصنوعی می‌تواند در تشخیص و پیشگیری از تهدیداتی که از سمت افراد خطرناک، گروه‌های تروریستی و افرادی که با اهداف خلاف قانون شکل می‌گیرند، مفید باشد. با استفاده از الگوریتم‌های هوش مصنوعی و تحلیل داده‌های مختلف، می‌توان به شناسایی الگوهای غیرعادی در رفتار افراد و گروه‌های مشکوک، و همچنین پیش‌بینی عملیات تروریستی و خطرات مختلف پرداخت. باتوجه‌به پیشرفت‌های روزافزون در حوزه هوش مصنوعی، انتظار می‌رود که در آینده این فناوری به‌عنوان یکی از ابزارهای اصلی در حوزه امنیت سایبری مورد استفاده قرار گیرد [۱]. برای تشخیص حملات سایبری با استفاده از هوش مصنوعی، الگوریتم‌های مختلفی وجود دارند که هرکدام به‌صورت خاص برای تشخیص انواع مختلفی از حملات سایبری طراحی شده‌اند [۲]. در جدول ۱، برخی از کاربردهای الگوریتم‌های هوش مصنوعی در امنیت سایبری دسته‌بندی شده‌اند.

۲.۳ بلاک‌چین

بلاک‌چین به‌صورت یک زنجیره از بلوک‌ها که حاوی اطلاعات مختلفی ازجمله تراکنش‌ها و معاملات است، عمل می‌کند. هر بلوک، شامل یک هش[۲] از داده‌های قبلی، هش داده‌های جدید و یک مهر زمانی[۳] است که نشان‌دهنده زمان ایجاد بلوک می‌باشد. هش، یک مقدار رمزگذاری شده است که با استفاده از تابع هش، از داده‌های ورودی به‌عنوان ورودی تولید می‌شود. بلاک‌چین به‌عنوان یک فناوری متن‌باز، در ابتدا برای پشتیبانی از ارزهای دیجیتال مانند بیت‌کوین طراحی شده بود؛ اما امروزه، در صنایع متنوعی از جمله بانکداری، بیمه، صنایع غذایی، حوزه حمل‌ونقل و غیره به کار گرفته شده است [۳].

بلاک‌چین به‌عنوان یک سیستم توزیع‌شده، از مشکلات امنیتی و نقص‌های سامانه‌های مرکزی برخوردار نیست. بااین‌وجود، توسعه شبکه‌های خصوصی بلاک‌چین، به‌عنوان یک راه‌حل امنیتی و افزایش کارایی در فضای سایبری، مورد توجه قرار گرفته است و بسیاری از سازمان‌ها و شرکت‌ها از این روش برای محافظت از داده‌های حساس و ارائه خدمات امن به کاربران استفاده می‌کنند [۵] و [۸].

۳.۳ اینترنت اشیا

در اینترنت اشیا[۴]، داده‌های حساس جمع‌آوری و منتقل می‌شوند، امنیت اطلاعات از جمله چالش‌های اصلی در این فناوری به حساب می‌آید. برای حفاظت از اطلاعات حساس، از راهکارهایی همچون رمزنگاری، شناسایی و احراز هویت، مدیریت دسترسی و مانیتورینگ استفاده می‌شود [۹].

برای مقابله با چالش‌های امنیتی در حوزه اینترنت اشیا، لازم است که به توسعه نیروی انسانی متخصص در امنیت سایبری و آشنایی با فناوری‌های نوظهور توجه شود. توسعه قوانین و مقررات مناسب برای حفاظت

[2] Hash
[3] Timestamp
[4] IoT: Internet of Things

جدول ۱: الگوریتم‌های هوش مصنوعی در امنیت سایبر

عنوان	شرح الگوریتم
شبکه‌های عصبی مصنوعی	در این الگوریتم ابتدا داده‌های مربوط به حملات سایبری و داده‌های عادی جمع‌آوری می‌شود. سپس با انجام آموزش‌های لازم و یادگیری ماشینی، شبکه عصبی مصنوعی، داده‌های حاوی حملات سایبری را تشخیص داده و اقدامات مناسب برای مقابله با این حملات را نیز به‌صورت خودکار انجام می‌دهد.
درخت تصمیم Decision Trees	الگوریتم‌های درخت تصمیم یکی از پرکاربردترین الگوریتم‌های یادگیری ماشینی هستند و برای حل مسائل طبقه‌بندی و پیش‌بینی از آنها استفاده می‌شود. درخت تصمیم، ساختاری سلسله‌مراتبی دارد که در هر سطح آن، یک مجموعه از تصمیم‌ها برای تقسیم داده‌ها به دو گروه انجام می‌شود. هر برگ این درخت، به یک کلاس خاص یا یک مقدار پیش‌بینی برای داده‌های ورودی متصل می‌شود. درخت تصمیم با استفاده از الگوریتم‌هایی مانند ID3، C4.5 و CART ساخته می‌شود.
درون‌یابی	با استفاده از الگوریتم‌های درون‌یابی، می‌توان گروه‌هایی از داده‌های مشابه را شناسایی کرد و برای ارائه پیش‌بینی‌های دقیق‌تر، از آنها استفاده کرد. در الگوریتم‌های درون‌یابی، داده‌ها به دو صورت مختلف می‌توانند گروه‌بندی شوند: گروه‌بندی سلسله‌مراتبی (Hierarchical) و گروه‌بندی غیر سلسله‌مراتبی (Non-hierarchical). در این مدل، گروه‌ها به‌صورت سلسله‌مراتبی تشکیل می‌شوند و می‌توان به‌راحتی به سطح‌های مختلف درخت دسترسی داشت. در گروه‌بندی غیر سلسله‌مراتبی، داده‌ها به گروه‌های مشابه تقسیم می‌شوند، بدون توجه به سطح سلسله‌مراتبی. برخی از مهم‌ترین الگوریتم‌های درون‌یابی عبارت‌اند از: K-Means، DBSCAN، Gaussian Mixture Mod-els (GMM) و Hierarchical Clustering.
ماشین بردار پشتیبان Support Vector Machines	الگوریتم‌های ماشین بردار پشتیبان یا SVM، یکی از الگوریتم‌های پرکاربرد در یادگیری ماشین است که برای مسائل طبقه‌بندی و بازشناسی الگو استفاده می‌شود. این الگوریتم‌ها با استفاده از داده‌های برچسب‌گذاری شده، سعی می‌کنند بهینه‌سازی مدل خود را انجام دهند و سپس با استفاده از مدل به‌دست آمده، برچسب‌گذاری داده‌های بدون برچسب را انجام می‌دهند. یکی از الگوریتم‌های شبه نظارتی معروف، الگوریتم شبکه‌های مولد است که در آن با استفاده از داده‌های برچسب‌گذاری شده، یک مدل شبکه عصبی برای تولید داده‌های مصنوعی آموزش داده می‌شود.

از اطلاعات حساس در این حوزه و ارتقای امنیت شبکه‌های اینترنت اشیا باید به طور جدی مورد توجه قرار گیرد. برای این منظور، باید از روش‌های مانیتورینگ و شناسایی تهدیدات و فایروال و آنتی‌ویروس استفاده کرد. همچنین، باید از روش‌های دسترسی محدود به داده‌ها و شناسایی دومرحله‌ای استفاده کرد [۴].

باتوجه به اینکه اینترنت اشیا به‌عنوان یکی از فناوری‌های نوظهور و مهم در دنیای دیجیتال شناخته می‌شود، توجه به امنیت در این حوزه بسیار حائز اهمیت است. باتوجه به رشد روزافزون اینترنت اشیا و تعداد دستگاه‌های هوشمند، لازم است که راهکارهای امنیتی مناسب برای حفاظت از اطلاعات حساس در این حوزه توسعه داده شود تا بتوان از امنیت اطلاعات کاربران و جامعه محافظت کرد. در جدول ۲ برخی از چالش‌های امنیتی در حوزه اینترنت اشیا آمده است.

۴.۳ رایانش ابری

رایانش ابری به‌عنوان یکی از فناوری‌های نوظهور در فضای سایبر، شامل استفاده از سرورهای ابری برای ذخیره‌سازی و پردازش اطلاعات است. این فناوری باعث شده است که سازمان‌ها و شرکت‌ها بتوانند به راحتی از خدمات ذخیره‌سازی و پردازش ابری استفاده کنند و نیازی به سرورهای خود نداشته باشند. از دیگر مزایای استفاده از فناوری ابر می‌توان به دسترسی سریع و آسان به داده‌ها، افزایش قابلیت اطمینان و کارایی در پردازش داده‌ها، کاهش هزینه‌های سرورها و مراکز داده، افزایش قابلیت اطمینان و پایداری در ارائه خدمات اشاره کرد. این امر به‌عنوان یک راه‌حل اقتصادی و عملی برای ذخیره‌سازی داده‌ها و پردازش آنها در نظر گرفته می‌شود [۱۰].

باتوجه‌به اینکه این فناوری از طریق اینترنت وصل می‌شود، تهدیدات امنیتی متعددی نیز برای آن وجود دارد. برای مقابله با این تهدیدات، باید دقت ویژه در مدیریت داده‌ها و اطلاعات حساس و افزایش امنیت این سرورها و رمزگذاری اطلاعات بر روی آنها داشت. همچنین، باید از روش‌های امنیتی مانند دسترسی محدود به داده‌ها و شناسایی دومرحله‌ای استفاده کرد. روش‌های رمزگذاری نیز می‌توانند به‌عنوان یک راهکار مؤثر برای افزایش امنیت در فناوری ابر مورداستفاده قرار گیرند. همچنین برای افزایش امنیت در فضای ابری، باید از روش‌های پیشگیرانه و شناسایی تهدیدات استفاده کرد. به‌عنوان مثال: شناسایی و جلوگیری از حملات DDoS (حملات توزیع‌شده از سرویس)، هوشمندسازی فرایندهای مدیریت و افزایش سطح اطمینان از امنیت و محرمانگی داده‌ها می‌تواند مؤثر باشد.

۵.۳ فناوری بیومتریک

فناوری بیومتریک یکی از فناوری‌های مهم و پیشرفته در حوزه امنیتی است که برای شناسایی افراد بر اساس ویژگی‌های فیزیکی مانند اثر انگشت، چهره و قلب استفاده می‌شود. این فناوری برای بسیاری از کاربردهای امنیتی، از جمله ورود به سیستم‌های کامپیوتری، حضوروغیاب در محیط کار، ورود به ساختمان‌های خصوصی و عمومی و ... استفاده می‌شود. باتوجه‌به اینکه در فناوری بیومتریک، اطلاعات حساس و شخصی کاربران شامل ویژگی‌های فیزیکی آنها مانند اثر انگشت و چهره استفاده می‌شود، تهدیدات امنیتی متعددی نیز برای آن وجود دارد. برای مقابله با این تهدیدات، باید از روش‌های امنیتی مانند رمزنگاری داده‌ها و افزایش امنیت

جدول ۲: چالش‌های امنیتی در اینترنت اشیا

عنوان	چالش‌های امنیتی
ارتباطات امن	در حوزه اینترنت اشیا، ارتباطات امن به‌عنوان یکی از چالش‌های اصلی مطرح است. برای ایجاد ارتباط امن در اینترنت اشیا، از روش‌هایی مانند رمزنگاری، شناسایی و احراز هویت، مدیریت دسترسی و مانیتورینگ استفاده می‌شود. همچنین، محافظت از اطلاعات حساس در ارتباطات در اینترنت اشیا بسیار حائز اهمیت است. برای محافظت از اطلاعات حساس کاربران، از روش‌هایی مانند رمزنگاری، توکن‌سازی و احراز هویت استفاده می‌شود. به‌عنوان‌مثال، از پروتکل امنیتی OAuth برای احراز هویت و توکن‌سازی استفاده می‌شود.
تهدیدات امنیتی	در حوزه اینترنت اشیا، تهدیدات امنیتی به‌عنوان یکی از چالش‌های اصلی مطرح است. یکی از نقاط ضعف موجود در اینترنت اشیا، نبود استانداردهای امنیتی مناسب است. باتوجه به اینکه بسیاری از دستگاه‌های اینترنت اشیا از پورت‌های باز و ناامن برای ارتباط با اینترنت استفاده می‌کنند، دسترسی به دستگاه‌ها توسط هکرها ممکن است بسیار ساده باشد. همچنین، حملات سایبری مانند حملات DDoS و malware نیز می‌توانند برای دستگاه‌های اینترنت اشیا خطرناک باشند.
رویکردهای امنیتی	فناوری رمزنگاری یکی از رویکردهای امنیتی اساسی در اینترنت اشیا است. با استفاده از رمزنگاری، اطلاعات جمع‌آوری‌شده در دستگاه‌های اینترنت اشیا رمزگذاری شده و به‌صورت ایمنی به سرورهای مرکزی ارسال می‌شوند. مدیریت دسترسی به دستگاه‌های اینترنت اشیا نیز یکی از رویکردهای مهم در حوزه امنیت است. با استفاده از این رویکرد، دسترسی به دستگاه‌ها و داده‌های حساس، تنها برای کاربران مجاز در دسترس خواهد بود و افراد نامتعهد نخواهند توانست به آنها دسترسی پیدا کنند. این رویکرد با استفاده از فناوری‌هایی مانند الگوریتم‌های تشخیص تهدیدات و تشخیص شبکه‌های نفوذی انجام می‌شود.
نیروی انسانی	متخصص در حوزه اینترنت اشیا، دسترسی غیرمجاز به داده‌های حساس، تهدیدات سایبری جدی برای امنیت گسترش این حوزه در آینده نزدیک محسوب می‌شوند. یکی از نیازهای اساسی در حوزه امنیت اینترنت اشیا، توسعه دانش و مهارت‌های متخصصان در حوزه امنیت سایبری است. متخصصانی که به این حوزه مسلط هستند، می‌توانند تهدیدات سایبری را تشخیص داده و در برابر آنها مقابله کنند. برای این منظور، توسعه دوره‌های آموزشی و مدارک مرتبط با امنیت سایبری می‌تواند به افزایش دانش و مهارت‌های متخصصان در این حوزه کمک کند.

اطلاعات حساس استفاده کرد تا داده‌های حساس موجود در این فناوری محافظت شوند.

یکی از تهدیدات امنیتی در فضای فناوری بیومتریک، حملات سایبری است که می‌تواند باعث دسترسی غیرمجاز به داده‌های حساس و اطلاعات شخصی کاربران شود. برای محافظت از داده‌های حساس و اطلاعات شخصی کاربران در فضای فناوری بیومتریک، باید از روش‌های رمزنگاری داده‌ها استفاده کرد تا داده‌های موجود در سامانه‌های بیومتریکی در هنگام انتقال و ذخیره‌سازی محافظت شوند. همچنین، برای افزایش امنیت در فضای فناوری بیومتریک، باید از روش‌های شناسایی تهدیدات و جلوگیری از وقوع حملات استفاده کرد [۷].

۶.۳ فناوری رباتیک

یکی از تهدیدات امنیتی در فضای رباتیک، دسترسی غیرمجاز به ربات‌ها است. برای مقابله با این تهدید، باید از روش‌های مدیریت دسترسی به ربات‌ها استفاده کرد تا دسترسی به ربات‌های حساس فقط برای افراد مجاز امکان‌پذیر باشد. همچنین، برای افزایش امنیت در فضای رباتیک، باید از روش‌های شناسایی تهدیدات و جلوگیری از وقوع حملات استفاده کرد. یکی دیگر از تهدیدات امنیتی در فضای رباتیک، سرقت اطلاعات حساس و داده‌های مربوط به فعالیت‌های رباتیک است. برای مقابله با این تهدید، باید از روش‌های امنیتی مانند رمزنگاری داده‌ها استفاده کرد تا از دسترسی غیرمجاز به داده‌های حساس در ربات‌ها جلوگیری شود [۶].

۴ راهبردهای مواجهه با فناوری‌های نوظهور در فضای سایبر

برای مواجهه هوشمند با فناوری‌های نوظهور در فضای سایبر و بهبود امنیت ملی سایبری جمهوری اسلامی ایران، در این مقاله، راهبردهای زیر بر اساس مطالعه مبانی نظری و به‌صورت تجویزی به شرح زیر احصاء شده است:

۱. **تقویت همکاری و تعامل با سازمان‌ها و نهادهای امنیت سایبری جهانی:** با توسعه روابط بین‌المللی، می‌توان به شناسایی و تبدیل تهدیدات سایبری به فرصت‌های اقتصادی و تجاری کمک کرد. در سطح بین‌الملل، سازمان‌هایی مانند اتحادیه اروپا، سازمان همکاری اقتصادی و توسعه و سازمان همکاری شانگهای و... در حوزه امنیت سایبری فعالیت می‌کنند. ایجاد شبکه‌های همکاری بین سازمان‌ها و تشکیل گروه‌های کاری مشترک در حوزه امنیت سایبری، می‌تواند به افزایش همکاری‌های بین‌المللی و تبادل تجربیات و دانش کمک کند.

۲. **به‌کارگیری فناوری هوش مصنوعی در تحلیل داده‌های سایبری:** به‌وسیله هوش مصنوعی، می‌توان الگوها و رفتارهای غیرعادی را در داده‌های سایبری شناسایی کرده و به رصد و پیشگیری از حملات سایبری کمک کرد. یکی از روش‌های استفاده از هوش مصنوعی در تحلیل داده‌های سایبری، استفاده از شبکه‌های عصبی پیچشی است. با استفاده از این روش، می‌توان به شناسایی الگوهای غیرعادی در داده‌های

سایبری پرداخت. همچنین، استفاده از الگوریتم‌های یادگیری ماشین مانند شبکه‌های عصبی بازگشتی[5]، می‌تواند به شناسایی الگوهای پیچیده‌تر در داده‌های سایبری کمک کند.

۳. استفاده از بلاک‌چین برای جلوگیری از حملات سایبری: بلاک‌چین به‌عنوان یک فناوری نوین، به جلوگیری از حملات سایبری مورد توجه قرار گرفته است. بلاک‌چین به‌عنوان یک فناوری توزیع‌شده، این امکان را فراهم می‌کند تا اطلاعاتی که در آن ذخیره می‌شوند، بدون وساطت ثبت و بازیابی شوند. این به این معنی است که هیچ‌کس نمی‌تواند به‌راحتی اطلاعات را تغییر دهد یا حذف کند. این امکان از بلاک‌چین، به جلوگیری از حملات سایبری و تغییر داده‌های مربوط به آنها کمک می‌کند.

۴. توسعه سیاست‌های امنیتی مبتنی بر ریسک: در این رویکرد، به‌جای تمرکز بر روی حملات و تهدیدات خاص، به تشخیص خطرات و ریسک‌های موجود در سازمان‌ها و اطلاعات مرتبط با آنها پرداخته می‌شود تا بتوان بهبود امنیت ملی را تسهیل کرد.

۵. ارتقای آموزش کاربران در زمینه امنیت سایبری: یکی از مزایای آموزش کاربران در مورد امنیت سایبری، کاهش خطرات سایبری است. با آموزش کاربران در مورد رفتارهای امنیتی، می‌توان خطرات سایبری را کاهش داد و از حملات سایبری جلوگیری کرد. همچنین، با آموزش کاربران در مورد محافظت از داده‌های مرتبط با امنیت ملی، می‌توان از دسترسی غیرمجاز به اطلاعات حساس و سوءاستفاده از آنها جلوگیری کرد.

۶. توسعه فرهنگ امنیت سایبری: برای توسعه فرهنگ امنیت سایبری، راهکارهای زیر پیشنهاد می‌شود: ۱. آموزش و آگاهی‌بخشی، ۲. ترویج مسئولیت‌پذیری ۳. ترویج امنیت در سازمان‌ها، ۴. ترویج امنیت در محصولات و خدمات، ۵. ترویج همکاری و هماهنگی، ۶. ترویج ارزش‌های امنیتی، و ۷. ترویج تحقیق و توسعه.

۵ نتیجه‌گیری

فناوری‌های نوینی که در فضای سایبر به کار می‌روند، می‌توانند برای توسعه و پیشرفت جوامع و کشورها بسیار مفید باشند. بااین‌حال، برای استفاده مؤثر و امن از این فناوری‌ها، نیاز به برخورداری از راهبردهای مناسب در فضای سایبر و امنیت ملی جمهوری اسلامی ایران است.

یکی از راهبردهای مهم در این زمینه، آموزش و آگاهی‌بخشی افراد و کاربران این فناوری‌ها است. باید به آنها آموزش داد که چگونه از این فناوری‌ها به نحو مؤثر و امن استفاده کنند و به اطلاعات شخصی و امنیت خود دقت کنند. همچنین، باید از طریق توسعه و ارتقای فناوری‌های امنیتی مانند رمزنگاری، تشخیص نفوذ، و مانیتورینگ، در فضای سایبر امنیت را تضمین کرد. علاوه بر این، باید مقررات و قوانین مناسبی برای استفاده

[5] Recurrent Neural Networks

از این فناوری‌ها در فضای سایبر و امنیت ملی جمهوری اسلامی ایران، تنظیم و اجرا کرد. این قوانین باید در جهت حفاظت از امنیت و حریم خصوصی کاربران و جامعه به کار گرفته شوند.

در نهایت، باید همکاری میان دولت، خصوصی‌سازی، و دانشگاه‌ها به‌منظور توسعه فناوری‌های امنیتی در فضای سایبر و امنیت ملی جمهوری اسلامی ایران، تقویت شود. این همکاری‌ها می‌توانند به افزایش امنیت و توسعه پایدار در فضای سایبر کمک کنند و تأثیر مثبتی بر رشد و پیشرفت جامعه و کشور داشته باشند. برخی از پیشنهادهای اجرایی برای این موضوع عبارت‌اند از:

- تشکیل واحد ملی اقدام‌کننده در خصوص فناوری‌های نوظهور سایبری ذیل مرکز ملی فضای مجازی
- توسعه و تدوین سند ملی راهبردی مواجهه با فناوری‌های نوظهور سایبر کشور
- تدوین سند ملی هوش مصنوعی و اخلاق به‌کارگیری آن

مراجع

[۱] محمدی، محمدجواد و علیجانی، بهاره (۱۳۹۸). هوش مصنوعی و نقش آن در امنیت سایبری، صص ۶۲-۷۷.

[۲] شکری، علی و موسوی، سید مجید (۱۳۹۸). کاربردهای هوش مصنوعی در امنیت سایبری. هشتمین کنفرانس ملی فناوری اطلاعات و ارتباطات، تهران، ایران

[۳] محمدی، علی؛ آقایی، علیرضا و رحمانی، مهدی (۱۳۹۹). هوش مصنوعی و کاربردهای آن در امنیت سایبری. مجله فناوری اطلاعات و ارتباطات در علوم تربیتی، صص ۶۹-۸۲.

[4] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys , Tutorials 247-276.

[5] Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. Applied Innovation, 71-81.

[6] Khosravi, H., Erfani, S. M. (2021). Security Threats and Solutions in Robotics Technology. Journal of Information Security and Cybercrimes 1-7.

[7] Li, S., Xu, L. D., Zhao, S. (2018). Security and privacy in the internet of things: Current status and future directions. Future Generation Computer Systems, 339-346.

[8] Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

[9] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

[10] Tapscott, D., Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin.

شناسایی تروریست در شبکه‌های اجتماعی به‌وسیله اطلاعات منبع‌باز

مهدي كوره‌پز[۱]، رضا شیبانی[۲]

[۱] گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد مشهد، ایران
korehpaz65@gmail.com
[۲] استادیار انفورماتیک پزشکی، مدیر گروه مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد مشهد، ایران
reza.shni@gmail.com

چکیده

در فعالیت‌های اطلاعاتی، امنیتی و انتظامی، برای شناسایی اهداف، از نظارت بر شبکه اجتماعی استفاده می‌شود. این رویکرد به تحلیل‌گران کمک می‌کند تا گروه‌های مخفی مانند یک شبکه ضد امنیتی، یک خانواده جنایتکار سازمان‌یافته یا یک باند تبهکار را با تحلیل داده‌ها شناسایی و از رشد افراط‌گرایی به هر شکل ممکن جلوگیری شود. فعالیت‌های تروریستی در سراسر جهان منجر به توسعه روش‌های پیچیده برای تجزیه و تحلیل گروه‌ها و شبکه‌های تروریستی شده است. تحقیقات فعلی و گذشته نشان داده است تجزیه و تحلیل شبکه‌های اجتماعی (SNA) رویکردی برای تجزیه و تحلیل شبکه‌های تروریستی و درک بهتر ساختار زیربنایی یک گروهک و شناسایی بازیگران کلیدی در گروه و پیوندهای آنها در سراسر سازمان است. در این رابطه مهم‌ترین چالش، حفظ حریم خصوصی برای دسترسی به اطلاعات است. این مقاله جنبه‌های مختلف تحلیل شبکه‌های اجتماعی را در مورد تروریسم، با در نظر گرفتن داده‌های تجربی و مطالعات مبتنی بر داده‌های منبع‌باز بررسی می‌کند. جمع‌آوری داده‌های باز بدون نیاز به داشتن مجوز از مراجع قضایی و با در نظر گرفتن اطلاعات منتشر شده توسط خود فرد در سطح وب صورت می‌گیرد. کار ما در درجه اول مطالعه‌ای بر روی انواع مختلف شبکه‌ها و گره‌های تروریستی غیرمتمرکز قابل دسترس بوسیله جمع‌آوری داده‌های باز است.

کلمات کلیدی: تحلیل شبکه‌های اجتماعی، اسینت، جرم کاوی، داده کاوی، هوش مصنوعی.

۱ مقدمه

سازمان‌های تروریستی از رسانه‌های اجتماعی برای گسترش تبلیغات و جذب اعضای جدید استفاده می‌کنند [۲]. در جنگ داعش بر علیه حاکمیت سوریه و عراق، رسانه‌های اجتماعی به ایجاد تحولات جدید کمک کردند. اتفاقاتی که از لیبی تا افغانستان و نیجریه تا بنگلادش را تحت تاثیر قرار داد [۳]. در شناسایی اهداف تروریستی با استفاده از داده‌کاوی، مرکزیت درجه و تعداد پیوندهای مستقیم متصل به هر گره اهمیت آن گره

را نمایان می‌کند و سایر اطلاعات مانند گره اصلی با رهبر قابل درک است [۴].

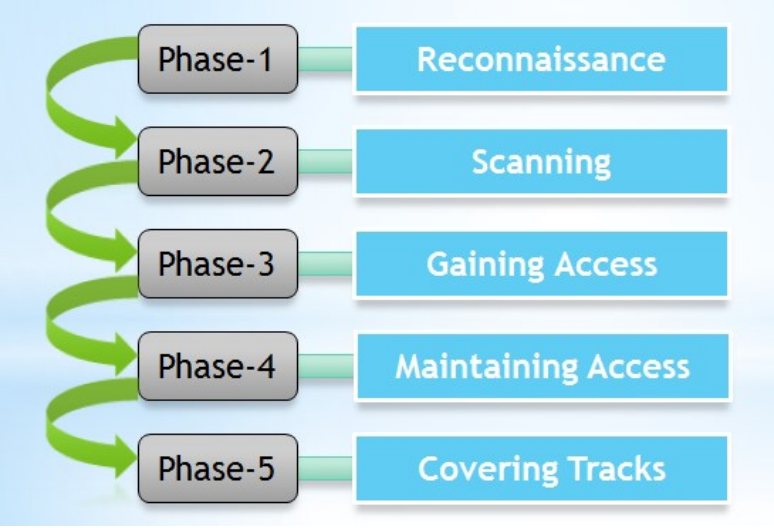
با افزایش شدید استفاده از شبکه‌های اجتماعی، بانک اطلاعاتی برخط در قالب نظرات، احساسات، عواطف و نیات تولید شد که نشان‌دهنده وابستگی‌ها و تمایل اعضا به یک نهاد، رویداد و سیاست است [۵]. شناسایی محتوای افراطی برای تجزیه و تحلیل احساسات کاربران نسبت به برخی از گروه‌های افراطی و جلوگیری از چنین اعمال غیرقانونی مرتبط و مهم است [۶].

تحلیل شبکه‌های اجتماعی Social networks analysis (SNA) می‌تواند به شناسایی رهبران یا افراد مهم تاثیرگذار در عملیات تروریستی کمک کند و باید به منظور ایجاد اختلال در فعالیت های سازمانی مورد هدف قرار گیرند [۱].

فرآیند استخراج OSINT در سه مرحله مشاهده می شود (الف) اکتساب داده، (ب) غنی‌سازی داده، و (ج) استنتاج دانش. در زمینه تروریسم، محققان کارهای قابل توجهی در انطباق با این سه مرحله انجام داده‌اند [۸].

OSINT یا اوسینت مخفف Open Source Intelligence به‌معنای جستجوی هوشمندانه در منابع اطلاعات آزاد است [۹].

OSINT به‌صورت آن‌لاین جهت شناسایی هدف توسط سازمان‌های جنایی، هکرها و آزمایش‌کنندگان نفوذ به‌طور بسیار گسترده مورد استفاده قرار می‌گیرد [۱۲] همان‌طور که در شکل ۱ آورده شده است، اولین مرحله اول نفوذ، شناسایی است.



شکل ۱: مراحل تست نفوذ

انواع ابزارهای هوش که می توان از آن برای جمع آوری اطلاعات منبع‌باز استفاده کرد.

- هوش منابع انسانی (HUMINT)

- هوش منابع تصویری (IMINT)
- هوش منابع جغرافیایی (GEOINT)
- هوش منابع سیگنالی (SIGINT)
- هوش رسانه‌های اجتماعی (SOCMINT)
- هوش منابع اقتصادی (FININT)
- هوش منابع باز (OSINT)

در سال ۲۰۱۲ برای اولین بار از عبارت SOCMINT یا هوش رسانه‌های اجتماعی استفاده شد؛ یعنی بررسی رسانه‌های اجتماعی برای به‌دست آوردن اطلاعات از منابع باز (OSINT) [۱۳]. از طرفی منابع اوسینت بدون نگرانی در رابطه با هر گونه مجوز حق انتشار، می‌توانند بین افراد مختلف به اشتراک گذاشته شوند، زیرا این اطلاعات قبلاً توسط صاحب اطلاعات، منتشر شده‌اند [۱۴]. برای به‌دست آوردن اطلاعات از رسانه‌های اجتماعی، از تکنیک‌های شرح داده شده زیر استفاده می شود [۱۵]:

۱. جستجوی مستقیم در رسانه‌های اجتماعی با موتور جستجوی داخلی و گزینه‌های جستجو پیشرفته.

۲. جستجوی ابزارهای خارجی که از طریق اتصال API به رسانه‌های اجتماعی به شما امکان دانلود می‌دهد.

۳. داده‌ها و ساختار آنها یا ابزارهایی که وظیفه آنهاست.

۴. ایجاد جستجوی پیشرفته در موتور جستجو گوگل با استفاده از عملگرهای پیشرفته و تکنیک‌های رشته بولی.

ابزارهای OSINT به‌سرعت در حال تکامل هستند [۱۶]، روش‌های رایج را می‌توان در چهار قالب اصلی دسته‌بندی کرد: روش‌های مبتنی بر متن، سیستم‌های اطلاعات جغرافیایی (GIS)، علوم شبکه و پزشکی قانونی بصری [۱۹].

روش مبتنی بر متن و Natural Language Processing: بررسی متن، از طریق موجودیت‌ها، کلمات کلیدی، روابط کلمه/ عبارت و نقش‌های معنایی/ نحوی. NLP روش‌های مبتنی بر متن معاصر مانند خلاصه‌سازی خودکار متن، تجزیه و تحلیل احساسات مبتنی بر ماشین، استخراج موضوع، پایه ابزارهای مدرن متن‌کاوی را تشکیل می‌دهد [۱۷].

پروفایل کاربر: شامل زبان استفاده شده و لحن کلمات، حساب‌های پیونده شده، دوستان مشترک با گره‌های تروریستی، رسانه‌ها و ویدئوهای بارگذاری شده، علاقه‌مندی‌ها، اخبار دنبال شده، هشتگ‌های استفاده شده، موقعیت‌های انتشار پست، متادیتا، استفاده از کلمات خاص ویژه گروه‌های تروریستی و ... [۱۷].

ابزارهای تسهیل کننده کسب و تجزیه و تحلیل اطلاعات در رسانه‌های اجتماعی: در زیر چند مورد منتخب از ابزارهایی برای تسهیل کسب اطلاعات از رسانه‌های اجتماعی را معرفی می‌کنیم. ابزارهایی که برای همه در دسترس هستند و استفاده از آنها آسان است و به‌راحتی در وب یافت می‌شود [۱۸].

روش‌های اوسینت: روش‌های داده‌کاوی و تجزیه و تحلیل داده‌های نوآورانه، روش جستجوی زبانی هوشمند، موتورهای جستجوی هوشمند، سیستم مرتب‌سازی موضوعی (مانند نظارت خودکار RSS)، نظارت بر سایت‌های جامعه (مانند ارزیابی فوری خطر فلش موب)، ارزیابی کد منبع وب‌سایت‌ها، نمایش محتوای پنهان، جستجوی دامنه، ابزار whois (بازیابی داده های مرتبط با مشترکین دامنه سایت)، نظارت بر مطبوعات و ...

حوزه‌های کلیدی اوسینت: اخبار اینترنتی، ادبیات خاکستری، شبکه‌های اجتماعی، رسانه‌های سنتی، مخازن باز داده‌ها، سوابق.

۲ مرور پیشینه

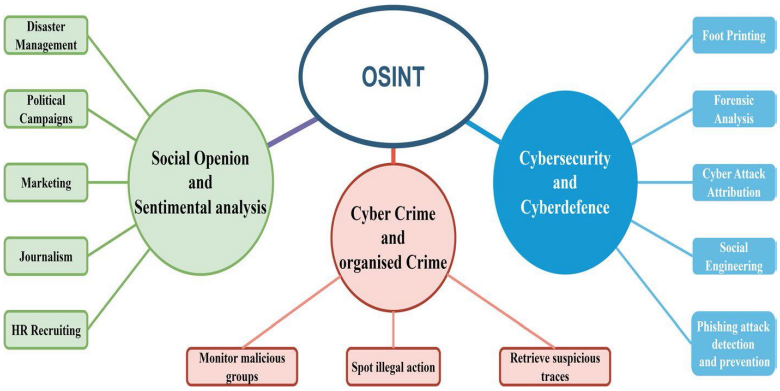
پزشکی قانونی دیجیتال و اطلاعات منبع‌باز دو نوع گسترده از تحقیقات جرایم سایبری هستند. قاچاق انسان، هرزه‌نگاری، پورنوگرافی کودکان، ترور، فروش مواد مخدر، فعالیت‌های تروریستی، بازارهای جرایم سایبری و مبادلات ارزهای دیجیتال از جمله هشت جنایت سایبری اصلی هستند که توسط Nazah و همکاران (۲۰۲۰) برجسته شده‌اند. آنها دریافتند که هیچ ابزار یا روش واحدی نمی‌تواند تمام شواهدی را که بازرسان نیاز دارند جمع‌آوری کند و به این دلیل از ترکیب‌های مختلف ابزارها و تکنیک‌ها برای انجام تحقیقات جرایم سایبری استفاده می‌کنند.

کوئیک و چو (۲۰۱۸) چارچوبی مبتنی بر OSINT پیشنهاد کردند که دقت دستگیری مجرم را افزایش می دهد و OSINT را در پزشکی قانونی دیجیتال برای بهبود تجزیه و تحلیل اطلاعات جنایی اعمال می‌کند.

توسط جونجینگ، یان، و جین چیانگ (۲۰۲۰) در راستای پزشکی قانونی شبکه اجتماعی، رابطه مبتنی بر داده‌های بزرگ با استفاده از ارتباط شبکه و فرآیند پزشکی قانونی تلفن‌های همراه را مطرح کردند.

در کار دیگری (Giudice, Paratore, Moltisanti, Battiato, 2017) بر روی پلت فرم Wechat به‌طور ویژه روش ارتباط شبکه‌های اجتماعی بر اساس مجموعه داده‌های نمونه را تجزیه و تحلیل می‌کند.

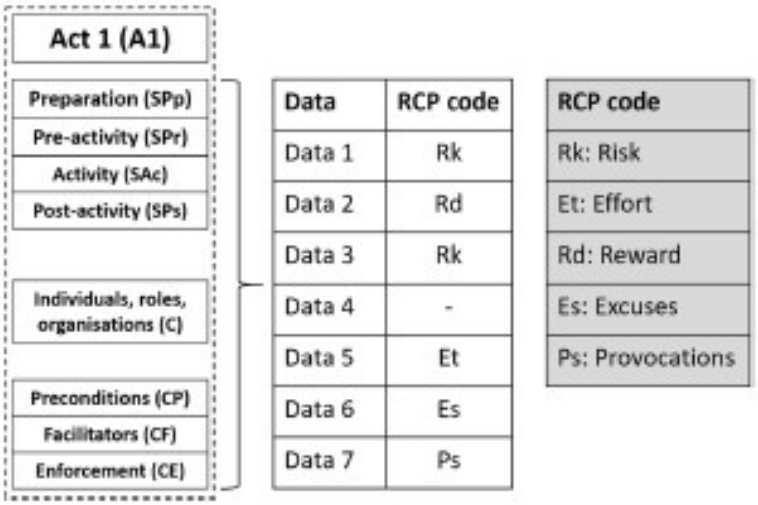
بر اساس مقاله (La Stampa, 2018)، هر فردی که در سایت‌های شبکه‌های اجتماعی حساب کاربری دارد، به‌طور متوسط هفت نوع اطلاعات از وی در آن سایت‌ها ثبت شده است (شکل ۲: نمایه اطلاعات و کاربردهای اوسینت).



شکل ۲: کاربردهای اوسینت

۱.۲ یک فرآیند روشمند ساختاریافته برای جمع‌آوری سناریوی جرائم سازمان‌یافته با استفاده از OSINT

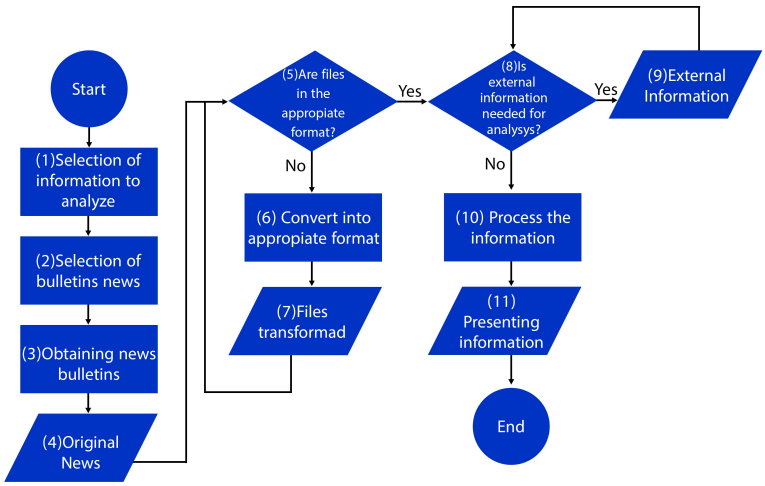
مقاله [۱۸] به‌دنبال اقدام‌شناسی مجرمان است. تحلیل‌گران منابع آشکار با کمک هوش مصنوعی اقدام به تولید فیلم‌نامه‌های جنایی کردند تا رویه وقوع جرم را بررسی و در مواردی منجر به تولید فیلم‌های جنایی با کیفیت و با موضوعات جدید و منحصر به فرد بشوند. این ایده به طور مؤثر باعث شده، اقدامات سازمان‌یافته جنایی پیش‌بینی شود. SCP شامل تعدادی تکنیک است که ارتکاب جرم را پر خطرتر، پاداش کمتر و تلاش را بیشتر می‌کند. تکنیک‌های SCP نیز می‌توانند کمک به حذف بهانه‌هایی که بر تصمیم‌گیری مجرم تأثیر می‌گذارند (مانند تنظیم قوانین واضح‌تر) و کاهش تحریکات به سمت مشارکت مجرمانه (مانند دلسرد کردن) را ایجاد کنند. در شکل ۳ پیش‌بینی نقش‌ها با استفاده از اوسینت رسم شده است.



شکل ۳: پیش‌بینی نقش‌ها با استفاده از اوسینت

۲.۲ تشخیص اخبار جعلی کرونا از طریق بررسی MedOSINT در بولتن‌های رسمی مراقبت‌های بهداشتی با توضیح CBR

بر مبنای الگوی مرجع [۸] گام دوم، روش‌های دسترسی به منابع اطلاعاتی سالم و قابل اعتماد بررسی شد. در بولتن‌های رسمی پزشکی حجم بسیار زیاد اطلاعات در مورد درمان‌های مختلف و درمان‌های خودساخته همراه با شایعات و اطلاعات نادرست منتشر می‌شود و باعث سردرگمی و بی‌اعتمادی مردم گردیده و سایت‌های خبری قانونی هم در دام پخش اطلاعات نادرست قرار می گیرند. MedOSINT با ارائه شیوه پیشنهادی کمک می‌کند مطمئن شوید آیا اخبار پزشکی مورد نظر، درست است یا غلط. با ادغام MedOSINT و سیستم استدلال مبتنی بر مورد ،(CBR) راهکارهای مورد اعتماد مهیا خواهد شد [۲۰]. در تصویر ۴ نمودار پیشنهادی MedOSINT آورده شده است. در این پژوهش ویژگی‌های تحلیل شده به دو دسته کلی تقسیم می‌شوند: ۱) منبع ۲) محتوا.



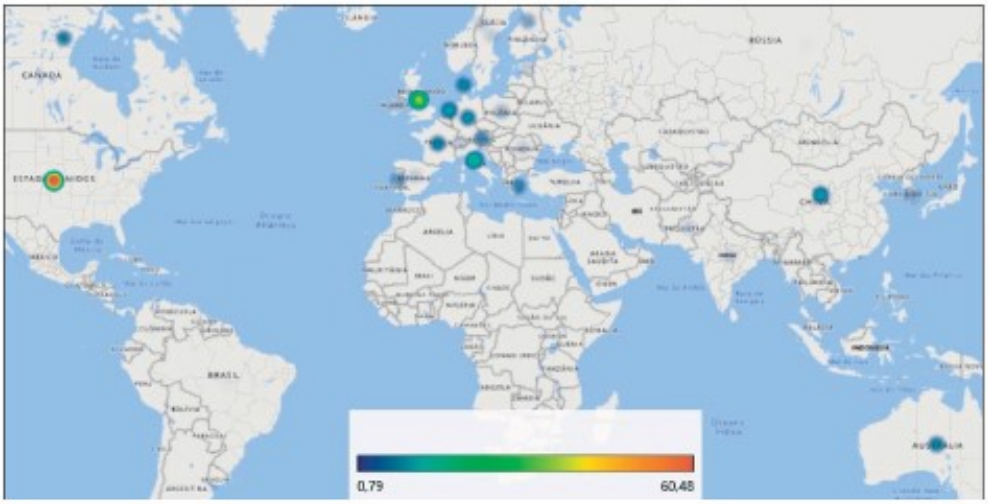
شکل ۴: نمودار جریان پیشنهادی MedOSINT

۳.۲ بررسی رسانه های اجتماعی مبتنی بر پیش‌بینی ناآرامی‌های مدنی

با در نظر گرفتن ناآرامی‌های اخیر ۲۰۲۳ که در ایران اتفاق افتاد بررسی ارتباط ناآرامی‌های مدنی و ارتباط با تروریست‌ها ضروری به‌نظر می‌رسد. در این کار، ابتدا پیش‌بینی ناآرامی مدنی مفهوم‌سازی شده و به‌نوبه خود، فناوری‌های پیش‌بینی ناآرامی‌های مدنی نیز به عنوان ابزار ارزیابی ریسک ارائه شده است که ناآرامی‌های آینده خطرناک را پیش بینی و قابل محاسبه می‌کند. در نهایت، روش‌های ارائه شده توسط محققان ارزیابی می‌شود [۲۱].

۴.۲ مروری بر ادبیات سیستماتیک برای بررسی کاربرد هوش منبع‌باز (OSINT) با هوش مصنوعی: تلفیق هوش منبع‌باز با هوش مصنوعی

در راستای انگیزه‌یابی تروریست در شبکه های اجتماعی با استفاده از اوسینت، با تجزیه و تحلیل نتایج، اطلاعات مرتبطی در مورد انتشاراتی که OSINT را با هوش مصنوعی یا سایر زمینه‌ها تلفیق می‌کنند، پیدا می‌کنیم [۲۲]. برای نمایش حوزه انتشارات OSINT از تجزیه و تحلیل اطلاعات به اشتراک گذاشته شده هوشمند در رسانه‌های اجتماعی برای تولید دانش جدید استفاده می‌شود. بنابراین، تنها در این ۴ سال، یعنی از ۲۰۱۶ تا ۲۰۱۹، انتشارات OSINT با هوش مصنوعی برای حوزه امنیت سایبری، بررسی و نقشه‌ای با بیشترین تمرکز برنامه‌ها در تصویر ۵ نشان داده شده است.



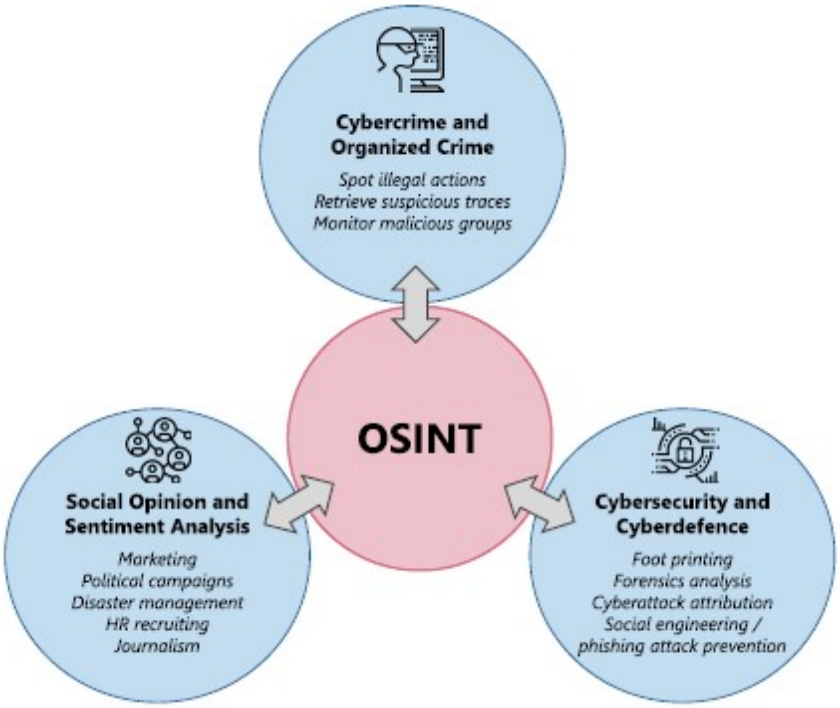
شکل ۵: کشورهای منتشر کننده بولتن‌های اوسینت

با تجزیه و تحلیل این نتایج، به این نتیجه رسیدیم که استفاده از یک مرور متون سیستماتیک می‌تواند کاربرد OSINT با هوش مصنوعی را نشان دهد.

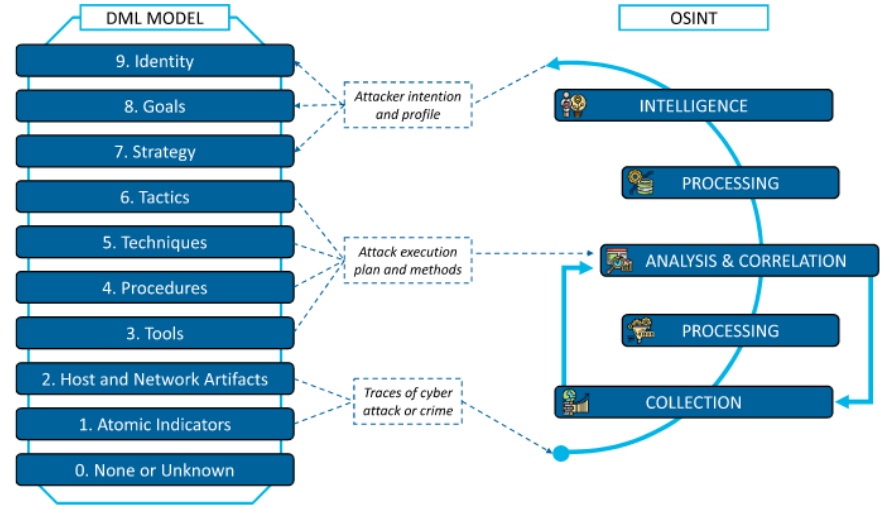
۵.۲ فرصت‌ها، چالش‌های منابع باز و روندهای آینده

در حقیقت اطلاعات منبع‌باز مانند معدن طلا هستند که در دسترس همه هست ولی فقط عده کمی قادر به استخراج آن هستند. در این مقاله سه مورد استفاده اصلی OSINT ذکر شده است. برای هر کاربر، در هر زمان و از هر نقطه از اینترنت، قابل دسترسی است. موارد استفاده اصلی اوسینت در تصویر ۶ آورده شده است.

در حالت ایده‌آل، OSINT در آینده باید بتواند اطلاعات خاصی را که در جستجوی کاربر بیشترین صحت و دقت را دارد برگرداند. چرخه و مدل جمع‌آوری و تحلیل داده‌ها پیشنهادی در تصویر شماره ۷ آورده شده است.



شکل ۶: موارد استفاده اصلی اوسینت



شکل ۷: مدل جمع‌آوری و تحلیل داده‌ها

۳ یافته‌ها

به همان اندازه که هوش منبع‌باز ارزشمند است، اضافه بار اطلاعات یک مشکل واقعی است. اکثر ابزارها و تکنیک‌های مورد استفاده برای انجام ابتکارات اطلاعاتی منبع‌باز برای کمک به متخصصان امنیتی تلاش‌های خود را بر روی حوزه‌های خاص مورد علاقه متمرکز می‌کنند.

مرجع [۱۹] (اسپنسر چنی و همکاران ۲۰۲۱) ایده‌ی اولیه بسیار عالی است و راهگشا در پیش‌بینی اقدامات تروریستی و لیکن حریم خصوصی مغفول مانده است و به‌نوعی ما از همه روش‌ها برای به‌دست آوردن اطلاعات استفاده می‌کنیم ولیکن در قواعد بین‌المللی قانون به ما اجازه دسترسی به اطلاعات خصوصی محرمانه در پرونده‌های قضائی را حتی به‌شرط انتشار توسط نفوذگران نمی‌دهد و برخی از صاحب‌نظران این موضوع را غیر اخلاقی و متضاد با روح اوسینت می‌دانند.

مرجع [۲۰] (سرجیو مائوریسیو و همکاران ۲۰۲۱) ایده پیشنهادی در راستای کشف اطلاعات منتشر شده غیر مستند در فضای مجازی است همان چیزی که در ادبیات ما به نوعی فیک‌نیوزها نام دارند. از جمله نگاه نویسنده به کار پیشنهادی نگاه عملیات روانی هر موضوع بوده و قصدش را کاهش بار روانی بر روی افکار مردم دانسته که در نوع خود کم نظیر است. نکته حائز اهمیت روش پیشنهادی این است که یک الگوریتم تحت نظارت CBR برای شناسایی اخبار مشابه تلفیق کرده است و باعث بالارفتن صحت دسته بندی شده است.

مرجع [۲۱] (گابریل گریل، دانشگاه میشیگان ۲۰۲۱) نویسنده با بهره‌گیری از روش‌های خزش در اطلاعات آشکار موجود، کاربرهای مختلف شبکه‌های اجتماعی را دسته‌بندی کرده و برای هر فرد یک الگوی سیاسی، اجتماعی، فرهنگی، اعتقادی و ... تهیه می‌کند که برای کارهای کارآگاهی بعدی از جمله جرم‌شناسی و پیش‌بینی مخالفت‌های مردم بسیار مؤثر است.

مرجع [۲۲] (ژائو رافائل گونسالوس اوانجلیستا و همکاران ۲۰۲۰) حاوی روش‌های مرسوم جمع‌آوری اطلاعات ازجمله هوش انسانی، هوش ماشین، هوش ارتباطی و هوش جمع‌آوری اطلاعات آشکار که در نهایت دانش ارتباطی انواع هوشمندی است.

مرجع [۲۳] (خاویر پاستور و همکاران ۲۰۲۰) علاوه بر کارهای قبلی، روش‌های جمع‌آوری اطلاعات در وب عمیق و وب تاریک را مورد بررسی قرار داده است. این مقاله با معرفی وب‌سایت‌های مرتبط با هر موضوع جمع‌آوری اطلاعات، اهمیت استفاده و درصد بهره‌وری هر روش را مشخص کرده است.

۴ نتیجه‌گیری

در کارهای پژوهشی بررسی شده به‌دلیل استفاده از دایرکتوری برخط ذخیره اطلاعات می‌توان یک آزمایشگاه جامع کارآگاهی در اینترنت راه‌اندازی کرد، به شکلی که با گسترش پرونده‌های کارآگاهی در وب هر روز به دایرکتوری تجمیعی اطلاعات برای پیش‌بینی‌های بعدی افزوده شود. علاوه بر داده‌های استخراج شده از اینترنت، باید به اهمیت اطلاعات دارک‌وب و دیپ‌وب توجه داشت.

با توجه به سرعت رشد اطلاعات و پیچیدگی تحلیل‌های اوسینت، در کارهای آینده بر روی جمع‌آوری

جدول ۱: مقایسه فنی بین روش‌های بررسی شده دسترسی به اطلاعات

مراجع بررسی شده	چالش‌ها	مزایا
[۸، ۹، ۱۷]	دسترسی به دیتاست برخط در دسترس آشنایی مجرمان سایبری به روش‌های دسترسی به داده‌های آشکار عدم ساختار واحد نمایه‌سازی اطلاعات	تولید سناریوهایی که تاکنون کمتر یا هرگز اتفاق نیافتاده و در آینده ممکن است با آن درگیر شویم دلایل ارتکاب به جرم قبل از وقوع افزایش هزینه اقدام مجرمانه
[۱۷، ۲۰]	هیجان باعث باورپذیری خبر جعلی می‌شود. ضعف سازوکار برچسب‌زنی به اخبار جعلی. تولید تنش‌های اجتماعی با پخش شایعه.	تحلیل اخبار با هوش مصنوعی. ایجاد بستر برخط و پرسرعت واکنش گسترش دسترسی به داده باز تولید ابزارهای صحت‌سنجی فردی تولید اخبار امن توسط هوش مصنوعی سازوکار برچسب‌زنی خبر
[۱۸، ۲۲]	دسترسی به اخبار محلی در حوادث ضعف NLP در زبان‌های بومی ضعف اطلاعاتی در دسترسی به منابع باز	گسترش روش‌های ثبت وقایع تولید مجلات هوشمند تحلیل وقایع تولید ابزار پرقدرت کشف ناهنجاری توسط منابع باز و هوش مصنوعی

اطلاعات با استفاده از کامپیوترهای کوانتومی متمرکز خواهیم شد.

مراجع

[۱] نهادا. حسن، رامی حجازی (۱۴۰۰). جمع‌آوری اطلاعات منبع‌باز: ابزار و روش‌های جمع‌آوری اطلاعات منابع آزاد از اینترنت، مترجم مهدی کوره‌پز، نشر شاملو.

[2] Mishra, Ranjit (2033). “Terror Attack Prediction Based on Time Series”. Journal of Defense Studies, 17(1).

[3] Berger J.M., Jonathon Morgan (2015). “Defining and Describing the Population of ISIS Supporters on Twitter”. The Brookings Institution.

[4] Koerner, Brendan I. (2017). “Why ISIS is Winning the Social Media War”. Wired (1 May 2017), available at https://www.wired.com/2016/03/isis-winningsocial-media-war-heres-beat.

[5] Hao F., Park D.S., Pei Z. (2018). “When social computing meets soft opportunities and insights”. Human-centric Comput Inform Sci, 8(8):1–18.

[6] Azizan, S. A., Aziz, I. A. (2017). “Terrorism detection based on sentiment analysis using machine learning”. Journal of Engineering and Applied Sciences, 12(3), 691-698.

[7] Dhillon, H. (2021). Building effective network security frameworks using deep transfer learning techniques (Doctoral dissertation, The University of Western Ontario (Canada)).

[8] Chaudhary, M., Bansal, D. (2022). "Open source intelligence extraction for terrorism-related information: A review". Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 12(5), e1473.

[9] Kumari, S., Yadav, R. J., Namasudra, S., Hsu, C. H. (2021). "Intelligent deception techniques against adversarial attack on the industrial system". International Journal of Intelligent Systems, 36(5), 2412-2437.

[10] Singer, G., Golan, M. (2019). "Identification of subgroups of terror attacks with shared characteristics for the purpose of preventing mass-casualty attacks: A data-mining approach". Crime Science, 8(1), 14.

[11] Rehman, A. U., Jiang, A., Rehman, A., Paul, A., Din, S., Sadiq, M. T. (2020). "Identification and role of opinion leaders in information diffusion for online discussion network". Journal of Ambient Intelligence and Humanized Computing, 1-13.

[12] Yadav, A., Kumar, A., Singh, V. (2023). "Open-source intelligence: a comprehensive review of the current state, applications and future perspectives in cyber security". Artificial Intelligence Review, 56(11), 12407-12438.

[13] Omand, D. (2017). "Social media intelligence (SOCMINT)". The Palgrave handbook of security, risk and intelligence, 355-371.

[14] Kuehn, P., Bäumler, J., Kaufhold, M. A., Wendelborn, M., Reuter, C. (2022). "The Notion of Relevance in Cybersecurity: A Categorization of Security Tools and Deduction of Relevance Notions".

[15] Thapa, B. (2022). "Applying socmint to extract cyber threat intelligence from the Russia-Ukraine conflict". IADIS International Journal on WWW/Internet, 20(2).

[16] Nastasi, C., Battiato, S. (2021). "Defamation 2.0: New Threats in Digital Media Era-An Overview on Forensics Approaches in the Social Network Ecosystem". IMPROVE, 121-127.

[17] Böhm, I., Lolagar, S. (2021). "Open source intelligence: Introduction, legal, and ethical considerations". International Cybersecurity Law Review, 2(2), 317-337.

[18] Camacho, D., Panizo-LLedot, A., Bello-Orgaz, G., Gonzalez-Pardo, A., Cambria, E. (2020). "The four dimensions of social network analysis: An overview of research methods, applications, and software tools". Information Fusion, 63, 88-120.

[19] Chainey, S. P., Alonso Berbotto, A. (2022). "A structured methodical process for populating a crime script of organized crime activity using OSINT". Trends in Organized Crime, 25(3), 272-300.

[20] Monterrubio, S. M. M., Noain-Sánchez, A., Pérez, E. V., Crespo, R. G. (2021). "Coronavirus fake news detection via MedOSINT check in health care official bulletins with CBR explanation: The way to find the real information source through OSINT, the verifier tool for official journals". Information Sciences, 574, 210-237.

[21] Grill, G. (2021). “Future protest made risky: Examining social media based civil unrest prediction research and products”. Computer Supported Cooperative Work (CSCW), 30(5), 811-839.

[22] Evangelista, J. R. G., Sassi, R. J., Romero, M., Napolitano, D. (2021). “Systematic literature review to investigate the application of open source intelligence (osint) with artificial intelligence”. Journal of Applied Security Research, 16(3), 345-369.

[23] Pastor-Galindo, J., Nespoli, P., Mármol, F. G., Pérez, G. M. (2020). “The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends”. IEEE Access, 8, 10282-10304.

تأثیر حکمرانی داده بر کارآمدی هزینه‌کرد بودجه در پروژه‌ها

علیرضا فخررحیمی[۱]، فربود تیموری[۲]

[۱]دانشجوی دکتری، گروه علمی مدیریت فضای سایبر، دانشگاه عالی دفاع ملی، تهران؛ امور نظام فنی، اجرایی مشاورین و پیمانکاران، معاونت فنی و زیربنایی، سازمان برنامه و بودجه کشور، تهران
alirfrahimi@iran.ir
[۲]دانشجوی دکتری، گروه علمی مدیریت فضای سایبر، دانشگاه عالی دفاع ملی، تهران
fa.teimouri01@sndu.ac.ir

چکیده

هدف این مقاله بررسی تأثیر حکمرانی داده بر کارآمدی هزینه‌کرد بودجه در پروژه‌های ایران است. حکمرانی داده به‌عنوان یک ابزار مدیریتی، توانایی تجزیه و تحلیل داده‌های پروژه را فراهم می‌آورد و از طریق بهبود برنامه‌ریزی و کنترل هزینه‌ها، به بهبود عملکرد پروژه‌ها و افزایش کارآمدی کمک می‌کند. بررسی نتایج این مقاله نشان می‌دهد که حکمرانی داده، ابزاری قدرتمند برای بهبود کارآمدی هزینه‌کرد بودجه در پروژه‌های عمرانی و غیرعمرانی است و می‌تواند به کشورها در ارتقاء زیرساخت‌ها و توسعه‌بخشی کمک کند.بدیهی است شرایط تحریم، تکانه‌های اقتصادی و سایر فشارهای بین‌المللی از یک سو، الزام به طی نمودن مسیر توسعه کشور و سعی در تداوم شتاب توسعه در ایران، لزوم استفاده از حکمرانی داده را بیش از بیش مهم می‌نماید. بدیهی است استفاده از حکمرانی داده پیش از هر چیز نیاز به برخی الزامات و معیارها دارد که در این مقاله به اختصار مورد بررسی قرار گرفته‌اند.

کلمات کلیدی: حکمرانی داده، هزینه، بودجه، پروژه‌های عمرانی، هزینه کرد، پایش.

۱ مقدمه

پایش بودجه هزینه شده در پروژه‌های کشور اهمیت زیادی دارد چراکه با پایش بودجه، می‌توان بهترین نحوه مدیریت و کنترل هزینه‌های پروژه را تعیین کرد و از افزایش ناگهانی هزینه‌ها جلوگیری کرد. همچنین برنامه‌ها و زمان‌بندی‌های اجرایی بهبود یابند و به‌موقعیت تغییرات پاسخ داده شود. با پایش مداوم بودجه، می‌توان پیشرفت فیزیکی و مالی پروژه را ارزیابی نموده و با دقت نسبی آنها را مقایسه کرد و نیز به استفاده بهینه از منابع کشور کمک نمود، هر چه پایش بودجه های هزینه شده در پروژه ها دقیق تر باشد، شفافیت بیشتری را به دنبال خواهد داشت و منجر به افزایش اعتماد عمومی خواهد شد؛ انجام تخلفات مالی کاهش یافته و در صورت وقوع، کشف آنها سریع تر و راحت تر خواهد بود. با پیاده شدن حکمرانی داده در این حوزه ، عملکرد مدیران بهتر و سریع تر رصد خواهد شد و کیفیت عملکرد آن ها در موقیت های مختلف قابل سنجش است.

۲ کاربرد حکمرانی داده بر پایش پروژه‌ها

حکمرانی داده (Data Governance) به پایش پروژه‌های دولتی در ایران کمک زیادی می‌کند و نقش مهمی در بهبود عملکرد این پروژه‌ها ایفا می‌کند. در ادامه، به توضیح چگونگی کمک حکمرانی داده به پایش پروژه‌های دولتی می‌پردازیم:

۱. جمع‌آوری داده‌ها و اطلاعات: حکمرانی داده با تعیین استانداردها و فرآیندهای مناسب، به جمع‌آوری داده‌ها و اطلاعات مرتبط با پروژه‌های دولتی کمک می‌کند. این اطلاعات شامل جزئیات مالی، فنی، زمان‌بندی و عملکرد پروژه‌ها است.

۲. استفاده از تحلیل داده‌ها: حکمرانی داده مجموعه‌های داده‌ها را تجزیه و تحلیل می‌کند و از ابزارهای تحلیلی پیشرفته برای استخراج اطلاعات ارزشمند و شاخص‌های عملکرد پروژه‌ها استفاده می‌کند.

۳. کاهش خطاها و ریسک‌ها: حکمرانی داده با تحلیل دقیق داده‌ها، امکان شناسایی خطاها و ریسک‌های مختلف در طول اجرای پروژه‌ها را فراهم می‌آورد و باعث کاهش آن‌ها می‌شود.

۴. بهبود تصمیم‌گیری: با داشتن اطلاعات دقیق و به‌روز، حکمرانی داده کمک می‌کند تا تصمیم‌گیری‌های بهتر و مستندتر در مورد اجرای پروژه‌ها صورت گیرد.

۵. افزایش شفافیت و حساب‌پذیری: حکمرانی داده با ایجاد شفافیت در جمع‌آوری و استفاده از داده‌ها، به افزایش حساب‌پذیری و اعتماد عمومی به پروژه‌های دولتی کمک می‌کند.

۶. بهبود پایش و نظارت: حکمرانی داده با ارتقاء نظارت و پایش مداوم بر پروژه‌ها، به تشخیص زودهنگام مشکلات و تغییرات غیرمنتظره کمک می‌کند و از اجرای موفق‌تر پروژه‌ها اطمینان حاصل می‌کند.

۷. بهینه‌سازی منابع: با تحلیل داده‌ها و اطلاعات موجود، حکمرانی داده امکان بهینه‌سازی استفاده از منابع مالی و انسانی در پروژه‌ها را فراهم می‌کند [۱].

۱.۲ گستره ایده‌آل کاربرد حکمرانی داده

گستره ایده‌آل کاربرد حکمرانی داده در نظارت بر پروژه‌های دولتی ایران بر اساس این مشخصه ها است. ایده آل بودن حکمرانی داده به در اختیار داشتن داده ها و اطلاعات کافی مرتبط با پروژه‌های دولتی و جمع‌آوری و مدیریت داده ها مرتبط می‌شود. این داده‌ها شامل اطلاعات مالی، فنی، زمان‌بندی و عملکرد پروژه‌ها می‌شوند.در ایده آل بودن حکمرانی داده ایده آل، از تکنولوژی‌های پیشرفته مانند ابراطلاعاتی، هوش مصنوعی و تحلیل داده‌های بزرگ برای تحلیل و بهره‌برداری از داده‌ها و اطلاعات پروژه‌ها استفاده می‌شود تا اطلاعات مرتبط با پروژه‌های دولتی را شفاف تر کرده و دسترسی آسان و عمومی به اطلاعات را فراهم کند. این امر باعث افزایش اعتماد عمومی و نظارت مؤثرتر می‌شود. حکمرانی داده ایده‌آل به کمک تحلیل دقیق

داده‌ها، امکان پیش‌بینی و تحلیل ریسک‌ها و مشکلات پروژه‌ها را فراهم می‌کند تا از قبل اقدامات مناسبی برای کاهش آنها صورت بگیرد [۱، ۲].

حکمرانی داده ایده‌آل با استفاده از داده‌ها و اطلاعات موجود، مدیریت بهتر منابع مالی و انسانی در پروژه‌ها را تسهیل می‌کند و باعث اجرای کارآمدتر پروژه‌ها می‌شود، پایش و نظارت مداوم بر پروژه‌ها با استفاده از اطلاعات به‌روز و دقیق امکان‌پذیر می‌شود و مشکلات ، زودهنگام شناسایی و اصلاح می‌شوند..حکمرانی داده ایده‌آل به مدیران و نظارت‌کنندگان امکان می‌دهد تصمیم‌گیری‌های بهتر و مستندتر در مورد اجرای پروژه‌ها صورت دهند تا ضمن بهبود نتایج،کیفیت و کارایی اجرای پروژه‌ها به‌طور کلی بهبود یابد و پروژه‌ها به شکل مؤثرتری اجرا شود.

۲.۲ ویژگی‌های مدل حکمرانی پایشگر

برای پایش پروژه‌های دولتی در ایران، مدل حکمرانی داده‌ای مناسب باید دارای ویژگی‌های زیر باشد:

۱. مدل مبتنی بر استانداردها: مدل حکمرانی داده باید بر مبنای استانداردها و قوانین مرتبط با حکمرانی داده تعریف شده باشد. این استانداردها می‌توانند به اطمینان از کیفیت داده‌ها، امنیت، شفافیت و دسترسی به اطلاعات کمک کنند.

۲. مدل مرکزی و هماهنگ: در پروژه‌های دولتی که ممکن است به تعداد زیادی از بخش‌ها و سازمان‌ها امکانات را در اختیار دهند، مدل حکمرانی داده باید به‌طور مرکزی تعریف و هماهنگ شود تا بهترین نتیجه‌گیری از داده‌ها و اطلاعات به‌دست آید.

۳. مدل تعاملی با کاربران: موفقیت یک مدل حکمرانی داده نیازمند تعامل مستمر با کاربران نهایی است. باید با نظرات و نیازهای کاربران هماهنگ شده و تغییرات و بهبودها را براساس بازخورد آنها اعمال کرد.

۴. مدل منعطف و تطابق‌پذیر: محیط پروژه‌های دولتی پویا است و ممکن است نیازها و شرایط تغییر کنند. مدل حکمرانی داده باید منعطفیت داشته باشد و قابلیت تطابق با تغییرات را داشته باشد.

۵. مدل باز و شفاف: مدل حکمرانی داده باید اطلاعات و داده‌ها را به‌طور باز و شفاف در اختیار کاربران قرار دهد. این امر باعث افزایش شفافیت و اعتماد عمومی به نظارت بر پروژه‌های دولتی می‌شود.

۶. مدل امن: امنیت اطلاعات بسیار مهم است، بخصوص در پروژه‌های دولتی. مدل حکمرانی داده باید برنامه‌ها و فرآیندهای مناسب را برای حفظ امنیت اطلاعات اعمال کند.

۷. مدل مبتنی بر تحلیل داده‌ها: مدل حکمرانی داده باید از تحلیل داده‌ها و بهره‌گیری از ابزارهای تحلیلی مناسب برای استخراج اطلاعات مفید از داده‌ها استفاده کند.

در نهایت، مدل حکمرانی داده‌ای برای پایش پروژه‌های دولتی در ایران باید با توجه به نیازها و شرایط خاص این پروژه‌ها طراحی شود تا بهترین نتیجه‌گیری از اطلاعات و داده‌ها به‌دست آید و نظارت موثرتری بر روی اجرای این پروژه‌ها صورت گیرد.

۳ مروری بر اقدامات پیشین

سابقه مقالات فارسی در خصوص تاثیر حکمرانی داده و دولت، به بررسی ارتباط این دو عامل و نقش حکمرانی داده در بهبود عملکرد دولت‌ها می‌پردازند. این مقالات به مطالعه اثربخشی کاربرد حکمرانی داده در سازمان‌دهی و مدیریت دولتی، بهینه‌سازی خدمات عمومی، افزایش شفافیت و حساب‌پذیری، کاهش ریسک‌ها و بهبود کیفیت خدمات ارائه‌شده توسط دولت می‌پردازند. تاکید این مقالات بر اهمیت حکمرانی داده در بهبود فرایندها و تصمیم‌گیری‌های دولتی به‌منظور خدمت بهتر به جامعه است. هیچ کدام از مقالات پیشین مستقیما به بررسی تاثیر حکمرانی داده بر پایش پروژه های دولتی نپرداخته‌اند [۳].

۴ حکمرانی داده و پروژه‌های دولتی

حکمرانی داده با پایش موفق پروژه‌های عمرانی به افزایش رضایتمندی عمومی و صرفه‌جویی مالی کمک زیادی می‌کند. این امر به دلیل افزایش شفافیت و بهره‌وری در اجرای پروژه‌ها، کاهش خطاها و بهبود تصمیم‌گیری‌ها در زیر آمده است:

۱.۴ افزایش شفافیت

حکمرانی داده با ایجاد فرآیندهای شفاف در جمع‌آوری و انتقال اطلاعات پروژه‌های عمرانی، اعتماد عمومی را به دولت و پروژه‌های آن افزایش می‌دهد. مردم اطلاعات دقیق‌تری از وضعیت پروژه‌ها خواهند داشت که باعث ارتقاء رضایتمندی و اعتماد به عملکرد دولت می‌شود.

۲.۴ کاهش خطاها و بهبود تصمیم‌گیری‌ها

حکمرانی داده با تحلیل داده‌های پروژه‌های عمرانی، مشکلات زودهنگام شناسایی می‌شوند و اقدامات مناسب برای پیشگیری و رفع آن‌ها انجام می‌شود. این امر منجر به بهبود تصمیم‌گیری‌ها و اجرای بهتر پروژه‌ها می‌شود که علاوه بر کاهش خطاها، باعث صرفه‌جویی مالی و منابع عمومی می‌گردد.

۳.۴ بهره‌وری بیشتر

حکمرانی داده با استفاده از اطلاعات دقیق و به‌روز، بهره‌وری منابع را بهبود می‌بخشد. با شناخت دقیق‌تر از عملکرد پروژه‌ها، امکان بهبود عملکرد و کارآمدی آن‌ها وجود دارد که نتیجه‌ای از ترکیب مدیریت موثر و تصمیم‌گیری‌های منطقی است. این امر به صورت مستقیم باعث صرفه‌جویی مالی و بهینه‌سازی استفاده از منابع می‌شود.

۵ الزامات و پیش‌نیازهای اجرا

اجرای حکمرانی داده در پروژه‌های دولتی کشورها نیاز به مجموعه‌ای از الزامات و پیش‌نیازها دارد تا به نحو مؤثر و کارآمد عمل کند.چنانچه حکمرانی داده به صورت موثر اجرا نگردد، مشکلاتی از قبیل کاهش دقت و اعتماد به داده ها، تصمیم گیری های نادرست، مسائل امنیت داده و ... رخ خواهند داد، از این رو درک الزامات و پیش نیازهای اجرا با هدف اماده سازی شرایط اجرای صحیح بسیار مهم و ضروری است.

۱.۵ پیش‌نیازها

اجرای حکمرانی داده به برخی پیش‌نیازها نیاز دارد که به‌صورت خلاصه عبارتند از :

۱. تعیین هدف و استراتژی: ابتدا باید هدف و استراتژی مشخصی برای اجرای حکمرانی داده در پروژه‌های دولتی تعیین شود. این هدف باید با اهداف کلان دولت و پروژه‌ها هم‌راستا باشد و مرتبط با ارتقاء کیفیت و کارآمدی پروژه‌ها باشد.

۲. منابع انسانی و مالی: برای اجرای حکمرانی داده نیاز به منابع انسانی با تخصص‌های مرتبط با تحلیل داده‌ها و استفاده از ابزارهای تحلیلی داریم. همچنین، برای ساختاردهی و مدیریت حکمرانی داده نیاز به منابع مالی و انفورماتیکی مناسب است.

۳. شناخت سیستم‌ها و بسترهای فناوری اطلاعات: برای اجرای حکمرانی داده، باید سیستم‌های موجود و بسترهای فناوری اطلاعات در پروژه‌های دولتی به‌درستی شناخته شوند و اطلاعات موجود در این سیستم‌ها باید قابل دسترسی و به‌روزرسانی باشند.

۴. توافق‌نامه‌ها و قوانین: برای اجرای حکمرانی داده، توافق‌نامه‌ها و قوانین مرتبط با حفظ امنیت و حریم خصوصی داده‌ها باید رعایت شوند. اطمینان از حمایت قانونی و انضباطی برای حفظ حقوق و حریم خصوصی مردم بسیار اهمیت دارد.

۵. شفافیت و اعتماد: اطمینان از شفافیت در اجرای حکمرانی داده، افزایش اعتماد عمومی به پروژه‌های دولتی را به همراه دارد. باید اطلاعات به‌روز و دقیق از پروژه‌ها در اختیار مردم قرار گیرد تا اعتماد به عملکرد دولت تقویت شود.

۶. زیرساخت‌های فنی و فیزیکی: برای اجرای حکمرانی داده، لازم است زیرساخت‌های فنی و فیزیکی مرتبط با شبکه‌ها، سرورها، نرم‌افزارها و امنیت فیزیکی مناسب فراهم شود تا اطلاعات به صورت امن و سریع منتقل و پردازش شوند.

به طور کلی اجرای حکمرانی داده در پروژه‌های دولتی نیاز به یک نگاه جامع و هماهنگ به تمامی عوامل مذکور دارد تا نتیجه‌گیری مؤثر و کارآمدی را به همراه داشته باشد. این عوامل باعث ارتقاء کیفیت اجرای پروژه‌ها، کاهش خطاها و افزایش بهره‌وری و صرفه‌جویی مالی می‌گردند.

۲.۵ معیارها

با بررسی نمونه قراردادهای همسان، شرایط عمومی پیمان های مختلف که در امور نظام فنی و اجرایی مشاورین و پیمانکاران سازمان برنامه و بودجه منتظر شده است، معیارهای پیشرفت، توقف، هزینه کرد بهینه و حساسیت پروژه جزو مهم ترین معیارهای عملیاتی پروژه ها و طبعتا از اجزای مهم در حکمرانی داده برای پایش پروژه‌ها است. این معیارها به‌صورت زیر می‌توانند تعریف و توضیح داده شوند:

۱. معیارهای پیشرفت: این معیارها مربوط به اندازه‌گیری پیشرفت فیزیکی پروژه‌ها هستند و شامل مواردی نظیر میزان پیشرفت انجام کارها، تعداد واحدهای انجام شده، میزان مطابقت با زمان‌بندی پروژه و دیگر شاخص‌های مرتبط دیگر است.

۲. معیارهای توقف: این معیارها مرتبط با شناسایی و ارزیابی علل و عواملی هستند که می‌توانند به توقف یا تأخیر در اجرای پروژه منجر شوند. این معیارها به‌صورت مشخص بررسی می‌شوند تا اقدامات مناسب برای پیشگیری از توقف‌های احتمالی انجام شود.

۳. معیارهای هزینه کرد بهینه: این معیارها مربوط به کنترل و بهینه‌سازی هزینه‌ها در اجرای پروژه‌ها هستند. با استفاده از حکمرانی داده، هزینه‌های مختلف پروژه‌ها مورد بررسی قرار می‌گیرند و اقداماتی برای کاهش هزینه‌ها و بهینه‌سازی مدیریت مالی انجام می‌شود.

۴. معیارهای حساسیت پروژه: این معیارها مرتبط با شناسایی نقاط ضعف و مستعد اختلال در اجرای پروژه هستند. با استفاده از حکمرانی داده، عوامل حساسیت پروژه شناسایی و ارزیابی می‌شوند و اقداماتی برای کاهش اثرات احتمالی آنها انجام می‌شود.

به طور خلاصه، معیارهای پیشرفت، توقف، هزینه کرد بهینه و حساسیت پروژه از جمله معیارهای مهم در حکمرانی داده برای پایش پروژه‌ها هستند. این معیارها به‌صورت دقیق و کارآمد اندازه‌گیری و ارزیابی می‌شوند تا بهبود عملکرد پروژه‌ها و کارآمدی آنها فراهم شود و امکان انجام اقدامات مناسب برای بهبود کیفیت پروژه‌ها و کاهش خطرات احتمالی فراهم گردد [۴].

۶ موانع و موفقیت‌های پیش رو

۱.۶ موانع پیش روی پیاده‌سازی عملی حکمرانی داده در نظارت بر پروژه‌ها

موانع پیش روی پیاده‌سازی عملی حکمرانی داده در نظارت بر پروژه‌های دولتی ایران عبارتند از:

۱. فرهنگ سنتی: اجرای حکمرانی داده به‌طور کامل نیاز به تغییر فرهنگ سنتی دارد. برخی دستگاه‌های دولتی هنوز به مدیریت سنتی عادت دارند و اجرای حکمرانی داده نیازمند توجیه و آموزش مداوم مدیران و کارکنان است.

۲. نقص زیرساخت‌ها: برای اجرای حکمرانی داده، نیازمند زیرساخت‌های مدرن فناوری اطلاعات و ارتباطات هستیم. در برخی موارد، زیرساخت‌های کافی و قدرتمند برای جمع‌آوری و پردازش داده‌ها وجود ندارد [۱].

۲.۶ موفقیت‌های پیش روی پیاده‌سازی عملی حکمرانی داده در پایش پروژه‌ها

در مقابل، موفقیت‌های پیش روی پیاده‌سازی عملی حکمرانی داده در نظارت بر پروژه‌های دولتی ایران شامل موارد زیر می‌شود:

۱. بهبود شفافیت: حکمرانی داده می‌تواند شفافیت در فرآیندهای نظارتی را افزایش دهد و اطلاعات دقیقی از وضعیت پروژه‌ها را در اختیار مدیران و عموم قرار دهد.

۲. افزایش کارآمدی: با بهره‌گیری از تحلیل داده‌ها و اطلاعات کمکی، می‌توان به بهبود کارآمدی پروژه‌ها و کاهش هدررفت منابع دست یافت.

۳. تصمیم‌گیری بهتر: حکمرانی داده به مدیران امکان می‌دهد تصمیم‌گیری‌های بهتری بر اساس اطلاعات دقیق و مستند انجام دهند و احتمال تصمیم‌گیری‌های نادرست کاهش می‌یابد.

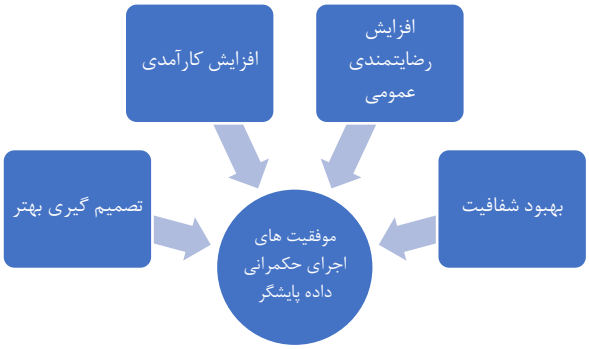
۴. افزایش رضایتمندی عمومی: افزایش شفافیت و بهبود کارآمدی پروژه‌ها می‌تواند منجر به افزایش رضایتمندی عمومی از عملکرد دولت در اجرای پروژه‌ها شود.

۷ نتیجه‌گیری

حکمرانی داده یک ابزار قدرتمند است که به افزایش کارآمدی و کیفیت پروژه‌های دولتی کمک می‌کند. با استفاده از حکمرانی داده، می‌توان داده‌ها و اطلاعات مرتبط با پروژه‌ها را بهبود داده و از آنها برای پایش و ارزیابی عملکرد پروژه‌ها استفاده کرد. این اقدامات می‌توانند به بهبود فرآیندهای تصمیم‌گیری و اجرای پروژه‌ها، کاهش هزینه‌ها، افزایش شفافیت و اعتماد عمومی و در نهایت افزایش رضایتمندی عمومی از عملکرد دولت در پروژه‌های عمرانی منجر شوند.

با این حال، اجرای حکمرانی داده نیازمند تغییرات زیادی است، از جمله تغییر فرهنگ سنتی در دستگاه‌های اجرایی دولتی، سرمایه‌گذاری در زیرساخت‌های فناوری اطلاعات و ارتباطات، ایجاد آگاهی کافی در کارکنان و مدیران از اهمیت و روش‌های حکمرانی داده و ایجاد شفافیت در فرآیندها و اطلاعات مرتبط با پروژه‌ها. همچنین، تأمین امنیت داده‌ها و حریم خصوصی نیز از جمله چالش‌های اجرای حکمرانی داده است که باید به‌طور جدی مدنظر قرار گیرد.

با کارآمدی و موفقیت در اجرای حکمرانی داده، دستگاه‌های دولتی قادر خواهند بود بهبود کیفیت خدمات عمومی و کارآمدی پروژه‌های عمرانی را تجربه کنند که نتیجه‌گیری مثبتی برای جامعه و اقتصاد کشور خواهد داشت.



شکل ۱: موفقیت‌های اجرای حکمرانی داده پایشگر

مراجع

[۱] صحرایی، فرامرز (۱۴۰۲). تحلیلی بر سند جامع دولت الکترونیک جمهوری اسلامی ایران از منظر شاخص‌های دولت دیجیتالی و حکمرانی داده.

[۲] مرادی مقدم، حسین (۱۴۰۱). حکمرانی داده و نقش آن در توسعه برنامه‌ریزی شهری،چهارمین همایش ملی مدیریت دانش و کسب‌وکارهای الکترونیکی با رویکرد اقتصاد.

[۳] ایزدخواستی، حجت (۱۳۹۵). تحلیل تاثیر فساد و کیفیت حکمرانی بر عملکرد نظام مالیاتی: رویکرد داده‌های تابلویی.

[۴] بنائی، سیدمجتبی و صابری، محسن (۱۳۹۶). دریاچه داده، بستری ضروری برای حکمرانی داده در سازمان‌ها، پنجمین همایش مدیران فناوری اطلاعات، تهران.

[5] www.tec.mporg.ir

بررسی قانون‌گذاری هوش مصنوعی در جهان و ایران با تکیه بر مدل چندذی‌نفعی جهانی

علیرضا فخررحیمی[۱]، فربود تیموری[۲]

[۱] دانشجوی دکتری، گروه علمی مدیریت فضای سایبر، دانشگاه عالی دفاع ملی، تهران؛ امور نظام فنی، اجرایی مشاورین و پیمانکاران، معاونت فنی و زیربنایی ، سازمان برنامه و بودجه کشور، تهران
alirfrahimi@iran.ir

[۲] دانشجوی دکتری، گروه علمی مدیریت فضای سایبر، دانشگاه عالی دفاع ملی، تهران
fa.teimouri01@sndu.ac.ir

چکیده

قانون‌گذاری هوش مصنوعی در کشور جمهوری اسلامی ایران ضروری است تا بهره‌برداری امن و اخلاقی از این فناوری را تضمین کند. هوش مصنوعی، با آثاری نظیر تأثیر بر اشتغال، اقتصاد، و امنیت مخاطبین اجتماعی، نیازمند استانداردها و مقرراتی است که مانع مشکلات احتمالی ناشی از استفاده ناصواب از آن شود. قوانین باید حریم خصوصی شهروندان، انسان‌مندی هوش مصنوعی و پیشگیری از تبعیض‌های اجتماعی را در بر داشته باشند. با توجه به اهمیت آموزش، تحقیقات و ایجاد همکاری‌های بین‌المللی، کشور باید برنامه‌ریزی و ارتقاء نیروهای متخصص در این حوزه را به‌عنوان اولویت مدنظر قرار دهد. توسعه فناوری هوش مصنوعی می‌تواند در مواجهه با چالش‌های جامعه مؤثر باشد، اما نیازمند قوانین محافظتی و همکاری بین‌المللی است. فقدان قوانین و مقررات مناسب برای هوش مصنوعی می‌تواند به تأثیرات منفی و پیش‌بینی نشده این فناوری در جامعه منجر شود. تأثیرات اصلی این فقدان قانون به صورت‌هایی نظیر عدم حمایت از حقوق شهروندان، عدم اطمینان در استفاده از هوش مصنوعی، تأثیرات اجتماعی و اقتصادی ناخواسته، عدم کنترل مسئولیت‌ها، نقض اخلاقیات و سایر موارد، بروز خواهد کرد.

کلمات کلیدی: هوش مصنوعی، قانون گذاری، مقررات، حاکمیت.

۱ مقدمه

هدف اصلی هوش مصنوعی، به‌کارگیری دانش و قدرت عقلانی انسان‌ها در مسائلی است که تا کنون به‌عنوان کارهایی پیچیده و وابسته به انسان شناخته می‌شده‌اند. با توسعه و پیشرفت هوش مصنوعی در دهه‌های اخیر و همچنین پیشرفت‌های هوش مصنوعی نرم‌افزاری و سخت‌افزاری، تحولات مهمی را در جهان ایجاد کرده و خواهد کرد. شناخت تحولات و کارکردهای هوش مصنوعی به منظور درک نیازها و نقاط حساس قانون‌گذاری

ضروری است، برخی از تحولات مهم هوش مصنوعی شامل:

۱. اتوماسیون و اتوماتیک‌سازی: هوش مصنوعی با توانمند سازی رایانه ها و ربات‌ها برای انجام کارهای پیچیده و تکراری، امکان اتوماسیون و خودکار سازی فرآیندها و صنایع را ایجاد خواهد کرد. این خودکار سازی منجر به کاهش هزینه‌ها، افزایش کارآیی و دقت، و حتی خلق شغل‌های جدید خواهد شد.

۲. حوزه‌های جدید کسب و کار: هوش مصنوعی به شرکت‌ها امکان می‌دهد تا از طریق تحلیل داده‌ها و پیش‌بینی‌های هوشمندانه، به بهبود تصمیم‌گیری‌ها، تحلیل بازار، و تشخیص الگوهای جدید بپردازند. این امر می‌تواند به دستیابی به رقابتی‌تر شدن در بازار و ایجاد فرصت‌های کسب و کار جدید منجر شود [۱].

۳. بهبود مسائل بهداشتی و پزشکی: کاربرد هوش مصنوعی در تشخیص بیماری‌ها، تصویربرداری پزشکی، تحلیل داده‌های پزشکی، طراحی داروها و درمان‌های جدید منجر به بهبود مراقبت‌های بهداشتی و پزشکی خواهد شد.

۴. خودرانی و خودرانندگی: هوش مصنوعی در توسعه خودروهای خودران و ربات‌های خودراننده تأثیر چشمگیری داشته که منجر به کاهش تصادفات و افزایش امنیت رانندگی خواهد شد.

۵. همکاری انسان و ماشین: هدف هوش مصنوعی ایجاد همکاری مثبت بین انسان و ماشین است. این امر می‌تواند در تسهیل و تقویت تصمیم‌گیری انسان‌ها، ارتقاء تجربه کاربری و ایجاد محصولات و خدمات هوشمندانه به کار گرفته شود.

هوش مصنوعی، با توجه به تحولات و پیشرفت‌های روزافزونش، احتمالاً تأثیرات جدید و غیرمنتظره‌ای بر جوامع و جهان خواهد گذاشت. در این بین، مسائل اخلاقی و اجتماعی مرتبط با حفظ حریم خصوصی، تاثیر برای بازار کار و نقش هوش مصنوعی در زندگی روزمره مردم نیز به چالش کشیده خواهند شد. برای بهره‌مندی بهتر از توانایی‌های هوش مصنوعی و کنترل مناسب آن، نیازمند توجه و تصمیم‌گیری‌های هوشمندانه از سوی جوامع و سیاست‌گذاران است.

۲ تأثیرات سوء و مخاطرات هوش مصنوعی

با وجود همه پیشرفت‌ها و امکانات، هوش مصنوعی برخی خطرات و چالش‌های جدی را نیز به همراه دارد. برخی از این خطرات عبارت‌اند از:

۱. از بین رفتن شغل‌ها: هوش مصنوعی و اتوماسیون نابودی برخی مشاغل، به خصوص کارهایی که قابلیت اتوماسیون و اجرای هوشمندانه را دارند، به دنبال دارد. این مسئله منجر به ناترازی در بازار کار شده و نیازمند تأمین شغل‌های جدید و آموزش مجدد افراد در حوزه های جدید باشد.

۲. نقض حریم خصوصی: استفاده از هوش مصنوعی برای جمع‌آوری و تحلیل داده‌های شخصی، مخاطرات امنیتی و احتمال نقض حریم خصوصی افراد را بدنبال خواهد داشت. انتشار و سوءاستفاده از اطلاعات حساس، می‌تواند تأثیرات منفی جدی داشته باشد.

۳. توجه ناکافی به اخلاقیات: بکارگیری هوش مصنوعی بدون رعایت ملاحظات انسانی و اخلاقی ممکن است در برخی موارد به تصمیمات ناعادلانه و تبعیض‌آمیز منجر شود. مثلاً در حوزه تصمیم‌گیری‌های خودروهای خودران، انتخابات اینترنتی یا سیستم‌های قضائی هوشمند.

۴. ایجاد وابستگی: وابستگی زیاد به هوش مصنوعی به‌ویژه در حوزه‌هایی مانند بهبود سبک زندگی و پزشکی می‌تواند منجر به کاهش توانمندی‌های انسانی افراد، فقر متخصصین کارآمد و افزایش وابستگی به فناوری شود.

۵. خطر امنیتی: گسترش کاربرد هوش مصنوعی، از جمله ربات‌ها و سیستم‌های خودران، در افق دراز مدت، احتمال از دست دادن کنترل و نفوذ بدنبال حملات سایبری را متصور می‌سازد. انسان‌ها نیز ممکن است هوش مصنوعی را به نحو نادرستی برای اهداف خودسرانه استفاده کنند.

به‌منظور مقابله با خطرات فوق الذکر، لازم است بعد اخلاقی و انسانی هوش مصنوعی تقویت شده و قوانین و مقررات مناسب برای محدود کردن کاربردهای نامطلوب آن تدوین شود. همچنین، آموزش و آمادگی افراد برای تطابق با تغییرات فناوری و استفاده هوشمندانه از هوش مصنوعی، نقش مهمی در مدیریت اثرات مثبت و منفی آن خواهد داشت.

۱.۲ پیش‌نیازهای قانون‌گذاری

قانون‌گذاری برای هر فناوری نوپدید، معمولاً یک فرآیند تدریجی است و تغییرات متفاوتی در مراحل مختلف رخ می‌دهد. این فرآیند ممکن است تفاوت‌هایی بین کشورها و مناطق داشته باشد و به عوامل زیر وابسته است:

۱. شناخت فناوری: در ابتدا، فناوری نوپدید نیاز به شناسایی و شناخت دارد. علماء، محققان، و متخصصان با انجام پژوهش‌ها و مطالعات علمی سعی می‌کنند برای نخستین بار نحوه کارکرد، اثرات، و کاربردهای فناوری را درک کنند.

۲. اطلاعات و آگاهی عمومی: بعد از شناخت فناوری، اطلاعات در مورد آن به جامعه عمومی ارائه می‌شود. این اطلاعات می‌تواند از طریق رسانه‌ها، کنفرانس‌ها، کارگاه‌ها و منابع دیگر منتشر شود. افزایش آگاهی عمومی از فناوری نقش مهمی در ایجاد قانون‌گذاری مناسب دارد.

۳. تحلیل تأثیرات: دولت‌ها، سازمان‌ها، و نهادهای مختلف به ارزیابی تأثیرات اجتماعی، اقتصادی، امنیتی و فناوری مرتبط با فناوری نوپدید می‌پردازند. این تحلیل‌ها می‌توانند تصمیم‌گیری‌ها را تحت‌تأثیر قرار دهند و نقش مهمی در ایجاد قوانین احتمالی دارند.

۴. ایجاد قوانین و مقررات: پس از اطلاعات کافی و تحلیل‌های مربوطه، قانون‌گذاران می‌توانند به ایجاد قوانین و مقررات مرتبط با فناوری نوپدید بپردازند. این قوانین به‌عنوان راهنمایی برای استفاده ایمن و منصفانه از فناوری در جامعه مطرح می‌شوند.

۵. تطبیق و به‌روزرسانی: با گذشت زمان و تجربه از استفاده از فناوری، قوانین و مقررات ممکن است نیاز به تطبیق و به‌روزرسانی داشته باشند. تغییرات در نحوه استفاده و پیشرفت‌های جدید در فناوری ممکن است نیاز به اصلاحات قانونی داشته باشند.

فرآیند قانون‌گذاری ممکن است با چالش‌ها و تعارض‌هایی همراه باشد، چرا که ممکن است نظرات مختلف و گاهاً متضادی درباره تأثیرات و کاربردهای فناوری وجود داشته باشد. بنابراین، ایجاد فرآیندی جامع و با مشارکت افراد و نهادها در قانون‌گذاری می‌تواند بهبود و کارآیی در قوانین مرتبط با فناوری نوپدید را به دنبال داشته باشد.

۲.۲ بلوغ و آمادگی برای قانون‌گذاری

فناوری هوش مصنوعی در حال حاضر به مرحله‌ای از بلوغ رسیده است که نیاز به آمادگی قانون‌گذاری و تنظیم قوانین و مقررات وجود دارد. هوش مصنوعی در دهه‌های اخیر پیشرفت‌های چشمگیری داشته و در بسیاری از زمینه‌ها کاربرد دارد. برخی از این زمینه‌ها عبارت‌اند از:

۱. خودروهای خودران: صنعت خودرو با توجه به پیشرفت‌های هوش مصنوعی، به سمت توسعه خودروهای خودران پیش می‌رود. این فناوری نیازمند قوانین و مقررات مناسبی است تا امنیت و حفاظت از مسافران و عابران پیاده را تضمین کند.

۲. پزشکی و بهبود بشریت: هوش مصنوعی در تشخیص بیماری‌ها، طراحی داروها، ایجاد ربات‌های پزشکی و کمک به بهبود کیفیت زندگی انسان‌ها تأثیرگذار است. این زمینه‌ها نیازمند قوانین و مقررات حفاظتی و اخلاقی هستند.

۳. حوزه بانکداری و مالی: هوش مصنوعی در حوزه مالی برای تحلیل داده‌ها، پیش‌بینی بازار، و جلوگیری از تقلب‌ها استفاده می‌شود. قوانین مناسب برای محافظت از حریم خصوصی مشتریان و پیشگیری از سوءاستفاده‌ها الزامی است.

۴. امنیت سایبری: هوش مصنوعی به عنوان یک ابزار قدرتمند در امنیت سایبری مورد استفاده قرار می‌گیرد. تنظیم قوانین مرتبط با استفاده از هوش مصنوعی در امنیت و مقابله با حملات سایبری ضروری است.

۵. اخلاقیات هوش مصنوعی: قوانین و مقررات مرتبط با اخلاقیات هوش مصنوعی نیازمند تنظیم شدن هستند تا از تصمیم‌گیری‌های ناعادلانه و تبعیض‌آمیز جلوگیری شود.

با توجه به اهمیت و گستردگی کاربردهای هوش مصنوعی، آمادگی قانون‌گذاری برای تنظیم مقررات و قوانین مرتبط با این فناوری بسیار ضروری است. این کار به عنوان یک چالش بزرگ و همه‌جانبه، همکاری بین دولت‌ها، صنعت‌ها، محققان، و نهادهای مختلف را می‌طلبد تا قوانین منصفانه و مؤثری را اجرا کنند که از یک سو توسعه فناوری را ترویج دهند و از سوی دیگر امنیت و حقوق افراد را حفظ کنند.

۳ مسیر قانون‌گذاری

قانون‌گذاری برای یک فناوری تازه یک فرآیند پیچیده و چالش‌برانگیز است که مراحل مختلفی را شامل می‌شود. برای قانون‌گذاری یک فناوری تازه، مراحل مهم زیر باید طی شوند:

۱. شناخت فناوری: نخستین مرحله در قانون‌گذاری فناوری تازه، شناخت دقیق و جامع از این فناوری است. این شناخت باید توسط علماء، متخصصان، و محققان انجام شود تا اطلاعات کامل و دقیقی در مورد عملکرد، کاربردها، و تأثیرات این فناوری بر جامعه به‌دست آید.

۲. تحلیل تأثیرات: پس از شناخت فناوری، باید از تحلیل تأثیرات آن استفاده کرد. این تحلیل باید شامل ارزیابی اثرات اجتماعی، اقتصادی، امنیتی و اخلاقی فناوری باشد تا ابعاد مختلف مورد تأثیر قرار گیرد.

۳. مشارکت عمومی: در این مرحله، اطلاعات و نتایج شناخت و تحلیل‌ها باید به جامعه و عموم مردم ارائه شود. بازخورد و نقدهای جامعه می‌تواند در تشکیل و تصمیم‌گیری‌های قانون‌گذاری تأثیرگذار باشد.

۴. تنظیم قوانین و مقررات: براساس تحلیل‌ها و بازخوردهای عمومی، قوانین و مقررات مرتبط با فناوری تازه باید تنظیم شود. این قوانین باید مراعات اهداف اجتماعی، اقتصادی، امنیتی و اخلاقی باشند.

۵. اجرا و نظارت: پس از تنظیم قوانین، اجرا و نظارت مناسب بر شیوه اجرا ضروری است. دولت‌ها و نهادهای ذی‌صلاح مسئول اجرا و نظارت بر اجرای قوانین و مقررات هستند تا از رعایت موارد قانونی و محافظت از حقوق و حریم خصوصی افراد اطمینان حاصل شود.

۶. تطبیق و به‌روزرسانی: با گذشت زمان و تجربه از استفاده از فناوری، نیاز به تطبیق و به‌روزرسانی قوانین ممکن است به وجود بیاید تا با پیشرفت‌ها و تغییرات جدید در فناوری هماهنگ شوند.

اهمیت مشارکت عمومی و دیدگاه‌های مختلف در این فرآیند نیز نباید نادیده گرفته شود. همچنین، قانون‌گذاری برای فناوری تازه به چالش‌های اخلاقی و اجتماعی نیز به همراه دارد که نیازمند توجه دقیق و کارآمد از سوی قانون‌گذاران است.

۴ مدل‌های حاکمیت جهانی بر فناوری هوش مصنوعی

در حال حاضر، مدل حاکمیت جهانی بر فناوری هوش مصنوعی هنوز در مراحل شکل‌گیری است و همچنان به چالش‌هایی برخورد دارد. برای مدل حاکمیت جهانی بر فناوری هوش مصنوعی می‌توان ایده‌ها و الگوهای مختلفی مطرح کرد که در آینده ممکن است شکل بگیرد:

۱. تشکیل سازمان‌ها و نهادها: برای مدیریت و نظارت بر فناوری هوش مصنوعی به نحو احسن، می‌توان سازمان‌ها و نهادهای جهانی برای همکاری و تعامل بین کشورها تشکیل داد. این سازمان‌ها می‌توانند به شناخت و تنظیم استانداردها، اخلاقیات، امنیت، حفاظت از حریم خصوصی و تدوین قوانین مرتبط با هوش مصنوعی مشغول باشند.

۲. تعامل ملت‌ها: مدیریت هوش مصنوعی نیازمند همکاری و تعامل بین ملت‌ها است. ایجاد فضایی برای تبادل دانش و تجربیات، مشارکت در پروژه‌های مشترک، و ایجاد ارتباطات میان کشورها می‌تواند به ایجاد حاکمیت جهانی بر هوش مصنوعی کمک کند.

۳. ایجاد قوانین مشترک: تعیین قوانین مشترک و استانداردهای جهانی برای استفاده از هوش مصنوعی می‌تواند به ایجاد یک محیط عادلانه و امن برای توسعه و استفاده از این فناوری کمک کند. این قوانین باید به توجه به نیازها و مشکلات مختلف جوامع بین‌المللی تدوین شوند.

۴. تأمین توافق‌ها و اجماع‌های بین‌المللی: از طریق تبیین توافق‌ها و اجماع‌های بین‌المللی، می‌توان برخی از چالش‌های حاکمیت جهانی بر هوش مصنوعی را حل کرد. توافق‌ها می‌توانند به تعیین خط‌مشی‌ها و مقررات مشترک و هماهنگی عملیات مرتبط با هوش مصنوعی کمک کنند.

۵. توسعه فناوری بهره‌ور: به منظور توسعه فناوری هوش مصنوعی با هدف بکارگیری مسئولانه و اخلاقی، نیازمند تدوین دستورالعمل‌ها و راهنماهایی هستیم که این فناوری را با رعایت تمامی ملاحضات قابل استفاده نماید.

اصول اخلاقی و انسان‌مندی، حفاظت از حریم خصوصی، پیشگیری از تبعیض‌ها و تأمین امنیت سایبری از جمله موضوعاتی هستند که باید در مدل‌سازی حاکمیت جهانی بر فناوری هوش مصنوعی مد نظر قرار گیرند. تشکیل تیم‌های بین‌المللی و همکاری میان کشورها می‌تواند به تسهیل این فرآیند کمک کند. همچنین، در طول زمان، ممکن است تغییرات و به‌روزرسانی‌های مکرر در این مدل حاکمیت اعمال شود تا با تغییرات فناوری هوش مصنوعی و نیازهای جامعه هماهنگ شود [۲] [۳].

۵ بررسی مدل چندذی‌نفعی برای مشارکت موثر

امکان استفاده از مدل چندذی‌نفعی با مشارکت تمامی کشورها برای کنترل و قانون‌گذاری هوش‌مصنوعی وجود دارد و این رویکرد می‌تواند بسیار مؤثر و پایدار باشد. مدل چندذی‌نفعی به معنای همکاری و تعامل بین

دولت‌ها، شرکت‌ها، سازمان‌ها و سایر نهادهای مرتبط در تصمیم‌گیری و قانون‌گذاری است.

۱.۵ کارکردهای مدل چندذی‌نفعی برای جلب مشارکت حداکثر

در صورت تحقق مدل چندذی‌نفعی، اجرای این مدل به منظور رفع مشکلات و کمک به حل مسائل زیر انتخاب مناسبی است.

۱. همسوسازی قوانین و مقررات : با همکاری و تعامل بین کشورها و نهادهای مختلف، می‌توان قوانین و مقررات مرتبط با هوش‌مصنوعی را همسو و یکپارچه کرد تا از ایجاد تضادها و اختلافات میان قوانین ملی جلوگیری شود.

۲. مطالعه اثرات اجتماعی و اقتصادی: با همکاری کشورها و نهادها، می‌توان تجربیات مفید را در مورد اثرات اجتماعی، اقتصادی و اخلاقی هوش مصنوعی جمع‌آوری کرد و بر اساس آن‌ها تصمیم‌گیری کرد.

۳. تعیین استانداردها: با تعامل بین کشورها و صنعت‌ها، می‌توان استانداردهای مشترکی برای هوش مصنوعی تعیین نمود تا به توسعه و استفاده از این فناوری کمک کند و از ناسازگاری‌ها جلوگیری شود.

۴. حفاظت از حریم خصوصی و امنیت: با مشارکت تمامی ذینفعان مرتبط، می‌توان بهترین روش‌ها برای حفاظت از حریم خصوصی و امنیت در استفاده از هوش مصنوعی تدوین کرد.

۵. تقسیم مسئولیت‌ها: با همکاری کشورها و نهادها، می‌توان مسئولیت‌های مرتبط با کنترل هوش مصنوعی را به‌طور مناسب تقسیم کرد و نقاط ضعف و نقاط قوت هر کشور را به نحو احسن مدیریت کرد.

البته توجه به چالش‌ها و موانع نیز ضروری است. مثلاً دریافت بازخورد از همه ذی‌نفعان ممکن است زمان‌بر و مشکلات سیاسی بوجود آورد. همچنین، تفاوت‌های فرهنگی، اقتصادی و سیاسی بین کشورها می‌تواند مانع هماهنگی کامل در مدل چندذی‌نفعی باشد. با این حال، این رویکرد همکاری و تعامل بین ملت‌ها و نهادها را به منظور ایجاد حاکمیت جهانی بر هوش مصنوعی بهتر و مؤثرتر می‌کند.

۲.۵ تعادل در نقش کشورها و سکوها

با تجربه فعلی از مدل حکمرانی اینترنت، توجه به انحصارگرایی سکوها و مشکلاتی که منافع سکوها با مولفه های امنیتی برخی کشورها وجود دارد، در قانون‌گذاری و تنظیم گری جهانی برای هوش مصنوعی، نقش هر دو کشورها و سکوهای مرتبط با هوش مصنوعی بسیار مهم است و باید به‌طور تعادل‌آمیز از هر دو استفاده شود. این دو عامل دارای نقاط قوت و ضعف خود هستند که نیازمند تعادل مناسب و همکاری همه‌جانبه هستند. دلایل اصلی این تعادل به شرح زیر است:

۱. قدرت و تأثیر کشورها: کشورها به عنوان موجودیت‌های سیاسی و اقتصادی با قدرت و تأثیر بالا در مسائل بین‌المللی، می‌توانند در تعیین سیاست‌ها و قوانین جهانی برای هوش مصنوعی نقش بسیار مهمی داشته باشند. این کشورها قادر به تعیین قوانین و تنظیم مقررات مرتبط با هوش مصنوعی بر اساس نیازها و منافع خود هستند.

۲. دستیابی به داده‌ها و تجربیات: پلتفرم‌ها و شرکت‌های مرتبط با هوش مصنوعی معمولاً دسترسی به داده‌ها و تجربیات گسترده‌تری دارند. این داده‌ها و تجربیات می‌توانند به عنوان مبنای تصمیم‌گیری در قانون‌گذاری و تنظیم‌های جهانی مورد استفاده قرار بگیرند.

۳. توانایی نوآوری و تکنولوژی: شرکت‌ها و پلتفرم‌های مرتبط با هوش مصنوعی معمولاً در زمینه تکنولوژی و نوآوری بسیار پیشرو هستند. آن‌ها می‌توانند به تعیین راهبردها و استانداردهای جهانی برای هوش مصنوعی کمک کنند.

۴. تعامل با اندازه‌ها و چالش‌های ملی: هر کشور نیازهای و چالش‌های ملی خود را دارد که ممکن است با هم کشورها تفاوت داشته باشد. در این زمینه، کشورها می‌توانند نقشی بسیار مؤثر در تنظیم قوانین برای هوش مصنوعی ایفا کنند.

هماهنگی و همکاری بین کشورها و پلتفرم‌های مرتبط با هوش مصنوعی امری ضروری است. از یک سو، کشورها می‌توانند به عنوان نماینده‌های سیاسی و اقتصادی در قانون‌گذاری جهانی نقش بیشتری داشته باشند. از سوی دیگر، پلتفرم‌ها و شرکت‌ها می‌توانند با تجربه‌های عملی و دسترسی به داده‌ها کمک کنند که تصمیم‌گیری‌های بر پایه‌ی اطلاعات دقیق‌تر و کاراتری انجام شود. همچنین، باید توجه داشت که در این فرآیند، حفظ امنیت داده‌ها و حریم خصوصی کاربران نیز از اهمیت بسیاری برخوردار است [۴].

۶ نقش فرهنگ، سنت و مذهب در فرآیند قانون‌گذاری هوش مصنوعی

بهره برداری امن و اخلاقی از فناوری هوش مصنوعی با ضرورت قانون‌گذاری هوش مصنوعی در کشور جمهوری اسلامی ایران تضمین می‌شود. مذهب، فرهنگ و سنت‌های جمهوری اسلامی می‌توانند تأثیر زیادی در قانون‌گذاری هوش مصنوعی داشته باشند به دلیل ماهیت ارزش‌ها، اخلاقیات و اولویت‌های اجتماعی و فرهنگی آنها. تاثیرات اصلی به شرح زیر است:

۱. حفاظت از حریم خصوصی: از نظر مذهبی و فرهنگی، حفاظت از حریم خصوصی افراد از اولویت‌های مهم است. این ارزش‌ها می‌توانند در تعیین قوانین حفاظتی و محافظت از حریم خصوصی در هوش مصنوعی تأثیرگذار باشند.

۲. اخلاقیات و عدالت: اصول اخلاقی و عدالت در فرهنگ اسلامی و مذهب جمهوری اسلامی بسیار مهم هستند. در قانون‌گذاری هوش مصنوعی، تأثیرات اجتماعی، اختلافات طبقاتی، و تعامل با محیط زیست باید مورد توجه قرار گیرند تا عدالت اجتماعی حفظ شود.

۳. حفظ انسانیت: مذهب و فرهنگ اسلامی انسان را به عنوان مخلوقی با ارزش تعریف می‌کنند و از آنها درخواست می‌کنند که در برابر تکنولوژی‌ها احتیاط و توجه کنند. قانون‌گذاری هوش مصنوعی باید به این مسئله توجه داشته باشد و محافظت از انسان‌مندی را مدنظر قرار دهد.

در نهایت، در قانون‌گذاری هوش مصنوعی در کشور جمهوری اسلامی ایران، توجه به ارزش‌ها، اخلاقیات، اولویت‌ها و نیازهای فرهنگی و مذهبی مهم است تا از ایجاد تضاد با ارزش‌های جامعه پرهیز کرده و بهره‌برداری مسئولانه از این فناوری تضمین شود [۲].

۷ موانع و موفقیت‌های پیش رو

موانع و مشکلات قانون‌گذاری هوش مصنوعی در ایران شامل این موارد می‌باشد:

۱. کمبود قوانین: در حال حاضر، قوانین کامل و جامع برای هوش مصنوعی در ایران وجود ندارد. این کمبود می‌تواند به عدم تنظیم‌گری کافی و ناتوانی در مدیریت مسائل اخلاقی، حفاظت از حریم خصوصی و مسئولیت‌ها منجر شود.

۲. نیاز به تخصص‌های برنامه‌ریزی: قانون‌گذاری هوش مصنوعی نیازمند تخصص‌های برنامه‌ریزی و حوزه‌های فنی است. کمبود نیروی متخصص در این زمینه می‌تواند مانع ایجاد قوانین کامل و جامع شود.

۳. تأخیر در تطبیق با فناوری: هوش مصنوعی به سرعت در حال توسعه است و تطابق قوانین با پیشرفت‌های تکنولوژیکی می‌تواند مسئله‌ای برای قانون‌گذاری در ایران باشد.

۴. نیاز به هماهنگی بین نهادها: در حال حاضر، مسئولیت قانون‌گذاری هوش مصنوعی ممکن است بین چند نهاد مختلف پراکنده شده باشد. هماهنگی مؤثر بین این نهادها برای تدوین قوانین مشکل می‌تواند باشد.

۵. ترس از عواقب ناخواسته: نگرانی‌ها از اثرات ناخواسته هوش مصنوعی بر اشتغال، اقتصاد و اجتماع ممکن است باعث تردید در قانون‌گذاری و ایجاد مشکلات دیگر گردد.

شکل ۱: موانع و مشکلات قانون‌گذاری فناوری هوش مصنوعی

برای حل این مشکلات، نیازمند توجه به آموزش نیروی متخصص، ایجاد تیم‌های متخصص در زمینه هوش مصنوعی و هماهنگی بین نهادها و مراجع ذیربط هستیم تا به قوانین مناسبی برای هوش مصنوعی دست یابیم و از فواید این فناوری بهره‌برداری امن و مسئولانه ایجاد کنیم.

۸ نقشه راه قانون‌گذاری هوش مصنوعی برای جمهوری اسلامی ایران

برای قانون‌گذاری هوش مصنوعی در ایران، می‌توان به مراحل زیر اشاره کرد:

۱. ایجاد یک کمیته تخصصی: ایجاد یک کمیته تخصصی با حضور نخبگان و متخصصان در حوزه هوش مصنوعی و حقوق به منظور تدوین قوانین و مقررات مرتبط با این فناوری.

۲. ارزیابی وضعیت کنونی: انجام تحقیقات و بررسی وضعیت کنونی هوش مصنوعی در ایران به همراه شناسایی مشکلات و نیازها.

۳. ایجاد قوانین محافظتی: ایجاد قوانین حفاظتی برای حمایت از حریم خصوصی شهروندان و جلوگیری از سوء استفاده از هوش مصنوعی.

۴. تنظیم‌گری اخلاقیات: تعیین اصول اخلاقی و مسئولیت‌های هوش مصنوعی در مواجهه با تصمیم‌گیری‌های اجتماعی و اقتصادی.

۵. تشویق به تحقیق و توسعه: ارتقاء تحقیقات در حوزه هوش مصنوعی و توسعه فناوری‌های مرتبط به منظور رشد این حوزه در کشور.

۶. ایجاد همکاری‌های بین‌المللی: برقراری همکاری با کشورها و سازمان‌های بین‌المللی برای تبادل دانش و تجارب و ایجاد قوانین جهانی.

۷. آموزش و آگاهی‌بخشی: آموزش نیروهای کارآمد در حوزه هوش مصنوعی و آگاهی‌بخشی عمومی درباره فواید و مشکلات این فناوری.

۸. تعیین نظام نظارتی: تعیین نظام نظارتی بر استفاده از هوش مصنوعی و تعیین مسئولین مربوطه برای اجرای قوانین.

۹. تجربه و اجرای آزمایشی: اجرای آزمایشی قوانین و برنامه‌ها به منظور بررسی اثربخشی و تطابق با نیازها و تغییرات تکنولوژیکی.

۱۰. ارزیابی و به‌روزرسانی: ارزیابی دوره‌ای و به‌روزرسانی قوانین هوش مصنوعی به منظور تأمین پایداری و انطباق با شرایط جامعه.

با پیروی از این نقشه‌راه و اجرای دقیق قوانین، هوش مصنوعی در ایران به نحوی مناسب و با مسئولیت‌پذیری اجرا خواهد شد که مزایا و فواید آن به نفع جامعه خواهد بود و همچنین از تأثیرات ناخواسته و منفی آن جلوگیری خواهد شد.

۹ نتیجه‌گیری

قانون‌گذاری هوش مصنوعی در کشور جمهوری اسلامی ایران از اهمیت بسیاری برخوردار است. هوش مصنوعی یک فناوری پیشرفته است که تأثیرات عمیقی بر جامعه، اقتصاد و امنیت دارد. در این زمینه، ایجاد یک نظام قانونی و مقررات مناسب برای مدیریت و کنترل هوش مصنوعی بسیار حیاتی است.

قوانین حفاظتی برای حریم خصوصی شهروندان، تنظیم‌گری اخلاقیات هوش مصنوعی، مدیریت مسئولیت‌ها و تعیین نظام نظارتی از جمله مواردی هستند که باید در قانون‌گذاری هوش مصنوعی در نظر گرفته شوند. همچنین، تأکید بر تحقیقات و آموزش در حوزه هوش مصنوعی و ایجاد همکاری‌های بین‌المللی نیز ضروری است.

ایجاد یک نقشه راه جامع و اجرایی برای قانون‌گذاری هوش مصنوعی به منظور استفاده امن، مسئولانه و مؤثر از این فناوری از اهمیت بالایی برخوردار است. با توجه به رشد سریع هوش مصنوعی و تأثیرات آن بر جوامع، مسئولان کشور نیازمند تلاش جدی برای تدوین و اجرای قوانین مناسب در این زمینه هستند. تأمین حفاظت حریم خصوصی شهروندان، اطمینان از اخلاقیات اجتماعی، ارتقاء تحقیقات و توسعه فناوری‌های مرتبط و همکاری با جوامع بین‌المللی، از مسائلی هستند که باید در قانون‌گذاری هوش مصنوعی در ایران به آنها توجه کرد. این گام‌ها می‌تواند به تحقق اهداف کشور در این حوزه و ایجاد اطمینان عمومی در استفاده از هوش مصنوعی کمک کند.

مراجع

[۱] علینقیان، اشکان؛ صفدری رنجبر، مصطفی و محمدی، مهدی (۱۴۰۰). اهداف و ابزارهای سیاستی توسعه هوش مصنوعی؛ جستاری در برنامه‌های سیاستی کشورهای منتخب.

[۲] قربانلو، رامین (۱۴۰۲). تأثیر هوش مصنوعی بر هنر، کار و خانواده، ششمین کنفرانس بین‌المللی پژوهش‌های نوین در مهندسی برق، کامپیوتر، مکانیک و مکاترونیک در ایران و جهان اسلام، تهران.

[۳] قاسمی، زهرا؛ پیروز، حکیمه و جابرزاده، ساناز (۱۴۰۲). هوش مصنوعی، سومین کنفرانس بین‌المللی مهندسی برق، کامپیوتر، مکانیک و هوش مصنوعی، مشهد.

[۴] محمدی، فرهاد و موسوی، فرانک (۱۴۰۲). بررسی مسائل اخلاقی و حریم خصوصی هوش مصنوعی در آموزش، سومین کنفرانس بین‌المللی مهندسی برق، کامپیوتر، مکانیک و هوش مصنوعی، مشهد.

[۵] عالی، فاطمه و سلطانی، رضا (۱۴۰۲). بررسی هوش مصنوعی بر آینده جهان و شیوه بکارگیری آن در آموزش، سومین کنفرانس بین‌المللی مهندسی برق، کامپیوتر، مکانیک و هوش مصنوعی، مشهد.

استراتژی تحول دیجیتال پارلمان در مسیر شفافیت و دموکراسی

یاشار ابری[۱]، احمد فرید اصیل[۱]

[۱]دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
yasharabri@ut.ac.ir ،faridaseel.4all@gmail.com

چکیده

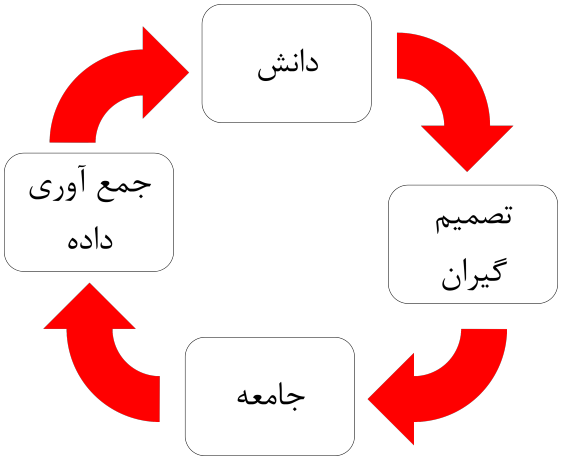
در این دوران دیجیتالی، سازمان‌های عمومی، مانند مجلس‌ها، ملزم به توسعه استراتژی‌های دیجیتالی هستند تا با متحول کردن عملکردها خود را بهبود دهند. این استراتژی باید از فناوری‌های دیجیتال استفاده کند تا با ایجاد شفافیت امکانات مهمی را هم برای شهروندان و هم برای نمایندگان مجلس در فرآیند سیاست‌گذاری فراهم کند. مجلس‌ها می‌توانند با استفاده از دانشی که در طول چرخه‌های زندگی مجلس از جمع‌آوری داده در جامعه به دست می‌آید تصمیمات سیاست‌گذاری مبتنی بر شواهد (EBP) را در انتخاب، تدوین و ارزیابی سیاست‌های عمومی دخیل کنند. این مقاله پیشنهاد می‌دهد که از ابزارهای دیجیتال در همه مراحل تصمیم‌گیری در مجلس استفاده شود. یک مسیر برنامه‌ریزی ارائه شده است، که در زمینه چارچوب تحول دیجیتال مبتنی بر کاربر و فناوری‌های دیجیتال آن قرار دارد. جنبه‌هایی که تحلیل می‌شوند، شرایط محدودیت برای ایجاد محیط دیجیتال EBP را نیز شامل می‌شود. راهکار دموکراسی مدرن با این سازوکارهای شفافیت مبتنی بر داده‌های دریافتی از جامعه موجب افزایش اطمینان مردم به آینده کشور خواهد شد.

کلمات کلیدی: شفافیت پارلمانی، سیاست گذاری مبتنی بر شواهد، استراتژی دیجیتال، تحول دیجیتالی پارلمان.

۱ مقدمه

بزرگترین تهدید و هزینه برای هر کشوری افزایش نگرانی‌های شهروندان و کاهش اعتماد شهروندان است. راهکار دموکراسی‌های مدرن ایجاد شفافیت، پاسخ‌گویی (دالتون، اسکارو، و کین، ۲۰۰۴) و پیروی از تدابیر سیاستی هستند که بر زندگی روزمره شهروندانشان تأثیر می‌گذارد .سیاست‌گذاران، تصمیم‌گیران و مدیران می‌توانند با استفاده از ابزارهای دیجیتال پیشرفته (فیتسیلیس، کوریزیس و شفبک، ۲۰۲۲) امکانات لازم برای این موضوع را فراهم کنند.

تصمیم‌گیری‌های مدیریتی بر اساس تجربیات گذشته و دانش به دست آمده از جامعه است. به همین دلیل، دانش سازمانی کسب‌شده در طول چرخه زندگی یک سازمان عمومی باید به طور فزاینده‌ای بر اساس داده‌های دیجیتال شناختی یکپارچه، در چارچوبی از استراتژی دیجیتال جامع قرار گیرد. عدم مشارکت



شکل ۱: دانش به دست آمده از جامعه را تصمیم گیران در سیاست گذاری‌ها دخیل می‌کنند و مجدداً بازتاب جامعه را به میزان رضایت از سیاست‌ها در سیاست گذاری‌های جدید اعمال می‌کنند.

تمام کاربران اصلی (سیاست‌گذاران، شهروندان، عوامل، دانشمندان و جوامع) در فرآیند تصمیم‌گیری، باعث می‌شود دانش به میزان زیادی نادیده گرفته شود.

نگاه کردن به تصمیم‌گیری‌های «سیاست‌گذاری مبتنی بر شواهد» یا همان EBP (که مخفف عبارت Evidence-Based Policy است) مطابق شکل ۱ به عنوان یک راه‌حل، تلاش دارد تمام افرادی که زندگی‌شان تحت تأثیر و درگیر در فرآیند سیاست‌گذاری (عمدتاً در فرمول‌بندی سیاست‌های عملیاتی عمومی) را در نظر بگیرد که این دانش مورد استفاده به طور فزاینده‌ای بر اساس داده‌های دیجیتال شناختی به دست می‌آید.

تلاش‌های هماهنگ برای اتصال برنامه‌ها و پروژه‌ها و اتصال بین واحدها و درک تنوع فرآیندهای داخلی و تکنیک‌های سازمانی در طراحی سامانه‌های الکترونیکی دسترسی به خدمات بهتر و مطابق با نیازهای عوامل و نیازهای افرادی که تحت تاثیر سیاست‌گذاری قرار می‌گیرند را فراهم می‌کند (فیتسیلیس، کوریزیس و شفبک، ۲۰۲۲) و به آن‌ها اجازه می‌دهد به طور مؤثر در توسعه یک استراتژی یکپارچه، یکنواخت و قابل درک با تأکید بر جهان دیجیتال مشارکت داشته باشند. پارلمان مجلس به عنوان یکی از مهم‌ترین و مرکز قانون گذاری و تصمیم گیری بایستی همراه با وظایف سنتی سازمانی معمول خود، استفاده از فناوری‌های دیجیتال پیشرفته و ابزارهای قانون‌گذاری الکترونیک را در دستور روند کاری خود قرار دهد (شکل ۲).

فرصت‌هایی که توسط فناوری‌های دیجیتال برای سیاست‌گذاری ایجاد می‌شود، به سه دسته اصلی تقسیم می‌شود: مدیریت دانش و افراد، تجزیه و تحلیل داده‌ها و دانش حاصل از مشارکت شهروندان در کل فرآیند (لوید، ۲۰۲۰). فناوری‌های دیجیتال نه تنها مانع نیستند بلکه به بهره‌برداری از حافظه نهادی، ایجاد روش‌های همکاری بیشتر و کمک به سیاست‌گذاران در بهره‌گیری بهتر از تجربه و مهارت کارکنان دولت در سراسر دستگاه دولتی کمک می‌کنند.

الگوی دانش افراد و سیستم‌های مجلس را مورد نظر دارد و همه شهروندان و کاربران مجلس را تحت


نتایج آرای نمایندگان داوطلب

عنوان رای گیری

فصل10ـ طرحهاي صنعت،معدن و رشد تولیدـ ماده 48 بند الف لایحه برنامه هفتم توسعه لایحه برنامه هفتم

تعداد آرای موافق	تعداد آرای مخالف	تعداد آرای ممتنع	تعداد نمایندگان حاضر
85	104	6	204

ترتیب نمایش اسامی نمایندگان بر اساس نام خانوادگی می باشد.

جستجو: نمایش محتویات 50

تصویر	نام نماینده	نام خانوادگی نماینده	وضعیت	رای
	علي	آذري (قوچان)	حضور	مخالف
	منصور	آرامي (بندرعباس)	عدم حضور	----
	رضا	آریان‌پور (مینودشت)	حضور	موافق

شکل ۲: سایت پارلیران آرا نمایندگان داوطلب شفافیت را در ایران منتشر می‌کند.

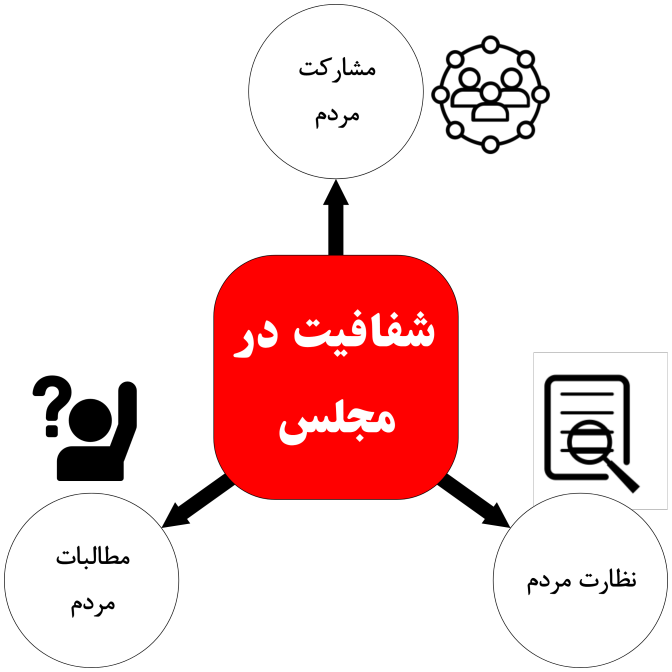
تأثیر قرار می‌دهد. داده‌های مجلس به عنوان بخشی از سیاست‌گذاری مبتنی بر شواهد در این محیط جدید، بدون شک بسیار حیاتی است.

در این مقاله به بررسی پیامدهای یک استراتژی دیجیتال در یک مجلس به عنوان بخشی از برنامه‌ریزی استراتژیک کلان مجلس پرداخته می‌شود. نقش تحول دیجیتال در رویه‌ها و عملکردهای مجلس و نیاز به تحول سازمانی نیز مورد بررسی قرار می‌گیرد. نوشتار پیش‌رو مجموعه از فناوری‌های دیجیتال قابل اجرا برای مجلس‌های تحول‌یافته دیجیتال و نقش آن‌ها در انتخاب سیاست‌های مبتنی بر شواهد (EBP) را مورد بررسی قرار می‌دهد. هدف ارائه پیشنهادی است که در مسیر ترکیب دیجیتالی در یک محیط عملیاتی مجلس پارلمانی توسعه پیدا می‌کند.

۲ استراتژی دیجیتال

در دوران عصر دیجیتال، رسانه‌های اجتماعی چالشی برای حکومت‌های مدرن محسوب می‌شوند (شفبک، اسپیلیوتوپولوس و ریسه، ۲۰۱۲؛ اسپیلیوتوپولوس، شفبک و کوریزیس، ۲۰۱۳). اکثر مجالس برنامه‌های استراتژیک یا برنامه‌های عملیاتی پیچیده را منتشر می‌کنند، اما تنها تعداد کمی استراتژی دیجیتال تدوین کرده‌اند که به طور اساسی عملکردهای مجلس را با بهره‌گیری از تکنولوژی‌های مشارکت و نظارت و مطالبات شهروندان متحول کند (شکل۳).

سؤال باقی می‌ماند که آیا کاربران نیاز به برنامه‌ها، ابزارها و خدمات فوق‌العاده دیجیتال دارند و آیا این‌ها عملکرد بهتری نسبت به جایگزین‌های غیر دیجیتال دارند. پاسخ مثبت است چرا که رسانه‌های اجتماعی به مشارکت مستقیم شهروندان در امور پارلمانی و تسهیل هم‌کاری اجتماعی اجازه می‌دهند. به همین دلیل، نیاز به تحقیقات کیفی وجود دارد تا ارزیابی شود که کدام ابزارها، خدمات و برنامه‌های مجلس مورد نیاز هستند و استفاده می‌شوند (تاینر، شفبک و کوریزیس، ۲۰۱۸).



شکل ۳: با بهره‌گیری از تکنولوژی‌ها در راستای شفافیت مجلس، می‌توان شهروندان را بیشتر در امور قانون‌گذاری سهیم کرد.

هدف استراتژی دیجیتال جذب همه کاربران، عوامل و شهروندان در فرآیندهای تصمیم‌گیری مجلس است. مجلس‌های مدرن امکان تبدیل شدن به شبکه‌های دستوری همکاری را از طریق استفاده از فناوری‌های دیجیتال دارند (منکارلی، ۲۰۲۱). منکارلی (۲۰۲۱) به نیاز به یک استراتژی دیجیتال پرداخته است که تعادل هیبریدی‌سازی یعنی ترکیب حضور حقیقی و حضور مجازی کاربران مجلس (اعضای مجلس، مشاوران علمی، شهروندان، لابی‌ها، کسب‌وکارها، دانشمندان، متخصصان) در تمام فعالیت‌ها و وظایف مجلس را به همراه دارد.

کوریزیس و همکاران (۲۰۲۱) استراتژی مجلس یکپارچه دیجیتال، دیجیتالی‌سازی عملکردهای مجلس، تسهیل تحول دیجیتال و استفاده از فناوری‌های دیجیتال نوظهور در زمینه مجلس به عنوان چهار پایه اصلی یک چارچوب تحول مجلس (شکل ۴) پیشنهاد می‌دهد. استراتژی دیجیتال حاوی دیدگاه، ارزش‌ها، دامنه و اهداف سازمان است، که با تعریف واضحی از دیجیتالی‌سازی در زمینه مجلس (مانند شفافیت، عدالت، پاسخگویی و نمایندگی اجتماعی) همراه است. با این حال، تنها تعداد کمی از برنامه‌های استراتژیک مجلس یک استراتژی دیجیتال قابل مشاهده را جمع‌بندی کرده‌اند که در آن دیجیتالی‌سازی اجتماعی که قبلاً در حال پیشرفت است (کوریزیس و همکاران، ۲۰۲۱) در نظر گرفته شده است.

تبدیل دیجیتالی مجلس به وظیفه‌ی تشریفات قانون‌گذاری می‌تواند به عنوان بخشی از یک استراتژی کلی در نظر گرفته شود، با طرح اصلی برنامه اقدامات وابسته به داده‌های مجلس. هدف باید رویکردی کاملاً دیجیتالی باشد، که شامل افراد تحت تأثیر سیاست‌گذاری در مراحل اصلی فرآیند سیاست‌گذاری (کوریزیس و

شکل ۴: چارچوب موردنیاز برای ایجاد تحول در مجلس در جهت افزایش مشارکت شهروندان

همکاران، ۲۰۲۰) است و فعالیت‌های انسانی و ویژگی‌های دیجیتال را در محیط حجیمی از داده‌ها و فرآیندها ترکیب می‌کند. سیستم‌های فناوری اطلاعات و ارتباطات ICT) یا همان Information & Communications Technology) مجلس می‌توانند بر اساس یک استراتژی دیجیتال به‌روزرسانی شوند، با دیجیتالی‌سازی عملکردهای مجلس به عنوان بخشی از یک نقشه‌راه قانون‌گذاری الکترونیکی که شامل رویه‌های عملکردی مجلس است.

در این استراتژی، نیاز به شناسایی و برنامه‌ریزی اقدامات دیجیتال با فناوری‌های دیجیتال مناسب وجود دارد. این می‌تواند با ارتقاء سیستم‌های فناوری موجود مجلس و توسعه سیستم‌ها، همراه با ابزارها و برنامه‌هایی که فعالیت‌های سلسله مراتبی و فرآیندهای قانون‌گذاری الکترونیکی / خودکار را به هم مرتبط می‌کنند، به‌دست آید.

معرفی اقدامات فناوری‌های نوآورانه، ابزارها و رویکردهای دیجیتال از طریق تدوین یک استراتژی دیجیتال اغلب با تحول کل سازمان همراه است، که منجر به بهبود عملکرد عملیاتی می‌شود (هس و همکاران، ۲۰۱۶).

۳ سیاست‌گذاری مبتنی بر شواهد (EBP)

به طور کلی تعداد کمی از محققان از ارتباط استراتژی دیجیتال با سیاست‌گذاری مبتنی بر شواهد مطلع هستند. برای درک این نوع از سیاست‌گذاری بایستی به درک مفهوم و منظور از شواهد پرداخته شود. اصطلاح «شواهد» بسیاری از کاربردها دارد و بیشتر به آزمایش‌های کنترل‌شده تصادفی و «آزمایش‌های

طبیعی» به عنوان مطالعات مشاهده‌ای که تأثیرات سیاست‌ها را ارزیابی می‌کنند، ارتباط دارد. نتایج می‌توانند در فرمول‌بندی سیاست‌ها و ارزیابی سیاست‌ها یا در درس‌های قابل انتقال مورد استفاده قرار گیرند. آن‌ها می‌توانند در یک چارچوب گسترده‌تر مصنوع شوند که شامل اصطلاحاتی مانند «تصمیم‌گیری آگاهانه»، «یادگیری از اشتباهات دیگران» و «بازخورد کیفی» از شهروندان است که راه را هم به تغییر سیاست‌ها و هم به «طراحی همکارانه سرویس‌ها» باز می‌کند (راتر، ۲۰۱۲). طراحی همکارانه همچنین می‌تواند در یافتن راه‌حل‌ها برای مسائل پیچیده با استفاده از طراحی مشارکتی، اندیشیدن طراحی و نوآوری بخش عمومی کمک کند (بلومکمپ، ۲۰۱۸).

هد (۲۰۱۶) بین عباراتی مانند «تعریف مسئله یا تنظیم برنامه»، «تحلیل داده‌ها»، «طراحی سیاست یا تدوین سیاست»، «پذیرش سیاست»، «اجرای سیاست» و «بررسی برنامه یا ارزیابی سیاست» تفاوت قائل می‌شود که در همه آن‌ها ابزارهای دیجیتال می‌تواند توسط کاربران / شهروندان مورد استفاده قرار گیرد.

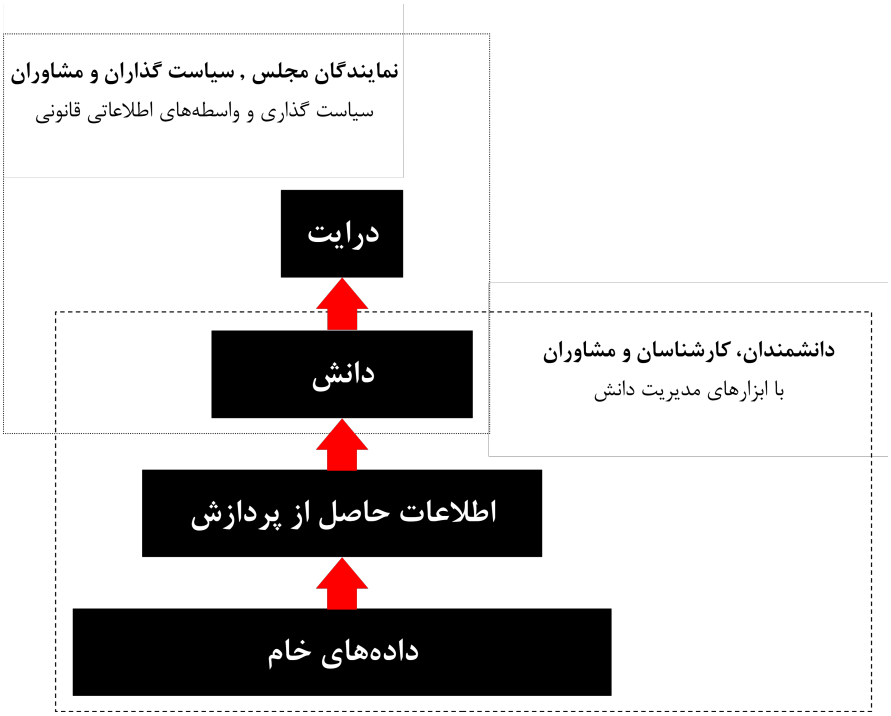
ترکیب شواهد علمی با اصول سیاست‌گذاری، و تبدیل شواهد پیچیده به عبارات و داستان‌های ساده‌تر برای درک افکار عمومی، در فرآیندهای قانونی معمولی است (کائیرنی و الیور، ۲۰۱۷) – اگرچه نمایندگان مجلس ممکن است بیشتر تمرکز خود را بر روی ارتباطات سیاسی قرار دهند که بر اساس شواهد علمی موثق نیست.

اما جمع آوری و تهیه شواهد خود نیز با چالش‌هایی رو به رو است. این چالش‌ها عبارتند از:

- تحلیل داده‌های قابل توجهی برای ایجاد اطلاعات علمی مفید برای استفاده از سیاست‌گذاران و تأثیر برنامه‌های سیاستی نیاز است.
- استفاده مناسب از مطالعات اثرات و پیش‌بینی قبل از اجرا و بعد از اجرا در مراحل سیاست‌گذاری مورد نیاز است.
- نتایج علمی و داده‌ها باید قابل اعتماد باشند زیرا راه‌حل‌ها و سناریوهای سیاستی بر اساس آن‌ها ایجاد می‌شود.
- کیفیت، قابلیت اعتماد، ارتباط و هزینه سیاست عوامل کلیدی هستند.

نمونه‌ای از سیاست‌گذاری مبتنی بر شواهد، استفاده کمیسیون اروپا از اطلاعات آماری برای سهولت در تصمیم‌گیری است که دقت اطلاعات یا داده‌ها در اساس آن وجود دارد. این امر کمک می‌کند تا سیاست‌های مؤثری توسعه یابد. هرم دانش برای سیاست‌گذاری که در شکل ۵ نشان داده شده‌است ارتباط بین داده‌ها، اطلاعات، دانش و حکمت و کاربران مرتبط با ابزارها و برنامه‌های سیاست‌گذاری خود را نشان می‌دهد که می‌تواند به عنوان بهترین شیوه عملکرد مورد استفاده قرار گیرد.

به طور خلاصه، استفاده از شواهد در سیاست‌گذاری مشروعی بسیار حائز اهمیت است. اگرچه استفاده کارآمد از اطلاعات پارلمانی – پس از جمع‌آوری، ادغام و بهره‌برداری از داده‌ها – می‌تواند به یک ذخیره دانش برای تعیین مسیر بهتر پارلمانی تبدیل شود (گرانیکاس، ۲۰۱۳). در استفاده از اطلاعات مبتنی بر شواهد



شکل ۵: هرم دانش نشان می‌دهد که چگونه داده‌های خام جمع‌آوری شده از جامعه در نهایت منجر به درایت در کار قانون‌گذاری و تعیین جهت سیاست‌گذاری‌ها می‌شود.

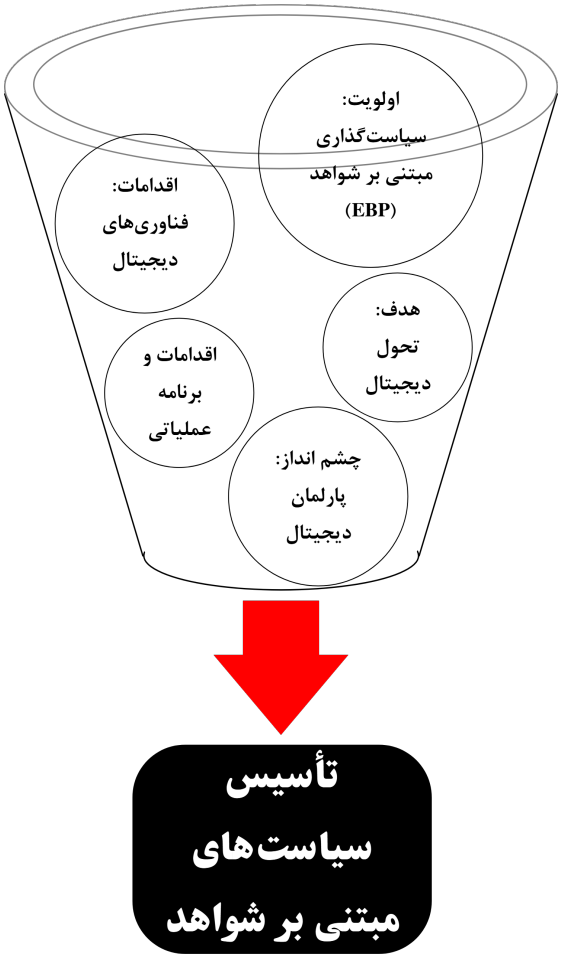
مشکلات متعددی وجود دارد (مونیرو، ۲۰۱۹). در برخی موارد، اطلاعات ارائه شده قابل درک نیست، این ممکن است به دلیل اصطلاحات تخصصی، داده‌های نامناسب، اطلاعات منسوخ، واژگان حقوقی پیچیده یا آمارهای گیج‌کننده باشد (فیتسیلیس، کوریزیس و شفبک، ۲۰۲۲). این ممکن است نتیجه کمبود منابع یا محققان با تجربه مرتبط در دپارتمان تحقیقات پارلمان یا عدم وجود نظارت بر فرآیند تحقیقات دپارتمان باشد.

براساس این، یک استراتژی دیجیتال برای تحول دیجیتالی پارلمان می‌تواند محرک تأسیس سیاست‌های مبتنی بر شواهد باشد، همان‌طور که در شکل ۶ نشان داده شده‌است.

۴ نتیجه‌گیری

پارلمان‌ها می‌توانند استراتژی‌های تحول دیجیتال را به عنوان بخشی از یک برنامه استراتژیک گسترده اتخاذ کنند که فناوری‌های دیجیتال نوآوری را به روند کاری خود ادغام کنند و وظایف سازمانی سلسه‌مراتبی آن‌ها را به‌روزرسانی کنند. پارلمان‌ها نیاز به یک استراتژی دیجیتال با اقدامات مشخص دارند تا پارلمان‌های دیجیتالی با عملکردهای سازمانی ایجاد کنند که آن‌ها را در مسیر تحول دیجیتال قرار دهد و ارزش‌های جدیدی را برای همه رویه‌ها، افراد و سیستم‌های پارلمانی به ارمغان آورد.

استفاده از مدل استراتژی دیجیتال برای سیاست‌گذاری مبتنی بر شواهد، نقش داده‌های پارلمانی به



شکل ۶: استراتژی دیجیتال برای سیاست‌گذاری مبتنی بر شواهد

عنوان بخشی اساسی از فرآیند سیاست‌گذاری مبتنی بر شواهد حائز اهمیت است. تبدیل داده‌ها به دانش پارلمانی برای سیاست‌گذاری هدف نهایی این استراتژی است که موجب سهیم شدن هرچه بیشتر شهروندان در شاخه‌های مختلف شفافیت نظیر نظارت بر مجلس و پیگری مطالبات از مجلس است. این راهکار دموکراسی مدرن موجب کاهش نگرانی شهروندان و افزایش اعتماد آن‌ها خواهد شد که اساسی‌ترین پایه هر کشوری است.

سپاس‌گزاری

از همه پژوهشگران عزیز که یافته‌های خود را در حوزه شفافیت به رایگان در اینترنت به اشتراک گذاشته‌اند و موجب آشنایی نویسندگان با این حوزه گردید و همچنین از اندیشکده شفافیت برای ایران سپاس‌گزاری و قدردانی می‌کنیم.

مراجع

[۱] سایت پارلیران. www.parliran.ir

[۲] وضعی، حسین (۱۳۹۶). «چیستی، چرایی و چگونگی شفافیت». اندیشکده شفافیت برای ایران. https://tp4.ir/408

[۳] نامه جمعی از تشکل‌های دانشجویی (۱۳۹۸). «درخواست دانشجویان از نامزدهای انتخاباتی برای پیوستن به پویش شفافیت».

[4] Fitsilis, F., Koryzis, D., & Schefbeck, G. (2022). "Legal Informatics Tools for Evidence-Based Policy Creation in Parliaments". International Journal of Parliamentary Studies, 1–25. https://doi.org/https://doi.org/10.1163/26668912-bja10031

[5] Mencarelli, A. (2021). "Parliaments Facing the Virtual Challenge: A Conceptual Approach for New Models of Representation". Parliamentary Affairs. https://doi.org/10.1093/pa/gsab052

[6] Koryzis, D., Fitsilis, F., Spiliotopoulos, D., Theocharopoulos, T., Margaris, D., & Vassilakis, C. (2020). "Policy Making Analysis and Practitioner User Experience". In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 12423 LNCS. https://doi.org/10.1007/978-3-030-60114-0_29

[7] Blaser Mapitsa, C., Ali, A. J., & Khumalo, L. S. (2020). "From Evidence to Values-Based Decision Making in African Parliaments". Evaluation Journal of Australasia, 20(2), 68–85. https://doi.org/10.1177/1035719X20918370

[8] Koryzis, D., Dalas, A., Spiliotopoulos, D., & Fitsilis, F. (2021). "ParlTech: Transformation Framework for the Digital Parliament". Big Data and Cognitive Computing, 5(1), 15. https://doi.org/10.3390/bdcc5010015

[9] Rose, D.C., Kenny, C., Hobbs, A., & Tyler, C. (2020). "Improving the Use of Evidence in legislatures: The Case of the UK Parliament". Evidence & Policy: A Journal of Research, Debate and Practice, 16(4), 619–638. https://doi.org/10.1332/174426420X15828100394351

[10] Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2020). "Barriers and Drivers of Digital Transformation in Public Organizations: Results from a Survey in the Netherlands". In G. Viale Pereira, M. Janssen, H. Lee, I. Lindgren, M.P. Rodríguez Bolívar, H. Jochen Scholl, and A. Zuiderwijk (eds.), Electronic Government, 19th IFIP WG 8.5 International Conference, EGOV 2020, Linköping, Sweden, 31 August–2 September, Proceedings, pp. 42–56. Cham: Springer. https://doi.Org/10.1007/978-3-030-57599-1_4

[11] Vial, G. (2019). "Understanding Digital Transformation: A Review and a Research Agenda". The Journal of Strategic Information Systems, 28(2), 118–144.

[12] Nutley, S., Boaz, A., Davies, H., & Fraser, A. (2019). "New Development: What Works Now? Continuity and Change in the Use of Evidence to Improve Public Policy and Service Delivery". Public Money & Management, 39(4), 310–316. https://doi.org/10.1080/09540962.2019.1598202

[13] Lloyd, L. (2020). "Policy making in a digital world", www.instituteforgovernment.org.uk

[14] Ubaldi, B., Van Ooijen, C., & Welby, B. (2019). "A Data-Driven Public Sector: Enabling the Strategic Use of Data for Productive, Inclusive and Trustworthy Governance". OECD Working Papers on Public Governance No. 33. https://doi.org/10.1787/09ab162c-en

[15] Theiner, P., Schwanholz, J., & Busch, A. (2018). "Parliaments 2.0? Digital Media Use by National Parliaments in the EU". In J. Schwanholz, T. Graham, & P.T. Stoll (eds.), Managing Democracy in the Digital Age: Internet Regulation, Social Media Use, and Online Civic Engagement, pp. 77–95. Cham: Springer. https://doi.org/10.1007/978-3-319-61708-4_5

[16] Munyoro, I. (2019). "Assessing Parliament of Zimbabwe's Informatics Database as a Tool for Providing Evidence-Based Information for Decision Making". Journal of Librarianship and Information Science, 51(1), 218–227. https://doi.Org/10.1177/0961000617726122

[17] Mair, D., Smillie, L., la Placa, G., Schwendinger, F., Raykovska, M., Pasztor, Z., & Bavel, R. van. (2019). "Understanding Our Political Nature: How to Put Knowledge and Reason at the Heart of Political Decision-Making". Luxembourg: Publications Office of the European Union. https://doi.Org/10.2760/910822

[18] Blomkamp, E. (2018). "The Promise of Co-Design for Public Policy". Australian Journal of Public Administration, 77(4), 729–743. https://doi.org/10.1111/1467-8500.12310

[19] Crewe, E. (2017). "Ethnography of Parliament: Finding Culture and Politics Entangled in the Commons and the Lords". Parliamentary Affairs, 70(1), 155–172. https://doi.org/10.1093/pa/gsw012

[20] Cairney, P., & Oliver, K. (2017). "Evidence-Based Policymaking Is Not Like Evidence-Based Medicine, so How Far Should You Go to Bridge the Divide between Evidence and Policy?". Health Research Policy and Systems, 15(1), 35. https://doi.org/10.1186/s12961-017-0192-x

[21] Majcen, Š. (2017). "Evidence Based Policy Making in the European Union: The Role of the Scientific Community". Environmental Science and Pollution Research, 24(9), 7869–7871. https://doi.org/10.1007/s11356-016-6247-7.

[22] Head, B.W. (2016). "Toward More 'Evidence-Informed' Policy Making?". Public Administration Review, 76(3), 472–484. https://doi.org/10.1111/puar.12475

[23] Campos, R., Miranda, R., & Rodrigues De Assis, N. (2016). "Initiatives of Knowledge Management in Brazilian Chamber of Deputies". Research in Economics and Management, 1(1). www.scholink.org/ojs/index.php/rem

[24] Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2016). "Options for Formulating a Digital Transformation Strategy". MIS Quarterly Executive, 15, 123–139.

[25] Eggers, W., & Bellman, J. (2015). "The journey to government's digital transformation. A Deloitte Digital global survey". www.deloittedigital.com

[26] Matt, C., Hess, T., & Benlian, A. (2015). "Digital transformation strategies". Business & Information Systems Engineering, 57(5), 339–343.

[27] Curry, D. (2014). "Trends for the Future of Public Sector Reform: A Critical Review of Future-Looking Research in Public Administration". The COCPUs Project, EU FP-7.

[28] Sapp, C. E., Mazzuchi, T., & Sarkani, S. (2014). "Rationalising Business Intelligence Systems and Explicit Knowledge Objects: Improving Evidence-Based Management in Government Programs". Journal of Information & Knowledge Management, 13(02), 1450018. https://doi.org/10.1142/S021964921450018X

[29] Granickas, K. (2013). "Parliamentary Informatics: What Data Should Be Open and How Multi-Stakeholder Efforts Can Help Parliaments Achieve It". European Public Sector Information Platform Topic Report, 2013/05.

[30] Spiliotopoulos, D., Schefbeck, G., & Koryzis, D. (2013). "Obtaining Societal Feedback on Legislative Issues through Content Extraction from the Social Web". Proceedings of the 16th International Legal Informatics Symposium IRIS 2013, Salzburg, Austria, 21–23.

[31] Rutter, J. (2012). Evidence and Evaluation in Policy Making. London: Institute for Government.

[32] Schefbeck, G., Spiliotopoulos, D., & Risse, T. (2012). "The Recent Challenge in Web Archiving: Archiving the Social Web". International Council on Archives Congress, Brisbane, Australia, 20–24 August, 1–5.

[33] Sutcliffe, S., & Court, J. (2005). Evidence-Based Policymaking: What Is It? How Does It Work? What Relevance for Developing Countries? London: Overseas Development Institute.

[34] Hemsley-Brown, J. (2004). "Facilitating Research Utilisation". International Journal of Public Sector Management, 17(6), 534–552. https://doi.org/10.1108/09513550410554805

[35] Dalton, R.J., Scarrow, S.E., & Cain, B.E. (2004). "Advanced Democracies and the New Politics". Journal of Democracy, 15(1), 124–138.

[36] Marston, G., & Watts, R. (2003). "Tampering with the Evidence: A Critical Appraisal of Evidence-Based Policy-Making". The Drawing Board: An Australian Review of Public Affairs, 3(3), 143–163.

[37] Sanderson, I. (2002). "Making Sense of 'What Works': Evidence Based Policy Making as Instrumental Rationality?". Public Policy and Administration, 17(3), 61–75. https://doi.org/10.1177/095207670201700305

بررسی و شناسایی کاربردهای فناوری بلاک‌چین و رمزارزها در حوزه‌ی هنرهای تجسمی دیجیتال و بازارهای مالی هنر در ایران

مهدی نصیری [۱]

[۱] کارشناس ارشد رشته‌ی تاریخ هنر جهان اسلام، گروه مطالعات عالی هنر، دانشکده‌ی هنرهای تجسمی
دانشکدگان هنرهای زیبا، دانشگاه تهران، ایران
nasiri.mehdi@ut.ac.ir

چکیده

خرید و فروش آثار هنرهای تجسمی دیجیتال بر بستر فناوری‌های نوینی مانند بلاک‌چین و رمزارزها، باعث شده‌است که هنرمندان و علاقه‌مندان به هنر در ایران اسلامی، امکان خلق، انتشار، خرید و فروش آثار خود را به‌صورت دیجیتال بر بستر بلاک‌چین با استفاده از رمزارزها داشته‌باشند. این مقاله به بررسی کاربردها، مزایا و چالش‌های این فناوری‌های نوین در حوزه‌ی هنرهای تجسمی دیجیتال و تأثیر آن بر بازار هنر دیجیتال در کشور می‌پردازد. با توجه به رشد سریع حوزه‌ی بلاک‌چین و NFT در سطح جهانی، این مقاله به‌دنبال پاسخ به این پرسش است که کاربردهای مهم فناوری بلاک‌چین و رمزارزها در حوزه‌ی هنرهای تجسمی دیجیتال چه هستند؟ و شرایط لازم برای ایجاد و راه‌اندازی یک رمز ارز ملی-ایرانی در حوزه‌ی هنرهای تجسمی در داخل کشور بر بستر بلاک‌چین چگونه است؟ بدین‌منظور با استفاده از روش تحقیق توصیفی-تحلیلی، پس از پژوهش و واکاوی در حوزه‌های ذکر شده مشخص گردید که استفاده از فناوری بلاک‌چین و رمزارزها می‌تواند باعث افزایش اعتماد و شفافیت در معاملات هنری، ردیابی منشأ اثر هنری، رهگیری تاریخچه‌ی مالکیت و فروش‌های ثانویه، امنیت خرید و فروش در معاملات هنری، قراردادهای هوشمند، توسعه و رشد بازارهای دیجیتال هنر در ایران شود.

کلمات کلیدی: بلاک‌چین، رمز ارز، NFT، بازار دیجیتال هنر، هنرهای تجسمی دیجیتال.

۱ مقدمه

موضوع این پژوهش بررسی استفاده‌ی هنرمندان از فناوری بلاک‌چین [۱] (زنجیره‌ی بلوکی) و رمزارز [۲]ها در حوزه‌ی هنرهای تجسمی دیجیتال است. با توجه به روند روبه‌رشد هنرهای دیجیتالی، بلاک‌چین و رمز ارزها می‌توانند به‌عنوان یک راهکار مؤثر برای حل مشکلاتی همچون عدم شفافیت در بازارهای جهانی هنرهای

[1] Blockchain
[2] Cryptocurrency

تجسمی دیجیتال، عدم امنیت در تراکنش‌های هنری و جلوگیری از بحث از آن‌خودسازی آثار هنری دیجیتال معرفی شوند. در سال‌های اخیر، افراد و شرکت‌های زیادی در حوزه‌ی هنرهای تجسمی دیجیتال، از بلاک‌چین و ارزهای رمزنگاری‌شده استفاده کرده‌اند تا برای هنرمندان، خریداران آثار هنری، موزه‌ها و گالری‌ها، امنیت و شفافیت بیشتری را فراهم آورد (Smith, 2019: 35). بلاک‌چین، یک فناوری ثبت داده‌ها است که به‌صورت شفاف و بدون واسطه، تمامی تراکنش‌هایی را که در آن انجام‌می‌شود ذخیره می‌کند. این تکنولوژی، به هنرمندان این امکان را می‌دهد که آثار هنری خود را به‌صورت دیجیتالی و با استفاده از بلاک‌چین ثبت و ضبط کنند (Jones، ۲۰۲۰: ۴۲-۴۳). این مزیت، به‌هنرمندان این امکان را می‌دهد که اطمینان حاصل کنند آثار هنری ایشان به‌طور قانونی در سراسر جهان به فروش رفته و از حفظ حقوق مالکیت معنوی آثار خود اطمینان حاصل نمایند (Wilson, 2022: 25-27).

بلاک‌چین یک تکنولوژی نوین است که در ابتدا برای انجام تراکنش‌های مالی و ارزهای دیجیتالی مانند بیت‌کوین[3] استفاده شد. درحالی‌که قبلاً برای انجام تراکنش‌های مالی، نیاز به واسطه‌هایی مانند بانک‌ها یا شرکت‌های پرداخت الکترونیکی بود، اما با ورود بلاک‌چین به بازار، امکان انجام تراکنش‌های مستقیم و بدون واسطه بین دو طرف فراهم شد (Lee, 2018: 20). بلاک‌چین به‌شکل زنجیره‌ای از بلوک‌ها عمل می‌کند که هر بلوک حاوی اطلاعاتی از تراکنش‌های انجام‌شده در یک بازه‌ی زمانی خاص است. هر بلوک شامل اطلاعاتی از بلوک قبلی است و با تأیید کامل تراکنش‌های جدید، به‌زنجیره اضافه می‌شود (Brown, 2021: 15). به‌عنوان نمونه، فرض کنید فرد A به فرد B مبلغی را به‌صورت دیجیتالی انتقال داده است. این تراکنش به‌صورت رمز شده، ذخیره می‌شود و سپس به یک بلوک در بلاک‌چین اضافه می‌شود. بعد از تأیید تراکنش‌های این بلوک توسط کاربرانی که به‌عنوان کاربران «ماینر»[4] شناخته می‌شوند، این بلوک به‌زنجیره‌ی اصلی بلاک‌چین اضافه می‌شود و از این پس، هیچ تغییری در این تراکنش‌ها نمی‌توان ایجاد کرد.

بلاک‌چین به‌دلیل ماهیت غیر متمرکز و شفافیت بالای آن، امکان انجام تراکنش‌های امن و بدون واسطه را فراهم می‌کند. همچنین، بلاک‌چین به‌عنوان یک راهکار مفید برای ذخیره‌سازی داده‌های حساس و اطلاعات فردی به کار گرفته‌می‌شود. به‌عنوان نمونه، بلاک‌چین می‌تواند در حوزه‌ی هنر برای ذخیره‌سازی اطلاعات آثار هنرهای تجسمی دیجیتال و ارائه‌ی گواهی‌های امنیتی برای اصالت آنها مورد استفاده قرار گیرد. در هنرهای تجسمی دیجیتال، بلاک‌چین می‌تواند به‌عنوان یکی از راه‌حل‌ها برای حفظ حقوق مالکیت معنوی و کپی‌رایت، پرداخت آنلاین به‌هنرمندان و تأمین امنیت تراکنش‌های مالی مورد استفاده قرار گیرد.

با توجه به مطالب مرقوم شده، هدف اصلی پژوهش حاضر ارائه‌ی دیدگاه‌هایی درباره‌ی نحوه‌ی استفاده از بلاک‌چین و رمز ارزها برای ایجاد تغییرات بنیادین در بازار هنرهای تجسمی سنتی در ایران است. همچنین، در این جستار بررسی می‌شود که بلاک‌چین و رمز ارزها چگونه می‌توانند تعادل قدرت در بازار هنرهای تجسمی دیجیتال در ایران را تغییر دهند. همچنین جستار پیش‌رو فرصت‌ها و امکانات مربوط به استفاده از NFTها را در بازارهای هنری ایران بررسی می‌نماید و به بررسی امکانات رمز ارز ملی-ایرانی می‌پردازد.

حوزه‌ی هنرهای تجسمی دیجیتال در سال‌های اخیر رشد چشمگیری داشته است. اما همچنان

[3] Bitcoin
[4] Miner

چالش‌هایی در زمینه‌ی حفظ حقوق مالکیت معنوی هنرمندان، شفافیت در معاملات و امنیت آثار هنری دیجیتال وجود دارد. از سوی دیگر، ظهور فناوری‌های نوینی همچون بلاک‌چین و رمز ارزها فرصت‌های جدیدی را برای حل این چالش‌ها فراهم کرده‌است. بر اساس تحقیقات و کاربردهای اولیه، به نظر می‌رسد بلاک‌چین و رمز ارزها پتانسیل لازم برای افزایش شفافیت، امنیت و سهولت معاملات در حوزه‌ی هنرهای دیجیتال را داشته‌باشند. از این رو، ضرورت دارد تا کاربردها و پتانسیل این فناوری‌ها به‌طور دقیق‌تری در حوزه‌ی هنرهای تجسمی دیجیتال ایران اسلامی مورد بررسی و ارزیابی قرار گیرد تا از این منظر بتوان از مزایای آن برای رفع چالش‌های موجود اقدام نمود.

۲ پیشینه‌ی پژوهش

بر بنیان مطالب نوشته‌شده، پیشینه‌ی پژوهش پیش‌رو به دو بخش تقسیم می‌شود. بخش اول منابع مرتبط با زیرساخت‌های فنی حوزه‌ی رمز ارزها و بلاک‌چین می‌باشد و در بخش دوم، حوزه‌ی NFTها و توکن‌های غیر قابل تعویض و هنرهای تجسمی بر بستر بلاک‌چین و رمز ارزها مورد مطالعه و پژوهش قرار گرفته‌اند.

در بخش اول (زیرساخت‌های فنی رمز ارزها و بلاک‌چین)، کتاب «مبانی حوزه‌ی بیت‌کوین و بلاک‌چین: مقدمه‌ای بر ارزهای دیجیتال و تکنولوژی‌های پشتیبان آنها[۵]» نوشته‌ی آنتونی لوئیس[۶] به چاپ رسیده‌است. این کتاب به معرفی بیت‌کوین، بلاک‌چین و سایر ارزهای دیجیتال می‌پردازد. در این کتاب، نویسنده به تاریخچه‌ی بیت‌کوین، بلاک‌چین و روش‌های خرید، فروش و استخراج بیت‌کوین می‌پردازد. نویسنده همچنین به مباحثی در حوزه‌ی رمزنگاری، معاملات آنلاین و تکنولوژی بلاک‌چین می‌پردازد (Lewis, 2018).

کتاب (مبانی بلاک‌چین: مقدمه‌ای غیر فنی در ۲۵ مرحله[۷]) نوشته‌ی دنیل در شر[۸]، به زبان ساده و بدون استفاده از فرمول‌های ریاضی، کدهای برنامه‌نویسی و اصطلاحات فنی کامپیوتری، مفاهیم پایه‌ی بلاک‌چین را به‌خواننده آموزش می‌دهد. این کتاب به دو بخش تقسیم شده‌است: بخش اول به معرفی مفاهیم پایه‌ی بلاک‌چین و بخش دوم به‌تبیین کاربردهای بلاک‌چین در صنعت و تجارت می‌پردازد (Drescher, 2017).

در بخش دوم (NFTها و توکن‌های غیر قابل تعویض)، به بررسی کتاب «تفکرات جدید هنرمندان درباره‌ی بلاک‌چین[۹]» پرداخته می‌شود. روث‌کتلو[۱۰] و همکاران در این کتاب به هم‌پوشانی هنر با فناوری بلاک‌چین پرداخته‌اند. این جستار شامل مجموعه‌ای از مقالات و تصاویر هنری است که چشم‌اندازهای مختلف هنرمندان را در مورد اینکه بلاک‌چین برای آینده‌ی جمعی هنرمندان چه معنایی باید داشته‌باشد، منعکس می‌کند (Catlow et al., 2017).

---

[5] The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them.
[6] Antony Lewis
[7] Blockchain Basics: A Non-Technical Introduction in 25 Steps
[8] Daniel Drescher
[9] Artists Rethinking the Blockchain
[10] Ruth Catlow

کتاب «راهنمای NFT: نحوه‌ی ایجاد، فروش و خرید توکن‌های غیرقابل تعویض[۱۱]» به قلم مت فورتنو[۱۲] و کوهریسون تری[۱۳] نوشته‌شده است. در این کتاب، نویسندگان به شرح زمینه‌های مرتبط با NFT یا توکن‌های غیرقابل تعویض می‌پردازند و روش‌های ساخت و توسعه‌ی آنها را برای کاربران توضیح می‌دهند. کتاب شامل مواردی مانند تاریخچه‌ی NFT، کاربردهای آن، فناوری بلاک‌چین و قراردادهای هوشمند، استانداردها و طراحی NFT، بازار توکن‌ها و مسائل حقوقی و مالی مرتبط با آنها می‌شود. این کتاب به‌عنوان یک راهنمای جامع برای کسانی که قصد دارند در این حوزه فعالیت کنند، مناسب است (Fortnow & Terry, 2021).

کالین بریز[۱۴] کتابی با عنوان «توکن‌های غیرقابل تعویض و سرمایه‌گذاری در هنر برای شروع و رشد: راهنمای کامل برای توکن‌های غیرقابل تعویض و دارایی‌های دیجیتال[۱۵]» به رشته‌ی تحریر در آورده‌است. این کتاب به‌عنوان یک راهنمای جامع برای کسانی که در حوزه‌ی توکن‌های غیرقابل تعویض (NFT) و سرمایه‌گذاری در هنر دیجیتال فعالیت می‌کنند، مناسب است. در این کتاب، نویسنده به شرح زمینه‌های مرتبط با NFT و هنر دیجیتال می‌پردازد و راهنمایی‌هایی برای سرمایه‌گذاری در این حوزه ارائه می‌دهد. در این کتاب، مفاهیمی مانند تعریف توکن‌های غیرقابل معامله، تاریخچه‌ی آنها و نحوه‌ی کارکرد در بازار هنرهای دیجیتال بررسی می‌شود. همچنین، در این کتاب به بررسی فناوری بلاک‌چین و نحوه‌ی استفاده از آن در بازار هنر دیجیتال پرداخته می‌شود. نویسنده در این کتاب به بررسی مسائل حقوقی، مالی و امنیتی مرتبط با سرمایه‌گذاری در هنر دیجیتال و توکن‌های غیرقابل معامله می‌پردازد (Breeze, 2022).

مارک بکمن[۱۶]، نویسنده‌ی کتاب «راهنمای جامع توکن‌های غیر قابل تعویض، هنرهای دیجیتال و فناوری بلاک‌چین[۱۷]» است. این کتاب به‌عنوان یک راهنمای جامع برای کسانی که در حوزه‌ی هنرهای دیجیتال و فناوری بلاک‌چین فعالیت می‌کنند، مناسب است. در این کتاب، نویسنده به شرح زمینه‌های مرتبط با هنر دیجیتال و فناوری بلاک‌چین می‌پردازد و راهنمایی‌هایی برای کار با هنر دیجیتال و بلاک‌چین ارائه می‌دهد. در این کتاب به بررسی مواردی مانند نحوه‌ی ارزیابی اثر هنری دیجیتال، تولید و فروش هنر دیجیتال، کار با بازار هنر دیجیتال و نحوه‌ی استفاده از تکنولوژی بلاک‌چین در این حوزه پرداخته می‌شود (Beckman, 2021).

با توجه به بررسی کتب و پژوهش‌های انجام‌شده، منابع فنی در خصوص فناوری بلاک‌چین و رمز ارزها به زبان انگلیسی در دسترس پژوهش قرار دارد؛ اما تاکنون پژوهشی در زمینه‌ی کاربرد این فناوری‌ها در حوزه‌ی هنرهای تجسمی در داخل کشور صورت نگرفته‌است. مطالعات منابع موجود، زیرساخت‌های فنی لازم برای انجام این پژوهش و بومی‌سازی این فناوری‌ها را فراهم می‌نمایند. بنابراین پژوهش حاضر، نخستین تلاش برای بررسی کاربرد فناوری‌های نوین بلاک‌چین و رمز ارز در عرصه‌ی هنرهای تجسمی داخل کشور به‌شمار

[11] The NFT Handbook: How to Create, Sell and Buy Non-Fungible Tokens
[12] Matt Fortnow
[13] QuHarrison Terry
[14] Colin Breeze
[15] Non-Fungible Tokens and Art Investing for Beginners and Advance: The Ultimate Guide to NFTs and Digital Assets
[16] Marc Beckman
[17] The Comprehensive Guide to NFTs, Digital Artwork, and Blockchain Technology

می‌رود.

۳ روش تحقیق

به‌کارگیری فناوری بلاک‌چین در هنرهای تجسمی یک پدیده‌ی جدید و روبه‌رشد است. این موضوع باعث می‌شود که بررسی این فناوری در کاربردهای هنری و تأثیرات آن برای متخصصان، هنرمندان و علاقه‌مندان به هنرهای تجسمی در ایران اسلامی اهمیت بیشتری پیدا کند. با پیشرفت‌های روزافزون در حوزه‌ی بلاک‌چین و هنر، نیاز به‌تحقیق بیشتر در این زمینه کاملاً احساس می‌شود. این مقاله از نوع مطالعات بینا رشته‌ای بوده و از منابع دست‌اول در حوزه‌های مبانی نظری و فنی بلاک‌چین و رمز ارزها، کاربردهای فناوری بلاک‌چین و رمز ارز در هنرهای تجسمی و ارتباط آن با توسعه‌ی هنر و بازارهای سنتی هنر در ایران اسلامی بهره می‌برد.

پژوهش حاضر از منظر هدف کاربردی است و نتایج حاصل از آن می‌تواند در اختیار مراکز پژوهشی، دانشگاه‌ها، حراجی‌های ملی و بین‌المللی، دولت‌ها، نمایندگان مجلس و عموم علاقه‌مندان به‌حوزه‌ی هنرهای تجسمی، خریدوفروش آثار هنری دیجیتال، فناوری بلاک‌چین و تبیین و پیاده‌سازی قوانین مرتبط با بلاک‌چین و رمز ارزها قرار گیرد. شیوه‌ی مورداستفاده در جمع‌آوری منابع موردنیاز پژوهش حاضر از نوع مطالعات کتابخانه‌ای و اسنادی است. تجزیه‌وتحلیل اطلاعات گردآوری‌شده به‌صورت تفسیری- تحلیلی مورد واکاوی و مداقه قرار گرفته و روش تحقیق مورداستفاده در این پژوهش از نوع توصیفی-تحلیلی می‌باشد.

با توجه به رشد روزافزون استفاده از فناوری بلاک‌چین و رمز ارزها در عرصه‌ی هنرهای تجسمی دیجیتالی، بنیان اصلی جستار پیش رو، بررسی جامع کاربردها، فرصت‌ها و چالش‌های به‌کارگیری این فناوری‌ها در حوزه‌ی هنرهای تجسمی دیجیتال در ایران اسلامی است. این پژوهش با رویکردی بینا رشته‌ای، به‌دنبال شناسایی قابلیت‌های بالقوه بلاک‌چین و رمز ارزها در ایجاد تحول و نوآوری در زمینه‌هایی همچون اثبات مالکیت معنوی، افزایش شفافیت معاملات و تسهیل دسترسی به بازارهای جهانی هنر برای هنرمندان ایرانی است.

۴ بلاک‌چین و رمزارز در حوزه‌ی هنرهای تجسمی

بلاک‌چین، به‌عنوان یک فناوری نوین، در حال حاضر در حوزه‌ی هنرهای تجسمی کاربردهای متعددی دارد. این فناوری، با امکاناتی مانند امنیت، شفافیت و عدم تغییرپذیری، می‌تواند به رسیدن به هدف‌های مختلف در این حوزه کمک‌های شایانی نماید. بلاک‌چین در حوزه‌ی هنر، از سال ۲۰۱۴ م. شروع به کار کرده‌است. اولین پروژه‌های مرتبط با بلاک‌چین، در زمینه‌ی نگهداری و ثبت اثر هنری بود. با استفاده از بلاک‌چین، اثر هنری به‌صورت دیجیتال ثبت و نگهداری می‌شود و همچنین تغییرات و تحولات آن نیز قابل رصد است (Whitaker, 2019: 22).

استفاده از بلاک‌چین و رمز ارزها در دنیای هنرهای تجسمی دیجیتال در سال‌های اخیر رشد قابل‌توجهی داشته‌اند. مطالعات و تحقیقات مختلفی به بررسی مزایا و چالش‌های بالقوه و مرتبط با این فناوری‌های نوین در حوزه‌ی هنرهای دیجیتالی پرداخته‌اند. برخی از مطالعات بر پایه‌ی مزایای استفاده از بلاک‌چین و رمز

ارزها در ردیابی منشأ آثار هنری، ایجاد گواهی اصالت و جلوگیری از جعل آثار هنری متمرکز بوده‌اند. علاوه بر این، استفاده از ارزهای رمزنگاری‌شده، به‌ویژه توکن‌های غیرقابل تعویض (NFT)ها، به‌عنوان ابزاری برای نمایش و خرید و فروش آثار هنری دیجیتال محبوبیت زیادی پیدا کرده‌اند (Cassidy, 2021: 23).

فناوری بلاک‌چین و رمز ارزها به‌عنوان یک نظام دیجیتالی جدید می‌توانند کاربردهای فراوانی داشته‌باشند. فناوری بلاک‌چین و رمز ارزها قادر هستند تعادل قدرت اقتصادی را در بسیاری از حوزه‌ها و هنرها تغییر دهند. این فناوری‌ها می‌توانند تبدیل به یک پلتفرم قابل‌مقایسه با اینترنت شده و جریان اطلاعات را پشتیبانی نمایند. سرفصل‌های درج‌شده، بخشی از مهم‌ترین دلایل استفاده از فناوری بلاک‌چین و رمز ارزها در حوزه‌ی هنرهای تجسمی دیجیتال در ایران می‌باشند:

- **ردیابی منشأ:** فناوری بلاک‌چین سوابق شفاف و تغییرناپذیر منشأ یک اثر هنری را ثبت و ضبط می‌نماید باعث ایجاد شفافیت و اعتماد درباره‌ی خلق اثر هنری و هنرمند آن اثر می‌شود.
- **ایجاد اصالت:** فناوری بلاک‌چین می‌تواند یک گواهی دیجیتالی اصالت اثر هنری ایجاد نموده و از اصالت آثار هنری دیجیتال اطمینان حاصل نماید و این کار باعث کاهش خطر جعل آثار هنری می‌شود.
- **امنیت در معاملات هنری:** ارزهای دیجیتال روش‌های پرداخت امن و کارآمدی را ارائه نموده و نیاز به‌واسطه‌ها را از بین برده و خطر تقلب را کاهش می‌دهند.
- **شفافیت:** استفاده از بستر بلاک‌چین می‌تواند منجر به افزایش امنیت و شفافیت در بازارهای هنر دیجیتال شده و نگرانی‌های مربوط به اصالت و مالکیت را برطرف کند.
- **قراردادهای هوشمند:** تهیه، تولید و پیگیری قراردادهای هوشمند با پرداخت خودکار هزینه‌ها توسط خریداران به هنرمندان پس از پایان قرار داد.
- **توسعه و رشد بازارهای هنری:** درک پتانسیل‌های حوزه‌ی بلاک‌چین و ارزهای دیجیتال در هنرهای تجسمی می‌تواند به رشد و توسعه بازارهای سنتی کمک نموده و هنرمندان و مجموعه‌داران بیشتری را جذب نماید.
- **توانمندسازی هنرمندان:** از طریق فناوری بلاک‌چین، هنرمندان می‌توانند کنترل بیشتری بر آثار هنری دیجیتال خود داشته‌باشند، از حقوق خود اطمینان حاصل نموده و سود مدت‌دار و عادلانه دریافت نمایند.

در نتیجه، استفاده از بلاک‌چین و ارزهای دیجیتال در زمینه‌ی هنرهای تجسمی دیجیتال فرصت‌ها و امکانات قابل‌توجهی را به هنرمندان ایرانی ارائه می‌دهد. تحقیقات بیشتر در این زمینه برای استفاده از مزایا، غلبه بر محدودیت‌ها و درنهایت ایجاد یک اکوسیستم پرداخت ایمن در حوزه‌ی هنرهای دیجیتال در جمهوری اسلامی ایران بسیار مهم است.

۵ توکن غیرقابل معاوضه (NFT)

هر توکن NFT، دارای یک شناسه منحصربه‌فرد است که به هنرمند اجازه می‌دهد تا اصالت و مالکیت خود را در قبال آن اثبات کند. یکی از مزایای استفاده از تکنولوژی بلاک‌چین در بازارهای هنری، دسترسی به بازار بین‌المللی برای هنرمندان است. با استفاده از تکنولوژی بلاک‌چین و NFT خریداران می‌توانند به‌صورت مستقیم با هنرمند در ارتباط باشند و اثر هنری را خریداری نمایند؛ بدون نیاز به واسطه‌گری‌های رایج سنتی در بازارهای هنری. همچنین، این روش می‌تواند به هنرمندان اجازه دهد که به‌صورت مستقیم با خریداران خود در ارتباط باشند و ارزش آثار خود را بدون واسطه‌گری افزایش دهند. استفاده از تکنولوژی بلاک‌چین و NFT در بازار هنر باعث بالا رفتن شفافیت در این بازار می‌شود (Schwab، ۲۰۱۶: ۲۹). در ارتباط با اهمیت استفاده از توکن‌های غیرقابل تعویض (NFT) در حوزه‌ی هنرهای تجسمی دیجیتال به‌موارد زیر می‌توان اشاره داشت:

- **مالکیت دیجیتال منحصربه‌فرد NFTها:** NFTها به هنرمندان اجازه می‌دهند تا آثار هنری دیجیتال خود را به‌صورت توکن درآورده و نمایشی منحصربه‌فرد از مالکیت و منشأ این آثار هنری ارائه دهند.
- **فرصت‌های کسب درآمد از NFTها:** NFTها، هنرمندان را قادر می‌سازند تا آثار دیجیتالی خود را مستقیماً به مجموعه‌داران بفروشند و جریان‌های درآمد جدیدی را ایجاد نمایند.
- **حفاظت از مالکیت معنوی:** NFTها می‌توانند حقوق مالکیت معنوی و حق امتیاز آثار را مستقیماً در آثار هنری دیجیتال درج نموده و تضمین نمایند که هنرمندان برای فروش‌های بعدی نیز سود دریافت نمایند.

۶ هنرمندان ایرانی، بلاک‌چین و رمزارزها

یکی از کاربردهای اصلی بلاک‌چین در هنرهای تجسمی دیجیتال، ثبت اثر و ایجاد اثر انحصاری است. با استفاده از تکنولوژی بلاک‌چین، هنرمندان ایرانی می‌توانند آثار هنری خود را در قالب یک عنوان یا شماره توکن بر روی بلاک‌چین ثبت نمایند. این کار باعث ایجاد یک رکورد امن و قابل تحقیق برای اثر می‌شود که نشان‌می‌دهد چه کسی این اثر را خلق کرده و به چه کسی تعلق دارد. این قابلیت می‌تواند در حفظ حقوق مالکیت هنرمندان ایرانی و جلوگیری از سوء استفاده‌های غیرمجاز بر روی آثار هنری ایشان در بازارهای بین‌المللی، تأثیرگذار باشد.

بلاک‌چین می‌تواند باعث شفافیت و امنیت در تراکنش‌های مالی هنرمندان ایرانی در بازارهای جهانی هنرهای دیجیتالی شود. یکی از مزیت‌های بلاک‌چین در این زمینه، ایجاد یک سیستم ثبت و تائید تراکنش‌ها است که قابل‌رؤیت و شفاف است. با استفاده از بلاک‌چین، تمام تراکنش‌ها در قالب بلوک‌های متوالی و بر اساس الگوریتم‌های رمزنگاری ثبت می‌شوند و هیچ تغییری در آن‌ها اعمال نمی‌شود. این امر منجر به

اطمینان از صحت و اعتبار تراکنش‌ها و جلوگیری از تقلب و تغییرات غیرمجاز می‌شود. همچنین، بلاک‌چین امنیت بالایی در برابر هک و دسترسی غیرمجاز فراهم می‌کند. اطلاعات تراکنش‌ها در بلاک‌چین به‌صورت رمزنگاری‌شده و در سراسر شبکه توزیع می‌شوند، به‌طوری‌که هرگونه تغییر در بلوک‌ها بلافاصله توسط سایر شرکت‌کنندگان تشخیص داده‌می‌شود. این موضوع منجر به اعتماد بیشتر و امنیت بیشتر در تراکنش‌های مالی هنرمندان ایرانی در بازارهای جهانی هنرهای دیجیتال می‌شود.

بلاک‌چین به‌عنوان یک فناوری قابل‌اعتماد و شفاف می‌تواند در حفظ حقوق مالکیت معنوی آثار هنری دیجیتال هنرمندان ایرانی کمک کند. با استفاده از قابلیت‌های بلاک‌چین، اطلاعات مربوط به‌مالکیت آثار هنری به‌صورت دیجیتالی ثبت و ذخیره می‌شوند و امکان تقلب و تغییر در آنها کاهش می‌یابد. به‌علاوه، تمامی تراکنش‌ها و تغییراتی که روی آثار صورت‌می‌گیرد، به‌صورت دائمی در بلاک‌چین ثبت می‌شود و قابل دست‌کاری نمی‌باشد. به‌عنوان‌مثال، فرض کنید یک هنرمند حوزه‌ی هنرهای دیجیتالی، آثار خود را در یک پلتفرم هنری آپلود می‌کند؛ با استفاده از بلاک‌چین، اطلاعات مربوط به‌مالکیت هر اثر به‌صورت دیجیتالی ثبت شده و در بلاک‌چین ذخیره می‌شود.

قراردادهای هوشمند بر بستر بلاک‌چین می‌توانند به خودکارسازی بخش‌هایی از بازارهای هنری کمک نمایند. قراردادهای هوشمند، قراردادهای خود اجرایی هستند که می‌توانند فرایندهایی مانند پرداخت‌ها در هنگام فروش یک اثر هنری را خودکار نمایند. این سیستم می‌تواند باعث افزایش کارایی در بازارهای هنر دیجیتال در ایران شود. قراردادهای هوشمند می‌توانند به‌طور خودکار حق امتیاز را به هنرمندان ایرانی پرداخت نمایند. در صورتی که آثار هنری دیجیتال هنرمندان دوباره فروخته شود، این امکان وجود دارد تا هنرمند از فروش اثر هنری خود مطلع شده و در فروش ثانویه اثر نیز سهیم باشد.

بلاک‌چین می‌تواند هنرمندان ایرانی را قادر سازد تا از طریق کمپین‌های سرمایه‌گذاری جمعی ارزهای دیجیتال[۱۸] برای پروژه‌های هنری خود، سرمایه جمع‌آوری کنند. این مقوله به هنرمندان امکان دسترسی به سرمایه و منابع مالی بیشتری را می‌دهد. پرداخت‌های خرد ارزهای دیجیتال[۱۹] می‌تواند به هنرمندان ایرانی اجازه دهد تا آثار هنری دیجیتال خود را با قیمت‌های پایین و در تعداد بالا به فروش برسانند. پرداخته‌ای خرد با ارزهای دیجیتال امکان‌پذیر است. حراج‌های هنری می‌توانند به‌صورت آنلاین آثار هنرمندان ایرانی را به فروش برسانند و موانع موجود در قالب‌های حراج سنتی را دور بزنند.

بلاک‌چین می‌تواند به‌عنوان یک راه‌حل مؤثر برای حل مشکلات تقلب و جعل در حوزه‌ی هنرهای تجسمی دیجیتال در ایران عمل کرده و اصالت آثار هنری دیجیتال را تائید نماید. با استفاده از بلاک‌چین، اطلاعات مربوط به آثار هنری دیجیتال به‌صورت رمزنگاری‌شده در شبکه‌ی بلاک‌چین ثبت شده و تغییر یا جعل در آنها تقریباً غیرممکن می‌شود. به‌عنوان‌مثال، فرض کنید یک هنرمند ایرانی یک اثر هنری دیجیتال ایجاد کرده و آن را در یکی از بازار جهانی هنرهای دیجیتال به فروش می‌رساند. با استفاده از بلاک‌چین، اطلاعات مربوط به این اثر هنری به‌صورت یک رکورد منحصربه‌فرد در بلاک‌چین ثبت می‌شود. این رکورد شامل اطلاعاتی مانند نام هنرمند، تاریخ ایجاد آثار هنری، توصیف آثار و اطلاعات دیگر است. اگر فرد دیگری قصد جعل یا تغییر در

[18] Digital Currency Crowdfunding Campaigns
[19] Digital Micropayments

آن اثر هنری را داشته‌باشد، باید تمامی تراکنش‌های قبلی را نیز تغییر دهد که عملاً غیرممکن است.

بنابراین، اصالت آثار هنری هنرمندان ایرانی توسط بلاک‌چین تأیید می‌شود و هنرمندان و خریداران می‌توانند با اطمینان کامل به تراکنش‌های صورت گرفته و اصالت آثار هنری اعتماد نمایند. استفاده از بلاک‌چین در حوزه‌ی هنرهای تجسمی دیجیتال به‌معنای ایجاد یک نظام شفاف و قابل‌اعتماد است که باعث کاهش تقلب و جعل آثار می‌شود و به هنرمندان و خریداران امکان می‌دهد تا با اطمینان کامل در بازار هنرهای تجسمی دیجیتالی فعالیت نمایند.

۷ رمز ارز ملی-ایرانی

رمز ارز «ملی-ایرانی» بر بستر فناوری بلاک‌چین می‌تواند به‌کمک هنرمندان ایرانی در بازارهای مالی جهانی بیاید. استفاده از بلاک‌چین و رمز ارزها امکاناتی را فراهم می‌کنند که هنرمندان ایرانی آثار خود را به‌صورت دیجیتالی ثبت و به فروش برسانند. این امر می‌تواند به هنرمندان ایرانی در ورود به بازارهای مالی جهانی و فروش آثارشان در سراسر جهان کمک‌های شایانی نماید. با استفاده از فناوری بلاک‌چین، اطلاعات مربوط به اثر هنری می‌توانند به‌صورت شفاف و بدون واسطه در شبکه بلاک‌چین ثبت‌شده و از بحث «از آن خودسازی آثار هنری» توسط دیگران جلوگیری شود.

این فناوری‌ها می‌توانند به هنرمندان ایرانی امکانات بیشتری در بازارهای جهانی هنر دیجیتال بخشیده و مالکیت معنوی آثارشان را تضمین نمایند. همچنین، رمز ارز ملی-ایرانی بر بستر بلاک‌چین می‌تواند به‌عنوان یک وسیله‌ی مالی برای خرید و فروش آثار هنری ایرانی استفاده شود. این رمز ارز می‌تواند به هنرمندان ایرانی امکان بدهد تا با خریداران جهانی به‌صورت مستقیم و بدون واسطه تعامل نموده و تراکنش‌هایشان را به‌صورت امن و شفاف انجام دهند. بنابراین، استفاده از رمز ارز ملی-ایرانی بر بستر فناوری بلاک‌چین می‌تواند به هنرمندان ایرانی در بازارهای مالی جهانی کمک کرده و امکانات جدیدی را برای آنها فراهم سازد.

اخیراً مفادی درباره‌ی طرح ایجاد رمز ارز ملی-ایرانی بر بستر فناوری بلاک‌چین منتشرشده است. این طرح جزئی از سیاست‌های دولت جمهوری اسلامی ایران برای عبور از تحریم‌ها و جلوگیری از فشارهای اقتصادی بر کشور است. بااین‌حال، موفقیت یا شکست این طرح به عوامل متعددی بستگی دارد که از جمله آنها می‌توان به توانایی تضمین امنیت و اعتماد در بستر بلاک‌چین، توانایی جذب سرمایه‌گذاری، توانایی تعامل با سایر رمز ارزها و ارزهای قابل‌تبدیل جهانی و توانایی تضمین پایداری ارزش رمز ارز ملی اشاره نمود.

با توجه به این موارد، هنرمندان ایرانی نیز می‌توانند نقش مهمی در معرفی و تبلیغ این رمز ارز داشته‌باشند. هنرمندان ایرانی معمولاً دارای شناخت بین‌المللی و طرفداران بسیاری هستند و این امر می‌تواند به‌عنوان یک فرصت برای تبلیغ رمز ارز ملی-ایرانی در بازارهای جهانی مطرح شود. همچنین، هنرمندان ایرانی می‌توانند به‌عنوان سفیران فرهنگی کشور در بازارهای جهانی عمل کرده و اعتبار و اعتماد به برند ملی ایران اسلامی را افزایش دهند که این امر نیز می‌تواند به روند موفقیت طرح رمز ارز ملی-ایرانی کمک نماید.

۸ نتیجه‌گیری

فناوری‌های نوین مانند بلاک‌چین و رمز ارزها باعث تغییر بازارهای سنتی هنرهای تجسمی در ایران و جهان شده‌اند و موجب تحول و گسترش این بازارها گشته‌اند. در سال‌های اخیر، حوزه‌ی هنرهای تجسمی دیجیتال و بازارهای مالی هنر در ایران نیز به بررسی کاربردهای این فناوری‌های نوین متمایل شده‌اند. حوزه‌ی هنرهای تجسمی در داخل کشور با چالش‌های مربوط به شفافیت، اصالت، مالکیت و ارزش‌گذاری آثار هنری دیجیتال مواجه است. فناوری بلاک‌چین و ارزهای دیجیتال پتانسیل مقابله با این چالش‌ها و ارائه‌ی راه‌حل‌های ایمن و کارآمد را دارند.

با استفاده از فناوری بلاک‌چین و رمز ارزها، حوزه‌ی هنرهای تجسمی دیجیتال و بازارهای مالی هنر در ایران می‌توانند شاهد رشد و توسعه‌ی بی‌سابقه‌ای باشند. مزایای ترکیب این فناوری‌ها را نمی‌توان نادیده گرفت زیرا راه‌حل‌های نوآورانه‌ای را ارائه می‌دهند که مدت‌ها است که این بخش‌ها را درگیر کرده‌است. با ایجاد تأیید منشأ و اصالت اثر، خودکارسازی مجوزها و حق امتیازها از طریق استفاده از فناوری بلاک‌چین، می‌توان به‌طور مؤثر به مسائل مربوط به جلوگیری از تقلب در آثار هنری پرداخت. نتایج این پژوهش نشان می‌دهند که فناوری بلاک‌چین می‌تواند سرعت، شفافیت و حجم فروش آثار هنری در ایران و سراسر جهان را افزایش داده و به بالا بردن قدرت و شفافیت این حوزه کمک‌های ارزشمندی داشته تا هنرمندان ایرانی، مجموعه‌داران و خریداران از توانایی‌های این فناوری‌ها بهره‌مند شوند. یک پلتفرم بلاک‌چین می‌تواند در کنار سایر بازارهای سنتی هنر وجود داشته‌باشد، اما قبل از پیاده‌سازی این فناوری، لازم است موانع فنی، حاکمیتی، قانونی، سیاسی و اجتماعی این حوزه را در کشور برطرف نماییم.

تحقیقات بیشتر در حوزه‌ی بلاک‌چین و رمز ارزها می‌تواند به بهبود امنیت و شفافیت در بازار هنر دیجیتال کشور منجر شود و نگرانی‌های مربوط به اصالت و مالکیت را برطرف نماید. علاوه بر این، بررسی پتانسیل‌های حوزه‌ی بلاک‌چین و رمز ارزها در هنر دیجیتال می‌توانند به رشد و توسعه‌ی بازارهای هنری در ایران اسلامی کمک نموده و هنرمندان و مجموعه‌های ایرانی و بین‌المللی را به خود جذب نمایند. از طریق فناوری بلاک‌چین، هنرمندان قادر خواهند بود بیشترین کنترل را بر روی اثرهای دیجیتالی خود داشته، حقوق خود را تضمین نموده و سود منصفانه‌ای را دریافت نمایند. علاوه بر مزایای ذکرشده، درک دقیق‌تر از چالش‌ها و محدودیت‌های مرتبط با استفاده از بلاک‌چین در بازار هنرهای تجسمی دیجیتال ایران اسلامی ضروری است. بررسی این چالش‌ها سبب دانش‌افزایی و نوآوری در حوزه‌های اجرا و پیاده‌سازی فناوری بلاک‌چین و رمز ارز ملی-ایرانی در حوزه‌ی هنرهای تجسمی دیجیتال در کشور شده و مشکلات فنی مرتبط و ملاحظات قانونی و نظارتی مرتبط با فناوری‌های نوین مانند بلاک‌چین موردپژوهش و مداقه قرار می‌گیرند.

بنابراین، تحقیقات بیشتر در حوزه‌های ذکر شده می‌تواند به توسعه و پیاده‌سازی یک سیستم بدیع بازار دیجیتال هنری بر بستر بلاک‌چین در هنرهای تجسمی ایران اسلامی بینجامد. این تحقیقات به سیاست‌مداران، قانون‌گذاران، هنرمندان، مجموعه‌ها، خریداران و سایر نهادهای مرتبط در فضای هنر دیجیتال کشور این امکان را می‌دهد تا به‌طور علمی و کاربردی از امنیت و اصالت بستر بازارهای مالی در حوزه‌ی بلاک‌چین اطمینان حاصل نمایند. درنهایت، این پژوهش به برنامه‌ریزان و تصمیم‌گیران، نمایندگان مجلس

و دولت‌مردان در حوزه‌ی بازارهای مالی، سیاست‌های کلان کشور، فرهنگ و هنر، فرصتی منحصربه‌فرد را ارائه می‌دهد تا به‌عنوان متصدیان ذی‌نفع در توسعه‌ی استفاده از بلاک‌چین و رمز ارزها در زمینه‌ی هنرهای دیجیتال کشور، مبانی نظری و اجرایی لازم را برای تحقق این اهداف تبیین و پیاده‌سازی نمایند. همچنین، نتایج این جستار می‌تواند به‌شکل سیاست‌های کلان کشوری و الگوهای جدید در بازار هنرهای تجسمی دیجیتال ایران اسلامی در نظر گرفته شود و به‌نوبه‌ی خود به رشد حوزه‌ی هنرهای تجسمی دیجیتال و سنتی و تبدیل آن به یک بخش روبه‌رشد در حوزه‌ی فرهنگ و هنر در کشور منجر شود.

مراجع

[۱] شهرام‌نیا، سیدامیر مسعود و همکاران، واکاوی مفهومی قدرت نرم و راهکار (فرصت)های ایران در قبال آن، مجله دانش سیاسی و بین‌المللی، شماره سوم، ۱۳۹۱، صص ۷۱-۸۸.

[۲] کاتوزیان، ناصر، کلیات حقوق: نظریه عمومی، تهران: شرکت سهامی انتشار، چاپ دوم، ۱۳۷۹.

[۳] نواح، عبدالرضا و همکاران، پیامدهای جامعه‌شناختی سواد رسانه‌ای بر آگاهی از حقوق شهروندی و دموکراسی خواهی، فصلنامه مطالعات رسانه‌های نوین، سال پنجم، شماره هشتم، ۱۳۹۸، صص۲۰۳-۲۲۸.

[۴] رشوند، علی‌اکبر، مقایسه عوامل موثر بر حساسیت افکار عمومی نسبت به مسائل اجتماعی در مناطق شهری و روستایی استان قزوین، پایان‌نامه کارشناسی ارشد، دانشگاه قزوین: گروه علوم اجتماعی، ۱۳۸۰.

[۵] لازار، ژودیت، ۱۳۸۰، افکار عمومی، ترجمه مرتضی کتبی، تهران: نشر نی، ۱۳۸۰.

[۶] حسینی، محمدرضا، الگوی مقررات‌گذاری در فضای سایبر: ارائه چارچوب جامع تنظیم‌گری برای محیط ملی، فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ۱۴۰۲.

[۷] عراقی، مهدی، اهمیت و کارکردها؛ بررسی و شناخت افکار عمومی، تهران: انتشارات فجر، ۱۳۸۳.

[۸] سهراب زاده، عباس، تاثیر رسانه‌های نوین بر ساخت قدرت سیاسی در ایران دهه‌ی هشتاد خورشیدی، رساله دکترای تخصصی، دانشگاه علامه طباطبایی، ۱۳۹۳.

[۹] نقیب‌زاده، احمد، درآمدی بر جامعه‌شناسی سیاسی، تهران: سمت، چاپ هفتم، ۱۳۸۸.

[۱۰] طلوع، ذکیه، تاثیر شبکه‌های اجتماعی بر خط بر دیپلماسی عمومی و بازتاب آن در سیاست مطالعه‌ی موردی ایالت متحده آمریکا، پایان‌نامه کارشناسی ارشد، دانشگاه اصفهان: گروه روابط بین‌الملل، ۱۳۹۲.

[11] Beckman, M. (2021). The Comprehensive Guide to NFTs, Digital Artwork, and The Blockchain Technology. Skyhorse.

[12] Breeze, K. (2022). Non-fungible tokens and art investing for beginners and advance: The ultimate guide to NFTs and digital assets. Publishing House Name.

[13] Brown, C. (2021). Registering artworks on blockchain. Journal of Digital Arts, 3(2), 10-20.

[14] Cassidy, R. (2021). Beyond Bitcoin: Understanding the Blockchain Revolution and How It Will Transform More Than Money. Harper Business.

[15] Catlow, R., Garrett, M., Jones, N. & Skinner, S. (2017). Artists Rethinking the Blockchain. Liverpool: Liverpool University Press.

[16] Drescher, D. (2017). Blockchain Basics A Non-Technical Introduction In 25 Steps. A press.

[17] Fortnow, M. & Terry, Q. (2021). The NFT handbook: How to create, sell and buy non-fungible tokens. Wiley.

[18] Fairfield, Paul, Lyotard and Politics, Discours, 2004, www.mises.com

راه‌اندازی یک واحد پایش امنیت چابک در شرکت‌ها و سازمان‌ها

محمدمهدی قاسمی‌نیا[۱]، محمدحسن میرعارفین[۲]، حسین مرادی[۳]

[۱] کارشناسی ارشد علوم کامپیوتر، دانشگاه یزد، یزد، ایران
ghaseminya@gmail.com
[۲] کارشناسی ارشد مدیریت فناوری اطلاعات، دانشگاه علم و صنعت، تهران، ایران
m_mirarefin@iust.ac.ir
[۳] دانشجوی کارشناسی ارشد مدیریت، دانشگاه تهران، تهران، ایران
ho3in14741@gmail.com

چکیده

ضرورت پیاده‌سازی یک واحد امنیت برای مقابله با تهدیدات محیطی و افزایش ایمنی سازمان، امری غیرقابل انکار است. گسترش روزافزون تهدیدات و پیشرفت‌های نرم و سخت‌افزاری، سازمان‌های بزرگ و کوچک را مجبور به حفاظت بیش از پیش از داده‌ها، سرویس‌ها و دارایی‌هایشان کرده و در این بین، وجود یک تیم منسجم و ساختارمند که بر روی این موضوع متمرکز باشند، امری ضروری است. واحد عملیات امنیت به همین منظور و در جهت مقابله با تهدیدات خارجی و افزایش ایمنی در سازمان تشکیل شده است. مقاله‌ی پیش رو، در آغاز به بررسی و مرور کارها و تحقیقات انجام گرفته در این حوزه می‌پردازد. سپس به شناخت اجزای سازنده‌ی واحد عملیات امنیت در قالب ساختار PPTGC که متشکل از افراد، فرایندها، تکنولوژی، قوانین و رویه‌هاست، پرداخته است. در انتها موارد مستعد تحقیق در این حوزه عنوان شده است.

کلمات کلیدی: واحد عملیات امنیت، امنیت سیستم‌های کامپیوتری، چارچوب پاسخگویی به حادثه، ساختار PPTGC.

۱ مقدمه

براساس آمار یک گزارش که از جمع‌آوری اطلاعات بیش از ۴۷۰۰ شرکت در ۱۸ کشور دنیا در سال ۲۰۲۱ به‌دست آمده، تعداد حملات امنیتی به شرکت‌ها در این سال، با ۳۳ درصد افزایش نسبت به سال ۲۰۲۰، به میانگین ۲۷۰ حمله به ازای هر شرکت رسیده‌است [۱۲]. از جمله دلایلی که می‌توان برای این تعداد حملات گزارش کرد، ضعف سازمان‌ها در داشتن شناختی کامل از مفاهیم و ابزارهای امنیتی سازمان خود، در کنار عدم توانایی در اولویت‌بندی مشکلات و تهدیدات و عدم شناخت کامل و استفاده از ابزارهای موردنیاز برای پاسخگویی به این تهدیدات است. در کنار این موارد، باید به سرعت بالای گسترش فناوری ابزارها، و نیز

پیچیده‌تر شدن حملات و به‌دنبال آن، سخت‌تر شدن شناخت و پاسخگویی به آن‌ها اشاره کرد.

واحد عملیات امنیت، تلاش دارد تا با هرچه واضح‌تر کردن حیطه وظایف، مسئولیت‌ها و ساختار این واحد، به سازمان‌ها در پیاده‌سازی بهتر و موثرتر آن کمک کند. در حالیکه در تصور برخی افراد، وظیفه واحد عملیات امنیت به نظارت بر شبکه داخلی سازمان محدود می‌شود، تعاریف و استانداردهای ارائه‌شده در بخش‌های پیش رو، نشان می‌دهند که این واحد، مرکز تمام عملیات‌های امنیتی سازمان محسوب می‌شود و دامنه گسترده‌ای از وظایف را در بر می‌گیرد.

۲ واحد عملیات امنیت

۱.۲ معرفی

واحد عملیات امنیت، متشکل از تحلیلگران، اپراتورها و متخصصانی است که وظیفه تامین امنیت دستگاه‌های پایانی[1]، زیرساخت تکنولوژی اطلاعات، برنامه‌ها و خدمات سازمان را دارند. اعضای تیم با استفاده از تکنولوژی‌ها و فرایندهای مختلف، در تلاش هستند تا تخطی‌های صورت گرفته از سیاست‌های امنیتی، تلاش‌ها برای اخذ دسترسی‌های غیرمجاز و نیز تهدیدات و حملات صورت گرفته به سیستم‌های سازمان را شناسایی و از آن جلوگیری کرده، یا اثر مخرب آن را کاهش دهند. به‌طور کلی، می‌توان گفت که واحد عملیات امنیت، مسئول حفظ و تعریف چشم‌انداز امنیتی کل سازمان است.

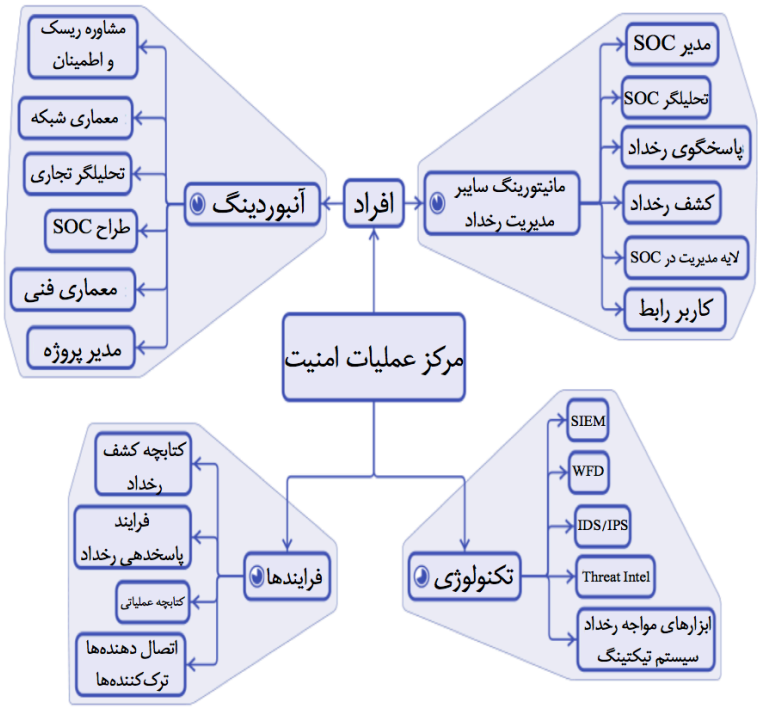
ساختار واحد عملیات امنیت در شکل ۱ قابل مشاهده است [۱۷].

۲.۲ پیشینه تحقیق

از نزدیک به ۱۸ سال پیش که اولین بار واحد عملیات امنیت معرفی شد، تعاریف و وظایف گوناگونی برای آن آورده شده‌است. در یک تعریف، واحد عملیات امنیت، یک واحد متمرکز برای نظارت بر رویدادهای شبکه و پاسخ به حوادث مربوط به رویدادها و حوادث امنیت سایبری است [۸]. مقاله سالانه موسسه SANS که در سال ۲۰۲۲ منتشر شده‌است، اینگونه بیان می‌کند که بیشتر تعاریف از واحد عملیات امنیت، مفاهیمی انتزاعی هستند که هر سازمانی با توجه به امکانات، توانایی‌های افراد و دانش خود آن‌را در جهت حفاظت از خود و پاسخ به تهدیدات محیطی پیاده‌سازی می‌کند که ممکن است همه‌ی از یک ساختار پیروی نکنند [۵]. علی‌رغم وجود اختلاف در بین تعاریف مختلف، شاید اکثر محققین حوزه امنیت بر این تعریف اتفاق نظر داشته باشند که یک مرکز عملیات امنیت، ساختاری پیچیده به منظور مدیریت و بهبود عملکرد امنیتی کل سیستم در یک سازمان است که به کمک فرآیندهای تعریف شده و به طور خاص متمرکز بر تهدید سایبری، نظارت، تحقیقات قانونی، و مدیریت حوادث و گزارش‌دهی فعالیت می‌کند [۱۶].

پس از ذکر تعاریف اولیه، به چارچوب‌های پیشنهادی و اجزای سازنده‌ی واحد عملیات امنیت پرداخته شده‌است. برای نمونه، یک پژوهش با اشاره به وجود سه عامل افراد، فرایندها و تکنولوژی، هماهنگی میان

[1] Endpoint

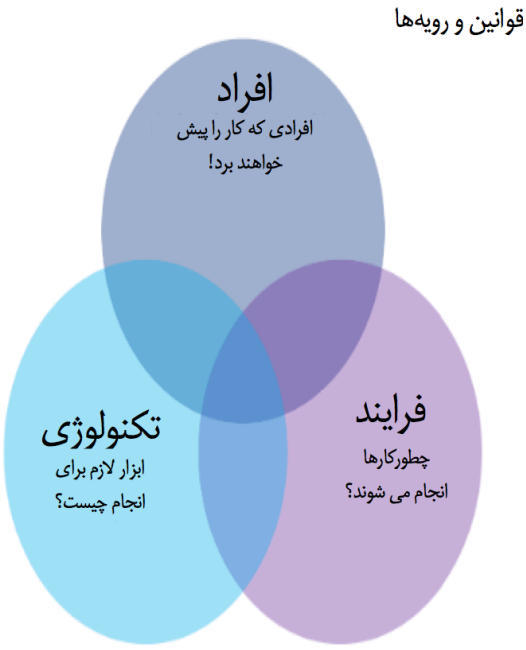


شکل ۱: معماری واحد عملیات امنیت

آن‌ها را عاملی در جهت تشکیل یک تیم واحد عملیات امنیت قوی برمی‌شمارد [۱۰]. پژوهشی دیگر، واحد عملیات امنیت را گروهی از افراد متخصص تعریف می‌کند که از روندها و ابزارها استفاده می‌کنند تا جلوی نفوذ به سیستم را بگیرند [۱۳]. در یکی از جدیدترین تعاریف از ساختار واحد عملیات امنیت، به‌دلیل اهمیت بالای بعد قوانین و رویه‌ها، این بعد از ذیل روندها جدا شده و به یک پایه‌ی اصلی و مستقل در ساختار واحد تبدیل شده‌است [۹]. مشخص است که در همه‌ی منابع مورد بررسی، به سه بعد افراد، روندها و تکنولوژی اشاره شده و در برخی منابع جدیدتر، بعد قوانین و رویه‌ها نیز به‌صورت مستقل بررسی شده‌است.

۳ راه اندازی واحد عملیات امنیت

در این قسمت، به توضیح هریک از ابعاد واحد عملیات امنیت پرداخته می‌شود. این بخش درواقع به افزایش کارایی و بهبود عملکرد واحد عملیات امنیت از طریق تعریف درست روندها، به‌کارگیری ابزار مناسب و استخدام و آموزش افراد شایسته برای جایگاه‌های تعریف شده در واحد می‌پردازد. با مطالعه ادبیات و تحقیقات انجام‌شده در زمینه اجزای سازنده این واحد، مشخص شد که ساختار متشکل از افراد، فرایندها، تکنولوژی، قوانین و رویه‌ها و معروف به PPTGC مطابق شکل ۲ در اکثر موارد پیشنهاد شده‌است [۹].



شکل ۲: اجزای سازنده واحد عملیات امنیت

۱.۳ منابع انسانی–افراد

منظور از افراد، هر جزء انسانی در مجموعه است که از طریق استفاده از ابزارهای فنی و در بستر فرایندها، در جهت تحقق اهداف واحد تلاش می‌کند. در ابتدا، باید افرادی به منظور تشکیل تیم واحد عملیات امنیت انتخاب شوند و سپس، با تشکیل تیم‌ها و تعریف نقش‌ها، مسئولیت به افراد مختلف واگذار شود.

تیم‌های مرکز عملیات امنیت: با حضور حداقل اعضا، اکنون باید برای رسمیت بخشیدن به واحد عملیات امنیت، به تعریف ساختارها و وظایف پرداخت. یکی از چارچوب‌های مورداستفاده در واحدهای عملیات امنیت، بهره‌گیری از سه تیم قرمز، آبی و بنفش است.

تیم قرمز: وظیفه اصلی تیم قرمز، حمله به تیم آبی و تلاش برای از بین بردن سپرهای امنیتی آن است. در واقع اعضای تیم قرمز، هکرهای اخلاقی[۲] هستند که نه با هدف سوءاستفاده، بلکه با هدف شناسایی نقاط ضعف سیستم به آن حمله می‌کنند [۴] [۹].

مهم‌ترین ابزارهایی که تیم قرمز از آن‌ها استفاده می‌کند، عبارتند از: تست نفوذ[۳] که با هدف شناسایی نقاط ضعف اپلیکیشن، شبکه و ابزارهای مورداستفاده یک سیستم اجرا می‌شود [۴]. نکته مهم در این خصوص، این

[2] Ethical hackers
[3] Penetration testing

است که اجراکنندگان تست نفوذ، بیشتر از آنکه به‌دنبال یافتن آسیب‌پذیری‌های کاملا جدید[۴] باشند، در صدد استفاده از آسیب‌هایی هستند که پیش از این شناخته شده، اما هنوز توسط توسعه دهنده سیستم برطرف نشده‌اند.

ابزارهای جعل هویت مانند فیشینگ[۵] و مهندسی اجتماعی[۶]. مهندسی اجتماعی، فرایند نفوذ به یک سیستم، با استفاده از نفوذ به افراد آن سیستم است که در اغلب مواقع، قدمِ پیش از نفوذ فنی می‌باشد [۱۵].

ابزارهای پیمایش درگاه‌ها و شبکه[۷] که در تلاش برای شناسایی درگاه‌های باز[۸] و ارتباطات ورودی و خروجی شبکه سیستم است. در عین حال که می‌توان از ابزارهای آماده نظیر زن‌مپ[۹] و وایرشارک[۱۰] برای این موارد استفاده کرد، برای دسترسی به اطلاعات دقیق‌تر و جزئیات اضافه، می‌توان به کمک کتابخانه‌های قدرتمند زبان‌هایی مثل پایتون و C، ابزارهایی را از ابتدا توسعه داد تا امکان کنترل بیشتر ر روی سیستم نیز مهیا باشد.

یکی از مهم‌ترین اقدامات پس از حملات آزمایشی، نگارش دقیق گزارش حملات است. این گزارش‌ها، شامل ۲ بخش است که در بخش اول، مواردی نظیر ابزارهای فنی مورداستفاده، اهداف مورد حمله و تلاش‌های موفق و ناموفق ذکر می‌شود. در بخش دوم نیز تیم قرمز به ارائه پیشنهادات و راهکارهای افزایش امنیت سیستم اشاره می‌کند. این گزارش‌ها در ادامه، مورد استفاده‌ی تیم آبی قرار خواهند گرفت.

تیم آبی: در نقطه مقابل تیم قرمز، تیم آبی قرار دارد که وظیفه اعضای آن، حفظ امنیت سیستم در مقابل تهدیدات و حملات، ارزیابی فنی ابزارهای مورد استفاده و کشف، شناسایی و از بین بردن آسیب پذیری‌های سیستم است [۳].

مهم‌ترین وظایف تیم آبی عبارتند از:

- نظارت بر عملکرد سیستم
- تشخیص و از بین بردن تهدیدات و حملات امنیتی
- جمع‌آوری داده‌های مربوط به ترافیک داخلی و خارجی شبکه و تحلیل آن‌ها
- پیاده‌سازی و مدیریت ابزارهای کنترل دسترسی کاربران
- به‌روزرسانی ابزارها و نرم‌افزارهای مورداستفاده
- اجرای مهندسی معکوس بر روی حملات صورت گرفته به سامانه‌های مجموعه

[4] Zero days
[5] Phishing
[6] Social Engineering
[7] Port and network scanner
[8] open ports
[9] Zenmap
[10] Wireshark

- طراحی و توسعه سیاست‌های پاسخ فوری جهت اطمینان از بازگشت سریع سیستم به حالت عادی پس از بروز حمله

یکی دیگر از وظایف مهم تیم آبی، به‌روز نگه‌داشتن دانش افراد و سرمایه انسانی مجموعه در جهت مقابله با تهدیدات است. در جایی‌که تیم قرمز، و نیز تهدیدات دنیای واقعی از ابزارهای مهندسی اجتماعی برای نفوذ به افراد استفاده می‌کنند، مقابله با آن‌ها وظیفه تیم آبی بوده تا با ارتقای دانش اعضا در خصوص جدیدترین تهدیدات انسانی در حوزه‌های مهندسی اجتماعی و جعل هویت، و نیز تعیین سیاست‌هایی در حوزه‌هایی مثل رمزهای عبور [۱۱]، از خطرات احتمالی جلوگیری کند.

همانند تیم قرمز، تیم آبی نیز باید به طور منظم از فعالیت‌های خود گزارش تهیه کرده و در آن، ضمن جمع‌آوری مدارک و لاگ‌های به دست آمده از حادثه، تجربیات تیم از این اتفاق و نیز اقدامات پیش‌رو را ذکر کند.

تیم بنفش: عنوان تیم برای تیم بنفش، شاید به طور کامل درست نباشد؛ از آن جهت که بیشتر از آنکه این تیم، یک تیم مستقل با اعضایی جدا باشد، ترکیبی از اعضای تیم‌های قرمز و آبی است که وظیفه اصلی آن، ایجاد و تسهیل ارتباط بین اعضای این دو تیم در جهت اشتراک‌گذاری یافته‌هایشان است[۳].

علی رغم وظیفه مشترک هر دو تیم قرمز و آبی در بهبود امنیت و کارایی سیستم، گاهی اوقات آن‌ها از به اشتراک گذاری رازهای خود امتناع می‌کنند؛ به این معنی که تیم قرمز، اطلاعات دقیقی از نحوه آسیب به سیستم را در اختیار تیم قرمز نمی‌گذارد، و تیم آبی نیز از نحوه کشف و یافتن جزئیات حملات تیم قرمز و مقابله با آن‌ها صحبت چندانی نمی‌کند. دلیل اصلی تشکیل تیم بنفش، که در واقع ترکیبی از اعضای این دو تیم است، همین تسهیل ارتباط است تا دانش به‌دست آمده از فعالیت‌های دو تیم، راحت‌تر به دیگری منتقل شود تا توسعه و پایدارسازی سیستم دچار مشکل نشود.

نقش‌ها و وظایف اعضای واحد عملیات امنیت: یک واحد عملیات امنیت، دارای ۴ دسته جایگاه اصلی به شرح ذیل است[۶][۲][۹]:

۱. نقش‌های مدیریتی

- هماهنگ‌کننده تیم پاسخگویی به حادثه [۱۲]
- مدیر واحد عملیات امنیت [۱۳]
- مدیر ارشد امنیت اطلاعات [۱۴]

۲. نقش‌های پاسخگویی به حادثه

[11] Password policies
[12] Incident response coordinator
[13] SOC manager
[14] Chief information security officer(CISO)

- پاسخگوی اولیه حادثه[۱۵]
- محقق امنیت[۱۶]
- تحلیلگر ارشد امنیت[۱۷]

۳. نقش های مشاوره‌ای

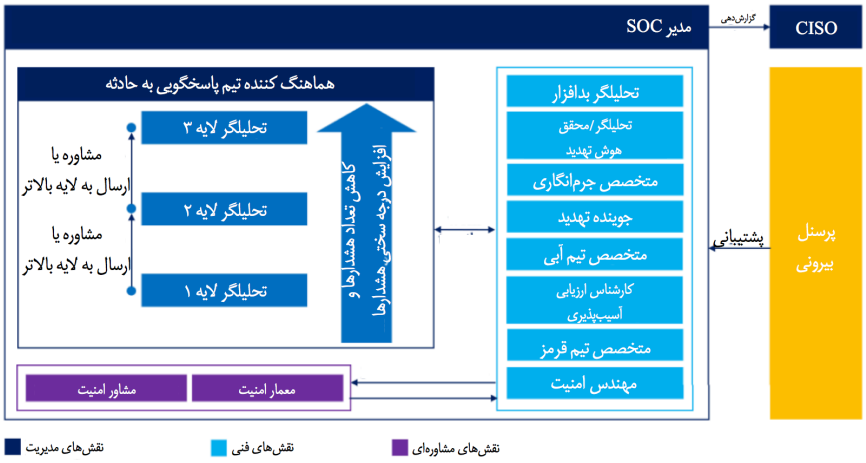
- معمار امنیت[۱۸]
- مشاور امنیت[۱۹]

۴. نقش‌های تکمیلی

- تحلیلگر بدافزار[۲۰]
- جوینده تهدید[۲۱]
- تحلیلگر/محقق هوش تهدید[۲۲]
- متخصص جرم‌انگاری[۲۳]
- متخصص تیم قرمز و تیم آبی
- کارشناس ارزیابی آسیب پذیری[۲۴]
- مهندس امنیت[۲۵]

وجود این نقش‌های مختلف در کنار یکدیگر، نیازمند ساختاری منسجم است تا نتیجه مطلوب که تامین امنیت سازمان است، حاصل شود. شکل ۳، مدلی پیشنهادی از نحوه ارتباط این نقش‌ها با یکدیگر است. مطابق این ساختار، افراد خارج از واحد عملیات امنیت، برای حصول نتیجه بهتر، با این واحد همکاری می‌کنند [۹].

[15] Incident responder
[16] Security investigator
[17] Advanced security analyst
[18] Security architect
[19] Security Consultant
[20] Malware analyst
[21] Threat hunter
[22] Threat intelligence analyst/researcher
[23] Forensics specialist
[24] vulnerability assessment expert
[25] Security engineer

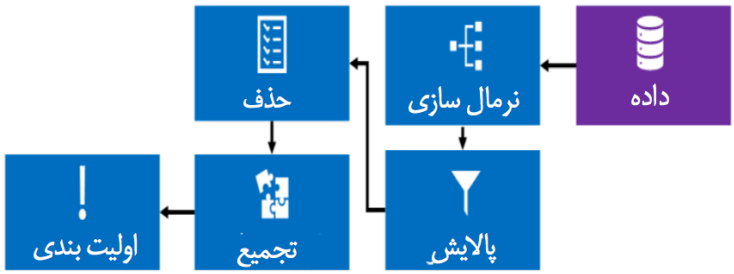


شکل ۳: نحوه ارتباط نقش‌های مختلف در واحد عملیات امنیت

۲.۳ ابزارها

اعضای تیم عملیات امنیت به منظور پیاده‌سازی فرایندها، به ابزارهایی نیاز دارند تا در بخش‌های مختلف از آن‌ها استفاده کنند. ۳ بخش اصلی ابزارهای این واحد به شرح زیر هستند:

۱. **جمع‌آوری اطلاعات**[۲۶]: اولین گام پیش از هرگونه اقدامی در سیستم، داشتن اطلاعات کافی از بخش‌های مختلف آن است. جمع‌آوری داده مراحل مختلفی را طی می‌کند تا به شکلی منظم و قابل فهم درآید. مراحل جمع‌آوری داده، مطابق شکل ۴ نمایش داده شده‌است [۹].



شکل ۴: فرایند جمع‌آوری داده‌ها

[26] Data collection

(آ) نرمال‌سازی: در بررسی تحقیقات، اغلب از نرمال سازی با عنوان پیش‌پردازش داده‌ها یاد شده‌است. این مورد به آن معنی است که داده‌های جمع‌آوری شده باید تحت یک قالب یکسان قرار گرفته و موارد ناهمگون احتمالی، یک شکل و استاندارد ثابت به خود بگیرند. مهم‌ترین نکته در هماهنگی داده‌ها، پیروی کردن همه‌ی آن‌ها از یک قالب متنی و زمانی استاندارد و یکسان است تا امکان استفاده ا آن‌ها در قالب مقایسه فراهم شود [۱].

(ب) پالایش و حذف: از آنجایی‌که دستگاه‌های موجود در سیستم، حجم بزرگی از داده‌ها را تولید می‌کنند، در این مرحله باید موارد کم‌اهمیت‌تر از دور خارج شوند تا داده‌های اصلی قابل استفاده باشند [۷].

(ج) تجمیع و اولویت‌بندی: موارد مختلفی از داده‌های تولیدشده که مشابه هستند، تجمیع می‌شوند و سپس موارد مهم‌تر که باید سریع‌تر مورد توجه قرار بگیرند، مشخص می‌شوند [۷].

پس از شناخت مراحل تبدیل داده‌های خام جمع‌آوری شده به داده‌های قابل استفاده، باید انواع سیستم‌های اطلاعاتی را شناخت. این سیستم‌ها دسته‌بندی‌های مختلفی دارند [۹] مانند: سیستم‌های اطلاعاتی توزیع‌شده[۲۷] / مرکزی[۲۸]، سیستم‌های اطلاعاتی جزئی[۲۹] / کامل[۳۰] و سیستم‌های اطلاعاتی بلادرنگ[۳۱] / تجمیعی[۳۲]

بخش‌ها و ابزارهای مختلفی در سیستم می‌توانند به جمع‌آوری داده بپردازند که به برخی از آن‌ها اشاره خواهد شد:

(آ) نرم‌افزارهای امنیتی نظیر سیستم‌های تشخیص/جلوگیری از ورود و دیوارآتش

(ب) ابزارهای شبکه مانند سرورها و روترها

(ج) بسترهای مجازی‌سازی نظیر مجازی‌سازها[۳۳]

(د) ابزارهای عملیاتی نظیر حسگرها[۳۴] و محرک‌ها[۳۵]

(ه) سایر نرم‌افزارها مانند پایگاه‌های داده و سیستم‌عامل‌ها

(و) ابزارهای فیزیکی مثل دوربین‌های نظارتی و سیستم‌های ورود و خروج[۳۶]

[27] Distributed
[28] Centralized
[29] Partial
[30] Full
[31] Real-time
[32] Historical
[33] Hypervisor
[34] Sensor
[35] Actuator
[36] Access control systems

(ز) افراد

بسته به میزان و نوع نیاز سازمان، کمیت و کیفیت استفاده از ابزارهای مختلف به منظور جمع‌آوری داده متفاوت است. در عین حال که جمع‌آوری داده‌های کم، می‌تواند منجر به ناشناس ماندن تهدیدات شود و امنیت سیستم را مختل کند، جمع‌آوری داده‌های زیاد نیز منجر به کاهش عملکرد سیستم می‌شود.

۲. **آنالیز و تشخیص**[۳۷]: با وجود گسترش ابزارهای تشخیص خودکار حملات، برخی از حملات پیچیده را نمی‌توان به این صورت شناسایی کرد که نیازمند مداخله انسانی به این منظور است. در این بین، از ۳ روش اصلی به شرح زیر، برای شناسایی حملات و تهدیدات متوجه سیستم، استفاده می‌شود:

(آ) شناسایی مبتنی بر ناهنجاری[۳۸]
این روش، رفتار عادی سیستم را به عنوان یک مبنا در نظر گرفته و انحراف از عملکردهای پیش‌آمده را از طریق مقایسه شناسایی می‌کند.

(ب) شناسایی مبتنی بر دانش[۳۹]
این روش بیشتر برای شناسایی حملات تکراری و مشابه استفاده می‌شود و در آن، از دانش تجمیع شده که از حملات قبلی به‌دست آمده‌اند، به عنوان تجربه استفاده می‌شود.

(ج) شناسایی مبتنی بر معیار[۴۰]
در روش شناسایی مبتنی بر معیار، با استفاده از نمایه‌ها[۴۱] و قراردادهای از پیش تعیین‌شده[۴۲]، حوادث تشخیص داده می‌شوند.

۳. **ارائه**[۴۳]: آخرین دسته از ابزارها، جهت نمایش رفتار سیستم به‌کار می‌روند. به منظور مدیریت بهتر بخش‌های مختلف سیستم، نیاز است تا داده‌های جمع‌آوری شده و یا تهدیدات شناسایی شده در ۲ بخش گذشته، به شکلی نمایش داده شوند تا به جز اعضای خبره‌ی واحد عملیات امنیت، برای سایر اعضای کم‌تجربه‌تر این واحد و یا اعضای سایر واحدها قابل فهم باشند. به این منظور در اغلب مواقع از داشبورهای گرافیکی استفاده می‌شود.

[37] Analysis & detection
[38] Anomaly-based detection
[39] Knowledge-based detection
[40] Specification-based detection
[41] Profile
[42] Protocols
[43] Presentation

۳.۳ رویه و دستورالعمل‌ها

است که صرفا مشخص می‌کند چه کاری باید انجام شود و نحوه انجام آن را مشخص نمی‌کند. چارچوب‌ها اغلب منعطف و ماژولار اند؛ به این معنی که قابلیت کم و زیاد کردن بخش‌های مختلف بسته به نیاز مجموعه وجود دارد و یک ساختار خشک و غیرقابل تغییر نیستند.

این چارچوب که توسط موسسه ملی استاندارد و تکنولوژی آمریکا توسعه داده شده‌است، دارای ۴ مرحله اصلی به شرح زیر است [۱۴] :

۱. آماده‌سازی[۴۴]

این مرحله ناظر به آماده‌سازی ابزارها و تجهیزات موردنیاز برای مقابله با تهدیدات است و به طور کلی شامل مواردی نظیر مهیاکردن ابزارهای فنی، آموزش کارکنان و سیاست‌های پاسخگویی به تهدیدات و روندهای مقابله با آنها، و نیز آماده‌سازی سیستم تشخیص تهدیدات است. در این بخش، ابتدا باید به اولویت‌بندی حملات پرداخت.

به‌این منظور، اعضای تیم باید لیستی از حملات رایج تهیه کرده، و سپس به صورت خاص درجه اهمیت هریک را گزارش کنند. شایع‌ترین حملات به سیستم‌های فناوری و اطلاعاتی عبارتند از [۱۱]:

(آ) بررسی درگاه‌های باز سیستم[۴۵]: در اغلب مواقع، اولویت پایینی داشته و اگر نشانه‌های دیگری مبنی بر وجود حمله گزارش نشوند، باید نادیده گرفته شوند.

(ب) آلودگی از طریق بدافزار[۴۶]: در این مواقع باید هرگونه ردی از بدافزار به‌سرعت از سیستم پاک شده و سپس با بررسی دقیق، اطمینان حاصل شود که ردی از بدافزار باقی نمانده‌است. این حملات معمولا اولویت متوسط دارند.

(ج) حملات انکار خدمت[۴۷] : بسته به طول مدت ادامه‌دار بودن این حملات، می‌توانند اولویت پایین یا بالایی داشته‌باشند. پاسخ مناسب در مقابل این دست حملات، سدکردن راه درخواست‌های مخرب به‌نحوی است که عملکرد کلی سیستم دچار خدشه نشود. معمولا می‌توان از طریق مدیریت سرویس‌ها و دستگاه‌های لبه‌ی شرکت (که مستقیما با اینترنت در ارتباط بوده و در معرض حمله هستند) و یا حتی ارتباط با ارائه‌دهنده خدمت اینترنت[۴۸] مبنی بر مسدودسازی برخی درخواست‌ها به مقصد سامانه‌های سازمان، به این مهم دست یافت.

(د) دسترسی غیرمجاز[۴۹] : این دسته از دسترسی‌ها، چه توسط کاربران داخلی سازمان و چه توسط مهاجمین بیرونی، باید به‌سرعت قطع شده و اقدامات بعدی لازم نظیر بازنگری قوانین و

[44] Preparation
[45] Port Scanning
[46] Malware Infection
[47] Denial of Service Attacks
[48] Internet Service Provider
[49] Unauthorized Access

رویه‌های دسترسی و تغییر گذرواژه‌های ضعیف انجام گیرند. این دسته از حملات که مهاجم به درون سیستم نفوذ کرده، اولویت بالایی دارند و باید در اولین فرصت بررسی شوند.

(ه) حملات سطح اینترنت: این دسته از حملات شامل مواردی نظیر XSS، SQL Injection و CSRF می‌شوند که از اولویت بالایی برخوردار بوده و معمولا با بررسی گزارش رخداد پایگاه‌داده [۵۰]، قوانین و رویه‌های حاکم بر سرویس‌ها و فایل‌های تنظیمات برنامه‌ها [۵۱]، قابل ردیابی به نقطه وقوع حمله و سپس از بین بردن آن است.

پس از دفع خطر حمله و برقراری آرامش نسبی، باید اقدام به تهیه راهنمای پاسخ به حملات کرد. بدیهی است که ثبت روند پاسخ به حملات، مخصوصا حملاتی که برای دفعات اول صورت گرفته و هنوز شیوه دقیق پاسخ به آن پیدا نشده‌است، امری ضروری است؛ چراکه با تکرار این حملات در سازمان، اگر چارچوبی برای ثبت و ضبط دقیق این موارد موجود نباشد، ممکن است نیاز باشد هر بار روند از ابتدا و همراه با آزمون و خطا طی شود که اینگونه، علاوه بر افزایش آسیب‌پذیری سیستم، سرعت و دقت در پاسخگویی به حملات نیز کاهش می‌یابد. افزون براین، با خروج اعضای قدیمی و جایگزینی اعضای جدید به‌جای آنان، نیاز به وجود چنین اسنادی بیش‌از پیش احساس می‌شود تا اعضای جدید، به جای آغاز روند تحقیق و توسعه از صفر، ادامه کارهای گذشته را پیش ببرند.

۲. تشخیص و بررسی [۵۲]

پس از آماده‌سازی سیستم تشخیص تهدیدات در مرحله ۱، هنگامی که نشانه‌هایی از ورود به سیستم مشاهده یا گزارش شود، وارد مرحله ۲ می‌شویم. این مرحله، خود شامل ۲ بخش بوده و در بخش اول که تشخیص خطر است، علامت‌هایی توسط نشانگرهای [۵۳] سیستم‌های نظارتی مشاهده شده و سپس روند گزارش‌دهی و طی مراحل بعدی آغاز می‌شود. در این مرحله می‌توان از سیستم‌های نظارتی در حوزه‌های مختلفی نظیر دیوار آتش [۵۴]، سیستم‌های تشخیص/ پیشگیری نفوذ [۵۵] و سیستم‌های آنالیز پهنای باند شبکه [۵۶] استفاده کرد.

در بخش دوم این مرحله، نوبت به آنالیز داده‌های دریافتی از نشانگرهای بخش قبلی می‌رسد. در اینجا، یک متخصص آنالیز حادثه باید تایید کند که آیا واقعا حادثه اتفاق افتاده است یا خیر. دلیل این امر، وجود خطاهای مثبت کاذب [۵۷] است که در آن، طبق داده‌های حاصل از نشانگرها یک نفوذ وجود دارد، اما در واقع خطری سیستم را تهدید نمی‌کند. این وظیفه یکی از مهم‌ترین و سخت‌ترین وظایف

[50] DataBase Logs
[51] Application Configuration Files
[52] Detect and analysis
[53] Indicators
[54] Firewall
[55] Intrusion detection/prevention systems
[56] Network traffic analysis systems
[57] False positive

در روند پاسخگویی به حادثه است و باید فرد یا افرادی باتجربه و بامهارت مسئولیت آن را به عهده بگیرند.

۳. نگهداری، از بین بردن و بازیابی[۵۸]

این مرحله دارای ۳ بخش است که در بخش اول، وظیفه نگهداری به معنی جلوگیری از بدتر شدن شرایط است و در ادامه باید به مرور کنترل سیستم را مجددا به دست گرفت.

بخش دوم، از بین بردن خطر است و شامل حذف بدافزار مخرب و یا قطع دسترسی و حذف کاربران مشکوک است.

در مرحله آخر، بازیابی سیستم به حالت عادی در دستور کار است و این کار، به‌کمک بازگردانی پشتیبان‌ها[۵۹]، نصب مجدد برخی نرم‌افزارها و تغییر گذرواژه‌های نامطمئن صورت می‌گیرد.

۴. فعالیت‌های پساحادثه[۶۰]

تمرکز مرحله آخر، بر روی درس‌های آموخته شده از حادثه و با ۲ محور است: اول آنکه توانایی پاسخگویی به حادثه در مجموعه افزایش یابد و به طور کلی آسیب‌پذیری در مقابل تهدیدات کاهش پیدا کند. دوم اینکه از تکرار اتفاقات مشابه در آینده جلوگیری شود. در این مرحله، به منظور کسب تجربه بهتر از حادثه رخ داده، تیم باید به چند سؤال پاسخ دهد، از جمله: دقیقا چه اتفاقی افتاد؟ چه چیزی خوب پیش رفت؟ چه چیزی خوب پیش نرفت؟ کدام افراد کارشان را به خوبی انجام دادند؟ کار چه کسانی می‌توانست بهتر انجام شود؟ کدام روندها به درستی اجرا شد؟ کدام روندها می‌توانستند بهتر انجام شوند؟ چگونه می‌توانستیم چلوی این اتفاق را بگیریم؟ با پاسخگویی دقیق به سؤالات بالا و سؤالاتی از این دست، می‌توان گزارشی دقیق از حادثه تهیه کرد تا ضمن ارتقای دانش مجموعه در مواجه با حوادث مشابه، پاسخگویی کلی نیز بهبود یابد.

۴ سخن پایانی

در این نوشته یک روشی برای ایجاد یک تیم واحد عملیات امنیت به همراه گام‌های راه‌اندازی و اهداف نهایی ارائه گردید، همچنین تفکیک اجزا و مشخص کردن راهبرد و راهبری کلی اجزا، تیمها و نقش‌ها در کنار هدف اصلی اجزا و چگونگی ارتباط آنها با هم به شکل کامل در اختیار خواننده قرار گرفت.

به عنوان موضوعات مستعد تحقیق بیشتر می توان در مورد بررسی ایرادات ممکن در استانداردهای بین‌المللی از قبیل ایزو در حوزه امنیت و تقابل آن با رویکردهای فضای سایبر جمهوری اسلامی ایران سخن گفت و همچنین چگونگی افزایش امنیت فضای سایبر جمهوری اسلامی ایران با الگو قراردادن این استانداردهای موجود، و باز تولید استاندارد بومی نیز می‌تواند زمینه های تحقیقاتی بعدی باشد.

[58] containment, eradication and recovery
[59] backups
[60] Post incident activity

سپاس‌گزاری

خدا را شاکریم که به ما کمک داد تا بتوانیم هر چند کوچک قدمی در حوزه فضای سایبر برداریم. از سازمان صدرا بابت پشتیبانی کامل در قالب یک پروژه پژوهشی و کمکهای بی دریغشان در تولید این مقاله نهایت سپاسگزاری را داریم.

مراجع

[1] S. Rezayi A. Madani and H. Gharaee. Log management comprehensive architecture in security operation center (soc). *Int. Conf. Comput. Aspects Social Netw. (CASoN)*, page 284–289, Oct 2011.

[2] O. Cassetto. Security operations center roles and responsibilities. *Exabeam, Foster City, CA, USA, Tech. Rep*, 2019.

[3] Svitlana Chaplinska. A purple team approach to attack automation in the cloud native environ-ment. *Aalto University*, 2022.

[4] Matthias Caretta Crichlow. A study on blue team's opsec failures. 2020.

[5] C. Crowley and B. Filkins. Sans 2022 security operations center survey. In *SANS Inst*, volume Swansea, U.K., 2022.

[6] Carson Zimmerman Kathryn Knerler, Ingid Parker. 11 strategies of a world-class cyber-security operations center. *MITRE Corp Bedford, MA, USA, Tech. Rep*, 2022.

[7] K. Kent and M. Souppaya. Guide to computer security log management: Recommendations of the national institute of standards and technology. *Nat. Inst. Standards Technol., Gaithersburg, MD, USA Tech. Rep. 800-92*, 2006.

[8] J. Mtsweni M. Mutemwa and L. Zimba. Integrating a security operations centre with an organization's existing procedures, policies and information technology systems. In *Intell. Innov. Comput. Appl. (ICONIC)*, page 1–6, Dec 2018.

[9] I. Fichtinger M. Vielberth, F. Böhm and G. Pernul. Security operations center: A systematic study and open challenges. *IEEE Access*, 8:227756–227779, 2020.

[10] M. Majid and K. Ariffi. Success factors for cyber security operation center (soc) establishment. In *1st Int. Conf. Informat., Eng., Sci.Technol.*, number Bandung, IN, USA, page 1–11, May 2019.

[11] J. Anuradha Mohan V. Pawar. Network security and types of attacks in network, procedia computer science. 48:503–506, 2015.

[12] NAdara. How aligning security and the business creates cyber resilience. *Accenture*, New York, NY, USA, 2021.

[13] C. Onwubiko. Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. In *International Conference on Cyber Situational Awareness*, volume Data Analytics and Assessment (CyberSA), 2015.

[14] T. Grance P. Cichonski, T. Millar and K. Scarfone. Computer security incident handling guide: Special publication 800-61 revision 2. *Nat. Inst. Standards Technol*, 2012.

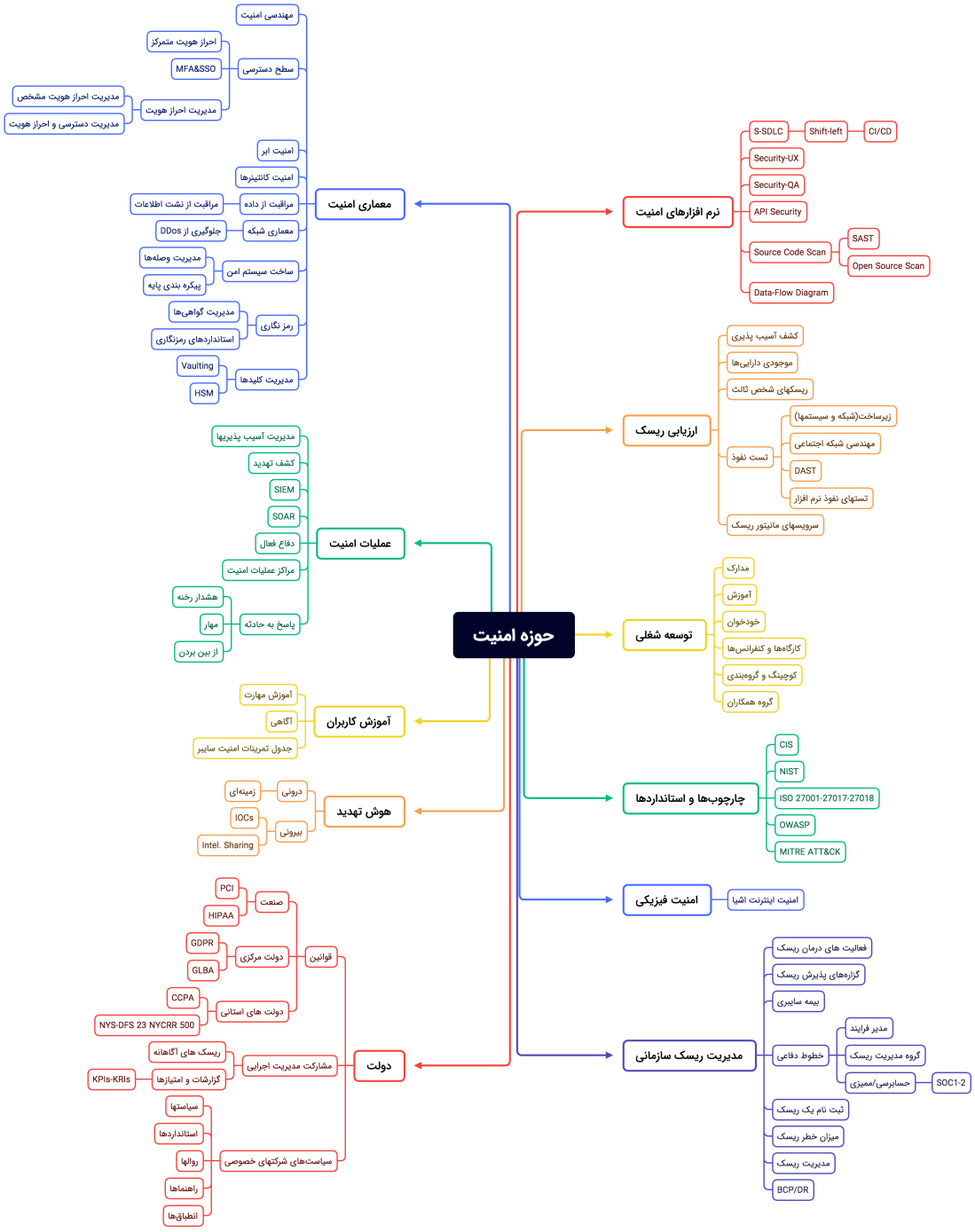
[15] Kaabouch N. Social Engineering Attacks Salahdine F. A survey. future internet. 2019.

[16] Keith & Paans Ronald Schinagl, Stef & Schoon. A framework for designing a security operations centre (soc). *10.1109/HICSS.2015.270*, pages 2253–2262, 2015.

[17] R. Vaarandi and S. Mäses. How to build a soc on a budget. *IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece*, pages 171–177, 2022.

پیوست

درخت دانش حوزه امنیت سایبر



شکل ۵: درخت دانش حوزه امنیت سایبر

طراحی الگوریتم استدلال، اولویت گام دوم در ارتقای علوم اسلامی

محمدحسن احمدی[1]

[1]دانشیار دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
ahmadi_mh@ut.ac.ir

چکیده

پژوهش‌های بسیاری است که در آنها پژوهشگر نسبت به مبانی و پیش‌فرض‌ها -یی که چه بسا خود به‌صورت مستقیم یا غیرمستقیم (با اتکا به مبانی دیگران) آنها را مفروض گرفته- بی‌توجه است. از سوی دیگر، متغیرهای به‌کارگرفته شده در تحلیل متون، بر اساس استاندارد خاصی تعیین نمی‌شوند. تحلیل‌های کمی هم که به مدد فراوری شدن متون، شیوع پیدا کرده است. این همه، گویای آن است که لازم است پیشنهاد طراحی الگوریتمی داده شود تا همواره به‌روزرسانی شده و در پیشخوان پژوهش‌ها قرار گیرند. روشن است که نه حافظه عادی پژوهشگر مجال این فرآیند به‌روزرسانی را دارد و نه اساساً حجم پژوهش‌های کنونی، اجازه پرداختن به این حوزه گسترده از مبانی و متغیرها را می‌دهد.این پژوهش بر آن است تا به مدد هوش مصنوعی و با وجود آسیب پژوهش‌های جاری از جهت عدم جامعیت نسبت به ابعاد موضوع، به تدوین الگوریتمی در این خصوص دست یازد تا نتایج پژوهش‌های مبتنی بر استدلال‌های متنی، به الگوی معیار نزدیک‌تر شود.

کلمات کلیدی: هوش مصنوعی، پیش‌فرض، روش تحقیق، حافظه، الگوریتم استدلال.

۱ مقدمه

متاسفانه، نوع نگاه ما به فضای مجازی هنوز هم یک نگاه درجه دومی است. تفکیک فضای پیرامونی به مجازی و حقیقی، خود گواه این مدعاست. در واقع، هنوز فضای سایبر را به معنی واقعی، جزء واقعیات زندگی به حساب نیاورده‌ایم. در تعریف پژوهش در بهترین حالت به پردازش اطلاعات برای رسیدن به سؤالی مشخص تکیه شده است.

در فضای پیشرفت مطالعات علوم انسانی، دو مرحله پیش روست که مرحله اول تا حدودی پشت سر گذاشته شده است:

۱. **دیجیتالی‌سازی و فرآوری متون دینی**

۲. **تهیه دستگاه مبتنی بر هوش مصنوعی برای تجزیه و تحلیل متون**

پردازش اطلاعات توسط یک الگوریتم استدلال متن-محور، الگوی پیشنهادی این مقاله است. مشکل اصلی امروز پژوهش‌های علوم انسانی ناشی از نداشتن ضابطه صحیح، دقیق و استاندارد برای فهم متون است. در واقع، سؤال مهمتری که در جستجوی فراهم آوردن اطلاعات بروز می‌کند، این است که چگونه فرآیند استدلال – و به‌طور دقیق‌تر در علوم اسلامی – فرآیند تجزیه و تحلیل متن چگونه سازمان‌یافته است؟ در واقع، مبنای مرحله دوم آن این است که متن به تنهایی دانش تولید نمی‌کند و تنها با انباشت اطلاعات، دانش تولید نمی‌شود. از این رو، لازم است متن را به دانش تبدیل کرد.

۲ تبیین ضرورت الگوریتم استدلال

مواردی که ضرورت تدوین الگوریتم استدلال متن-محور را توجیه می‌کند، عبارتند از:

۱.۲ سوگیری بازماندگی

سوگیری بازماندگی (Survival Bias) یکی از نمونه‌های بروز خطا در استدلال است. این خطا زمانی پیش می‌آید که تنها بر روی افراد یا چیزهایی که از یک فرآیند انتخاب گذشته‌اند، تمرکز شود و آن‌هایی را که نتوانسته‌اند عبور کنند به دلیل اینکه قابل‌مشاهده نیستند نادیده گرفته شوند. به‌عنوان نمونه، فردی بر اساس تعداد محدودی از دانش‌آموختگان یک دبیرستان که توانسته‌اند در دانشگاه‌های خوب قبول شوند، نتیجه بگیرد که آن دبیرستان خدمات آموزشی برتری ارائه می‌دهد. یا اینکه تنها با مقایسه ساختمان‌های قدیمی باقی‌مانده با ساختمان‌های امروزی نتیجه گرفته شود که در گذشته ساختمان‌های بهتری ساخته می‌شده است.[۱]

[۱] در جنگ جهانی دوم، رهبران نظامی انگلستان و آمریکا که به دنبال کاهش تلفات بمب‌افکن‌های خود بودند به این نتیجه رسیدند که باید زره تقویتی بیشتری به هواپیماهای خود اضافه کنند تا آن‌ها را در برابر آتش ضدهوایی و جنگنده‌ها حفاظت کند؛ اما افزودن زره به همه قسمت‌های هواپیما امکان‌پذیر نبود و سرعت آن را کم می‌کرد؛ بنابراین آنان باید تصمیم می‌گرفتند که به کدام قسمت‌های هواپیما زره بیفزایند. برای این منظور آنان شروع به جمع‌آوری داده کردند. پس از هر مأموریت، هواپیماهایی

عدم گنجاندن مرحله‌ای با عنوان روش استدلال، در ضمن مراحل تحقیق، به عدم شفافیت تحقیق منجر خواهد شد. به گونه‌ای که هر پژوهشگری به خود حق خواهد داد تا در معرض قرار دادن برخی متغیرهای دلخواه، نتیجه پژوهش را آن گونه که می‌خواهد جهت دهد. به عنوان نمونه، پژوهشی که موضوع خود را نقش عقل در تفسیر قرآن می‌نهد؛ سعی می‌کند با تاکید بر متغیرهای مورد نظر خود این نقش را در حداکثر سعه موضوع خود نمایان می‌کند. مثلاً نمونه آیات قرآن یا نمونه مفسران را به گونه‌ای انتخاب کند که عنوان خود را برجسته کند. جالب آن که پژوهش دیگری مبتنی بر متغیرهایی دیگر و چه بسا حتی مبتنی بر همان داده‌های قبلی، نتایج دیگری می‌گیرد. در واقع یک دسته داده ثابت دو خروجی متفاوت دارد.

در واقع هر محقق سؤال پژوهش خود را تنها بر اساس متغیرهای انتخابی و دلخواه خود ارزیابی کرده و نتیجه آن را اعلام می‌کند و مثلاً هیچگاه اعلام نمی‌کند که من در تحقیق خود به متغیرهای کذا و کذا توجهی نداشته‌ام یا مثلاً خروجی بررسی داده‌ها بر اساس متغیرکذا، صفر بوده است و خروجی نداشته است. نمونه بارز این خلاء را در فقه و در مقام یاس فقیه از دسترسی به ادله و استفاده از اصول عملیه دانست. اما واقع آن است که پردازش بدون داشتن معیارها و متغیرهای متناسب، پردازشی ناقص خواهد بود. ملاک قضاوت ما نسبت به نتایج یک تحقیق به همان میزان که به ارزش سؤال تحقیق بستگی دارد؛ به متغیرهایی بستگی دارد که سؤال تحقیق در بوته آن آزمایش شده اند.

یکی از ویژگی‌های پژوهش ماهیت جمعی بودن آن است. در جامعه عمل پوشیدن به این ویژگی تحقیق، باید دخالت متغیرهای دخیل در نتیجه پژوهش را نمایه سازی و استانداردسازی کرد. در واقع چه بسا ظاهر یک تحقیق نشان از سعی و پشتکار محقق دهد اما به جهت این که پژوهشگر سعی نکرده روش خود را تقریر کند و مسیری که وی را به چنین نتیجه‌ای رسانده به صورت ملموس نشان دهد؛ پژوهشی ابتر است. در صورتی که این اتفاق نیفتد ممکن است محقق دیگری تحقیقی متضاد با این تحقیق طراحی کند و کسی هم متوجه اشکال کار نشود. سوگیری بازماندگی، از این جهت آسیب جدی یک پژوهش است. سوگیری بازماندگی به معنای دخالت دادن متغیرهای روی پیشخوان ذهن پژوهشگر است و نه همه متغیرهای دخیل.

۲.۲ فراموشی مبانی

یکی از نکات مهم در استدلال، توجه به مبانی و پیش‌فرض‌هاست. مگر ممکن است در فضای خلا و بدون توجه به مبانی استدلالی فراهم آید؟ قطعاً هر استدلالی باید از جهت میزان پایبندی استدلال به مبانی آزموده شود. این که مثلاً با استناد به یک آیه قرآن یا یک فرمایش معصوم، فردی به نتیجه لزوم مذاکره یا لزوم جنگ با مخالفان برسد؛ از نتایج چنین غفلتی است.

را که بازگشته بودند به‌دقت بررسی می‌کردند و تعداد آسیب‌های ناشی از ترکش‌ها و گلوله‌ها و جای آن‌ها را روی هواپیما مشخص می‌کردند. به‌تدریج معلوم شد الگوی خاصی در توزیع آسیب‌ها روی هواپیما وجود دارد. بر این اساس کارشناسان نظامی نتیجه‌گیری کردند که قسمت‌هایی که بیشترین گلوله‌ها به آن اصابت کرده، نیازمند زره حفاظتی بیشتری هستند. در نگاه اول، این نتیجه‌گیری درست به نظر می‌رسد اما خطای مهمی در تحلیل‌ها صورت گرفته بود؛ چراکه نتیجه‌گیری تنها بر اساس داده‌های هواپیماهایی است که از مأموریت بازگشته‌اند؛ اما در مورد هواپیماهایی که در طول مأموریت سقوط کردند، چه می‌دانیم؟ اتفاقاً برعکس، آن قسمت‌هایی از هواپیما نیاز به حفاظت دارند که کمترین اصابت را داشته‌اند. درواقع نقاط آسیب در هواپیماهای بازگشتی بیانگر آن است که اگر هواپیما در این نقاط هدف قرار داده شود، با احتمال بیشتری می‌تواند سالم بازگردد.

احیانا در بسیاری از تحقیق‌ها مشاهده می‌شود که ارتباط بدنه اصلی پژوهش با مبانی روشن نیست. امروزه نه تنها ارتباط بسیاری از پژوهش‌ها با مبانی آشکار و پنهان مشخص نیست بلکه بسیاری از آن‌ها در اثر غفلت، مورد فراموشی قرار می‌گیرد. به عنوان نمونه، محقق، هنگام سخن از رابطه عقل و نقل، بر این باور است که اساساً عقل یا در بحث‌های اصولی و فلسفی به مبنایی قائل می‌شود ولی در عمل در فضای فقه یا حدیث و تفسیر بدان پایبند نیستند. در این میان پژوهش‌های فردی - نه جمعی – به آسیب‌زایی این روش بیشتر دامن می‌زند.

یکی از مباحث درازدامن در فقه، بحث تعارض ادله نقلی است. این تعارض در قالب‌هایی چون تخصیص، تخصص، ورود و حکومت خود را نشان داده است. امروزه فاصله گرفتن ما از زمان صدور، نوع جدیدی از تعارض را موجب شده است. تعارض این ادله با مبانی و ادله غیرلفظی دیگر. در واقع علت آن است که بسیاری از مبانی، به دلیل گسترش موضوعات از متون فاصله گرفته است. مثلا تعارض قوانین مدنی با قوانین فقهی (مانند تعارض سند و بینه) در مورد همه پژوهشگران اینگونه نیست که مبانی ایشان به نوعی رسوخ در روش آن‌ها پیدا کند، از این رو ممکن است بین صدر و ذیل کلامشان هماهنگی نباشد.

۳.۲ جستجوهای لفظی

متاسفانه، یکی از نتایج ناگوار مرحله اول و رهاوردهای فراوری متون، شکل گیری پژوهش‌های سطحی مبتنی بر جستجوهای لفظی است. جستجوهای لفظی، آسیبی جدی در مسیر پژوهش وارد کرده است. مثلاً اینکه محقق با جمع‌آوری واژه «شاب» در کلمات یک امام، به اهمیت جایگاه جوان در جامعه پرداخته و از آن به موارد زیر استدلال کرده است:

۱. **پیشینه تفسیر روایی**
۲. **عدم حجیت عقل در تفسیر**
۳. **مذمت تفسیر به رأی**

در فاصله گرفتن از آسیب نتایج جستجوهای لفظی، به عنوان نمونه، یکی از ملاک‌های مهم در تحلیل هر متن، توجه به غرضی است که متن به خاطر آن تولید یا نقل می‌شود. این مسئله در مورد تفسیر آیات قرآن کریم و به ویژه مفسران معاصری چون علامه طباطبایی (ره) که قائل به وحدت غرض سور قرآن هستند؛ حائز اهمیت است. بر همین اساس چه بسا مثلاً موضوع آیات سوره شعرا، قصه حضرت موسی (ع) باشد؛ اما غرض این سوره امر دیگری چون دلداری پیامبر (ص) باشد. پر واضح است که غرض کاملاً بر متن سایه می‌اندازد و محتوای متن، در همان راستا تحلیل می‌شود. می‌توان گفت مدخلیت غرض به حدی در شناخت معنای کلام دخالت دارد که تا غرض کلام، استخلاص نشود؛ تحلیل متنی کلام، فرآیندی ابتر خواهد بود (اذا عرفتم معانی کلامنا).

۳ نمایی از الگوریتم پیشنهادی

هوش مصنوعی (Artificial Intelligence) خواسته یا ناخواسته آینده علوم انسانی را متحول خواهد کرد و آن را از نزاع صوری میان مفاهیم عبور خواهد داد. بر اساس تحقیق بونیه، بازنمایی نمادین، روش اکتشافی و بازنمایی معرفت، از ویژگی‌های هوش مصنوعی اند که مبتنی بر هرنوع داده‌ای حتی داده‌های ناقص یا حتی متناقض نیز عمل خواهد کرد و عملاً دوقطبی اخبار جعلی و غیرجعلی را به عنوان دغدغه اصلی تحقیقات دینی، از بین خواهد برد. علم جبر که توسط خوارزمی ابداع شد در واقع روشی برای علم هندسه و ... بود. در واقع نوعی علم آلی بود. امروزه نیز با وجود روی‌کار آمدن انبوه نرم‌افزارها، اما نیازمند یک روش مانند هوش مصنوعی هستیم. مهمترین ویژگی در طراحی این الگوریتم استدلال که متناسب با دغدغه‌های فعلی علوم متن محور باشد؛ عبارتند از:

۱.۳ زبان شناسی تاریخی

به نظر می‌رسد که در عین این‌که استناد به گزارش‌های‌تاریخی، امری متداول در اثبات مسائل دینی شمرده می‌شود؛ اما صرف‌نظر از مبانی، روش‌های روشنی نیز در این استناد وجود ندارد. پله اول در مواجهه با یک متن در ساختار، محک‌زدن فهم صحیح است نه واکاوی اصالت متن. مشکل تعدد فهم و بدفهمی، بیش از آن که معلول تاریخی‌بودن متن باشد؛ ناشی از عدم توجه به زبان‌شناسی است. چنانچه صرف یادگیری زبان گویش یک کشور، ضرورتاً به معنای شناخت فرهنگ آن نیست؛ داننده گزارش‌های تاریخی نیز ضرورتاً یک تحلیل‌گر نخواهد بود. «زبان‌شناسی تاریخی» (Historical Philology) یا فنّ مواجهه با متون تاریخی، حوزه‌ای مهم در الهیات تاریخی و حلقه مفقوده «الهیات تاریخی» اسلامی است. این حوزه که مبتنی بر بررسی تغییرات تاریخی زبان به‌عنوان تکمیل‌کننده عوامل دخیل در فهم متن است؛ پاسخگوی بخش قابل‌توجهی از سؤالات مورد اشاره است. زبان‌شناسی باید به عنوان بخشی از علوم قرآنی و علوم حدیث، دیده شود. واقعیت آن است که مقوله استدلال در علوم متن‌محور، عمدتاً بر استناد و در علوم قرآن و حدیث، به صورت مشخص بر استناد به آیات قرآن و احادیث و گزارش‌های تاریخی استوار است. اما آن چه معمولاً مشاهده می‌شود این است که این استدلال‌ها معمولاً بدون هیچ تبیینی رها می‌شوند. در حالی که در مورد متون هر یک از موارد استناد، ضروری است تا شیوه استناد، روشن و استدلال، تبیین گردد.

به عنوان نمونه لزوم اتخاذ رویکردی تاریخی، یکی از اصول مهم در تحلیل اصطلاحات تاریخی در حوزه پژوهش‌های دینی است. معمولاً ذهن پژوهشگر برای پررنگ نشان‌دادن پیشینه یک اصطلاح، سعی دارد تا بدون توجه به تمایز کاربرد اصطلاحی و غیراصطلاحی یک واژه و صرفاً با جمع‌آوری هرگونه کاربردی از واژه، به قطور کردن پیشینه معنای اصطلاحی واژه مورد نظر کمک برساند. اما باید دید امکان استصحاب تاریخی معنای لغوی واژه برای رسیدن به معنای اصطلاحی، چه بهره‌ای از مشروعیت از نظر دانش زبان‌شناسی تاریخی دارد؟

در تحلیل تاریخي اصطلاحات توجه داشت که اصطلاح، یک بسته معنايي حاوي یک مفهوم چند ضلعي تخصصي است که به صورت قراردادي و در ضمن یک وضع ثانوي ایجاد شده است و امکان اجتهاد لغوي و

توسعه وتضییع معناي آن وجود ندارد. از سنخِ «بسته يِ معنايي»بودن اصطلاح، مانعي در اجراي روش تعميم و تسري معناي لغوي به اصطلاحي و همين طور موجب غيرمنطقي‌شدن تحليل آن بر اساس «تحليل لغوي» است. خروجي اصل فوق، عدم امكان اجتهاد در مورد اصطلاحات تاريخي است.

لزوم ارتباط بخشی متون با شبکه تاریخی واژگان یک ضرورت مهم در تحلیل متون است. در مطالعات دینی از این جهت که با واژگان تاریخی مواجه هستیم؛ ارتباط واژگانی در یک دوره خاص، اهمیت بیشتری می یابد. مثلا اینکه کاربرد کلمه تاویل در قرن دوم و سوم، ناظر به تفسیر است؛ اهمیت دارد و پژوهشگر نمی تواند این معنا را به بهانه کالبدشکافی معنای لفظ، به کل ادوار تاریخی تسری دهد. فکر کردن روی این روایت که: ازری بنفسه من استشعر الطمع، آن است که:

۱. این کلام از یک معصوم است. به زبان عربی است. کلام در منتهای بلاغت است.

۲. متغیرها عبارتند از این که: مخاطب کلام کیست؟ منابع لغوی، تطور تاریخی لغت، خانواده حدیث، مشابهت لفظی مشابهت معنوی؟

۲.۳ امکان ارتقا و تولرانس متغیرها

اگر پیش‌فرض‌ها و متغیرها را به کامپیوتر بدهیم، کامپیوتر بر اساس داده‌ها به نتیجه واحد می‌رسد. علت اینکه انسان‌ها هرکدام به نتیجه‌های متفاوتی می‌رسند، آن است که هرکدام از آن‌ها بر اساس منطق خود به تجزیه و تحلیل می‌پردازند. در واقع، پردازش کامپیوتر دقیق‌تر است چون همه متغیرها را دخیل می‌کند. اگر تفکر بشر یک روز حدیث: اقوام معمقون را به مفهوم عمیق معنا می‌کند، فردا می‌فهمد که به مفهوم دیگری است. چرا که متغیر خاصی (تطور معنایی) را دخالت نداده است. یک کسی از یملا الارض قسطا و عدلا علامت بودن می‌فهمد یکی شرط بودن یکی می‌گوید باید ظلم کرد یکی ... چون منطق تحلیل واحد وجود ندارد.

به این منظور لازم است نرم‌افزاری را که طراحی می‌کنیم که می‌تواند پیوسته ارتقا پیدا کند (بر اساس پیش‌فرض‌های جدید و متغیرهای جدید)، اما آن چه مهم است یک نفر به جای همه و با یک استاندارد خاص فکر می‌کند نه چند نفر. اکثر مقالاتی که مدعی نوعی نوآوری اند به دلیل فهم جدید ایجاد شده در مورد متن تاریخ است که در واقع اگر این گزارش به دل این کامپیوتر داده شود؛ جواب ثابت است حداکثر آن است که اگر متغیری داده ندارد، می‌گوییم داده ندارد نه این که آن را در نظر نگیریم.

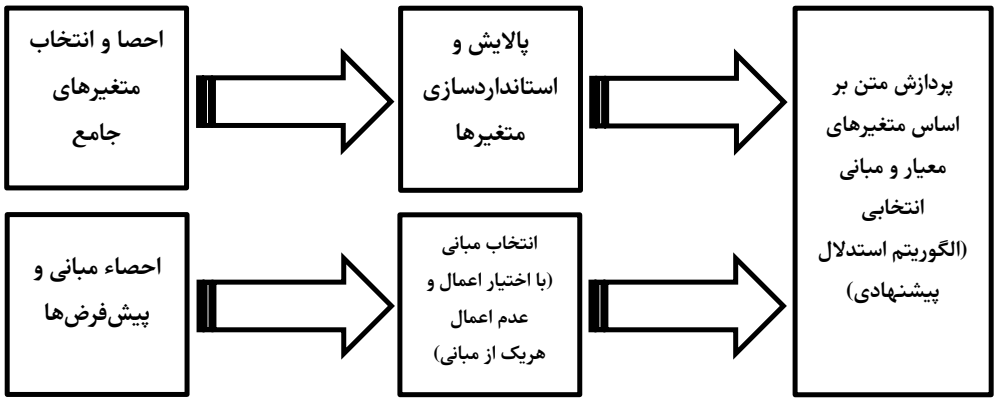
و باز از همین رو لازم است تا در الگوریتم پیشنهادی طراحی شده، هوش مصنوعی بتواند خود اقدام به برچسب و عنوان‌زنی برای متون فارغ از ماهیت الفاظ آن کند. هوش مصنوعی باید بتواند خود غیر از برچسبی که کتاب به متن زده است؛ عنوان یا عناوینی برای آن تعریف کند. مثلاً چه بسا روایت در مورد الف است اما موضوع آن را تشخیص دهد.

۳.۳ ماهیت خود ترمیمی متن

اساسا به صورت ذهنی و عملی دو روال کلی در تحلیل متن وجود دارد. نخست، رویکرد از جزء به کل و دوم، رویکرد از کل به جزء. رویکرد نخست، همان رویکرد رایج معناشناسی (Logical Semantics) است. در این

رویکرد که به شدت در محافل بومی رایج است؛ فهم مفردات، مقدمه ای بر فهم ترکیبات و نهایتا فهم جمله و کلام است. البته غیرقابل انکار است که این رویکرد – حداقل در نگاه نوپدید آن – نیز به شدت به نقش سیاق – با همه انواع آن – در فهم کلام ملتزم است. رویکرد دوم که رویکرد مختار ماست، فهم کلام را ترکیبی از فهم اجزای کلام نمی‌داند. در این رویکرد برای فهم معنای متن باید از کل به جزء رسید. برای رسیدن به این مقصود، اولویت دادن به سیاق کلام و مراد مولف است. اساسا تا خمیرمایه ای از اراده مولف در ذهن مخاطب جا نیفتد؛ کلمات بسان الفاظی مهمل هستند که در کنار هم آمده‌اند. از این منظر، تحلیل هایی که بر تحلیل لغوی متن تکیه می‌کنند؛ تلاش هایی پسینی و خارج از حوزه زبان‌شناسی به مفهوم Philology است بلکه این نوع تلاش‌های زبانی، از نوع Linguistic است. البته در شناخت علت رسوخ این رویکرد در میان تحقیقات بومی نباید نوع نگرش منطق‌دانان مسلمان به زبان را نادیده گرفت. هویت بخشی به لفظ بدون کاربرد، شالوده این نگرش است.

بنابراین خود متن نیز قابلیت تولید محتوا دارد. (سطح دوم و تحلیل انعکاسی) به عبارتی دیگر خود متن می‌تواند ابزار فهم خود باشد. مثلاً معانی برخی الفاظ جمله، از طریق کلمات همجوار به دست می‌آید. به عنوان نمونه مخاطب این متن که کرونا، جان بیست نفر را گرفت؛ می‌فهمد که کرونا، یک ویروس است و لزومی ندارد در کتب لغت به دنبال معنای واژه جان گرفتن، قتل و قاتل و جنگ و ... باشد.



۴ نتیجه

یکی از نتایج به کارگیری هوش مصنوعی در استناجات آن است که نتایج تحقیقات تا حدود زیادی از وحدت رویه برخوردار خواهد شد و از انجام تحقیقات سلیقه‌ای جلوگیری خواهد شد. استفاده از هوش مصنوعی، مفهوم پژوهش را متحول خواهد کرد و بسیاری از پژوهشگران نیز عملاً از صحنه پژوهش حذف خواهند شد. پژوهش‌ها صرفاً به طراحی جدید الگوهای استنتاج و تقویت مدل‌های جدیدتر استنتاج منتهی خواهد شد. در این فضا اگر نقدی هست به این سامانه الگوریتمی است نه یک پژوهش مشخص. نتیجه تدوین چنین الگوریتمی آن خواهد بود که هر سؤال پژوهشی صرفاً باید بر اساس متغیرهای تعیین شده در الگوریتم، به فرضیه خود نزدیک شود. در مباحث فقهی این مسئله اهمیتی مضاعف می‌یابد. چه آن که تغییر مبانی یک

فقیه یا جابجایی آن‌ها موجب تغییر فتوا خواهد شد. رسیدن به الگوریتم استدلال قطعاً یکی از اولویت‌های پژوهش در علوم انسانی به خصوص علوم اسلامی میان رشته‌ای در افق آینده پژوهی است.

مراجع

[۱] احمدی، محمدحسن، زبان‌شناسی تاریخی در مطالعات حدیثی، دانشگاه قم، ۱۳۹۷.
[۲] بونیه، الان، الذکاء الاصطناعی، واقعه و مستقبله، ترجمه علی صبری فرغلی، کویت: عالم المعرفه، ۱۹۹۳.
[۳] سبحانی، جعفر، الموجز في اصول الفقه، مکتبه التوحید، ۱۴۲۰.
[۴] شیخ انصاري، مرتضي، فرائد الاصول، مجمع الفکر الاسلامي، ۱۴۲۳.
[۵] طباطبائی، سیدمحمدحسین، المیزان‌في‌تفسیرالقرآن، بیروت: الأعلمي‌للمطبوعات، ۱۳۹۳ق.
[۶] طبری، محمدبن‌جریر، جامع البیان عن تاویل آي القرآن، بیروت: دارالمعرفة، ۱۳۹۲ق.
[۷] طوسی، محمدبن‌حسن، التبیان في تفسیرالقرآن، بیروت: دار احیاءالتراث العربي، بي‌تا.
[۸] کلیني، محمدبن‌یعقوب، الاصول من الکافي، دارالکتب الاسلامیة، ۱۳۶۳.
[۹] مجلسي، محمدباقر، بحار الانوار، بیروت: موسسة الوفا، ۱۴۰۳ق.
[۱۰] مینایی، بهروز، هوش مصنوعی در علوم اسلامی، جزوه موسسه اشراق و عرفان، ۱۳۹۸.

جایگاه شبکه ملی اطلاعات در ایران بر اساس حقوق بین‌المللی ارتباطات

سید محمد علی مرتضوی شاهرودی[1]

[1]دانشجوی کارشناسی ارشد علوم ارتباطات اجتماعی، دانشگاه صدا و سیما
m.shahroudy90@gmail.com

چکیده

تکنولوژی ارتباطی در حال توسعه است و نقش دولت در کنترل امور، به‌ویژه جریان اطلاعات، روز به روز ضعیف‌تر می‌شود. فضای سایبر به دلیل پیشرفت ارتباطات و فراگیر شدن آن در سراسر جهان، به یک مسئله مهم تبدیل شده است. این فضا همچنین، همراه با مزایای فراوان، در بردارنده آفت‌ها و سوء استفاده‌هایی نیز است. فضای مجازی سبب دگرگونی ریخت جامعه و اخلال در نظام ارزشی، گسترش جاسوسی نوین و توسعه نبردهای هیبریدی شده و از این جهت، تهدیدات امنیتی جدی را شکل داده است. تضمین استقلال و امنیت کشور در فضای سایبر بسیار حائز اهمیت است که به تحقق شبکه ملی اطلاعات در سه بعد زیرساخت، سرویس و محتوا وابستگی دارد. بسیاری از کشورهای صاحب قدرت سایبری برای مدیریت فضای سایبر خود مبادرت به طراحی و اجرایی نمودن شبکه ملی اطلاعات بومی نموده‌اند. در این پژوهش، با استفاده از روش تحقیق کیفی و توصیفی- تحلیلی، به تبیین مؤلفه‌های مطلوبیت استقرار شبکه ملی اطلاعات در کشور با استفاده از تجربیات سایر کشورهای پیشرفته مثل روسیه و چین و کشورهای حامی حقوق بین‌الملل ارتباطات پرداخته شده است. در این مقاله، به بررسی این مسئله پرداخته شده است که آیا حقوق بین‌الملل ارتباطات می‌تواند به تمام نیازهای کشورها از جمله جمهوری اسلامی ایران در حفظ و صیانت سایبرنتیک پاسخ دهد یا نیازمند قوانین داخلی هستند؟ به طور کلی، تحقیقات در این حوزه نشان می‌دهد که حفاظت از فضای سایبر برای حفظ امنیت و استقلال کشورها بسیار حائز اهمیت است و تحقق حکمرانی این فضا برای مدیریت کلان جامعه دارای اهمیت حیاتی است.

کلمات کلیدی: شبکه ملی اطلاعات، اینترنت ملی، حقوق بین‌الملل ارتباطات، آزادی بیان.

۱ مقدمه

در کنار حقوق داخلی ارتباطات در دهه‌های اخیر، در سطح جهانی مقررات مختلفی از سوی سازمان‌های بین‌المللی و به‌ویژه «مجمع ملل متحد»، «یونسکو»، «اتحادیه بین‌المللی ارتباطات دور» و سازمان جهانی مالکیت معنوی و همچنین برخی سازمان‌های منطقه‌ای مانند «شورای اروپا»، «اتحادیه اروپایی»، «پیمان

همکاری و امنیت اروپا»، «سازمان کشورهای آمریکایی و سازمان وحدت آفریقا» مقررات بین‌المللی و منطقه‌ای که در قالب قطعنامه‌ها، اعلامیه‌ها، عهدنامه‌ها و رهنمودهای حقوقی پدیدآمده‌اند که برای توسعه و تحکیم حقوق بین‌المللی ارتباطات به‌عنوان یک شاخه جدید حقوق بین‌الملل موقعیت مناسبی فراهم ساخته‌اند [۹، معتمدنژاد ۱۳۸۸: ۴۴] که در ارتباط نوین و ارتباط بین انسان‌ها توسط متخصصین بسیاری مورد ارزیابی قرار گرفته است.

فضای مجازی به‌عنوان یک تمدن جدید، بدون قلمروی مشخص و حکومتی متعارف، در دنیای امروز وجود دارد. به همین دلیل، حکمرانی بر فضای مجازی یکی از چالش‌های بزرگی است که پیشروی حاکمیت‌ها قرار دارد. برای موفقیت در این حوزه، نیازمند کسب شناخت صحیح از این پدیده و مواجهه فعالانه با آن هستیم. در واقع، در استفاده یا عدم استفاده از فضای مجازی، هیچ‌گونه حق انتخابی وجود ندارد. به همین دلیل، بهترین گزینه برای ما، بهره‌گیری از فرصت‌ها و پرهیز از تهدیدات آن است. برای مدیریت فضای سایبر خود، بسیاری از کشورهای صاحب قدرت، شبکه ملی اطلاعات بومی خود را طراحی و اجرایی نموده‌اند. شبکه ملی اطلاعات به‌عنوان زیرساخت ارتباطی فضای مجازی کشور شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده است به صورتی که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داد داخلی نگهداری می‌شوند به‌هیچ‌وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت، خصوصی و امن داخلی در آن فراهم شود (مرکز ملی فضای مجازی ۱۳۹۲).

باتوجه‌به فراگیرشدن فضای مجازی و تأثیر آن بر جوامع و به‌ویژه کشورمان، حکمرانی این فضا برای مدیریت جامعه دارای اهمیت حیاتی است. به‌منظور مدیریت صحیح فضای مجازی و ارتقاء حکمرانی آن در کشورمان، طراحی کلان شبکه ملی اطلاعات و بهره‌برداری از آن ضروری است. عدم استقرار شبکه ملی اطلاعات، نظام مدیریت این فضا را ناکارآمد و تهدیدات سیاسی، اجتماعی، اقتصادی و... را بیشتر خواهد کرد.

در این مقاله سعی در این است که ثابت شود داشتن اینترنت ملی و محدودیت‌ها در فضای سایبر خلاف حقوق بین‌الملل نیست، به همین علت در ابتدا حقوق بین‌الملل ارتباطات و آزادی بیان که اصلی‌ترین بحث در حقوق بین‌الملل ارتباطات هست را توضیح داده و بعد قرائنی آورده می‌شود که محدودیت‌ها در فضای سایبر و داشتن اینترنت ملی در برخی کشورها حتی کشورهای مبدع و مدعی آزادی بیان، مسئله حل شده‌ای هست و بعد به مسئله استیضاح تیک‌تاک پرداخته می‌شود که این کار خلاف حقوق بین‌الملل ارتباطات دانسته نمی‌شود و برای این مسئله دلایل خود را دارند و بعد از اینکه ثابت شد که هر محدودیتی در فضای سایبر خلاف حقوق بین‌الملل ارتباطات نیست، وارد بحث اینترنت ملی ایران شده و ثابت می‌شود که اینترنت ملی ایران خلاف حقوق بین‌الملل نیست و امری لازم است.

۲ پیشینه پژوهش

کاظم معتمدنژاد (۱۳۸۳) در کتاب ایران و اجلاس جهانی سران درباره جامعه اطلاعاتی، کاظم معتمدنژاد (۱۳۸۸) در کتاب حقوق ارتباطات، و حافظ محمدی (۱۳۹۹) در پژوهش شبکه ملی اطلاعات و تحقق حکمرانی سایبری در جمهوری اسلامی ایران با رویکرد تجربه کشورها که به تعریف علوم ارتباطات و آزادی

بیان و شبکه ملی اطلاعات در سایر کشورها پرداخته‌اند؛ اما مشخص نکردند که این شبکه ملی اطلاعات ایران ناقض این حقوق هست یا نه مقاله در صدد این است که ثابت کند در شرایط فعلی که فضای سایبر نقش مهمی در حاکمیت کشورها دارد آزادی بی‌قیدوشرط این فضا از نظر هیچ کشور و حاکمیتی و تحت هیچ حقوقی درست نمی‌باشد.

۳ حقوق بین‌المللی ارتباطات

رشته‌ی حقوق را می‌توان رشته‌ای مادر دانست که بنا به نیازهای جامعه انشعابات گوناگونی چون حقوق خصوصی، حقوق جزا، حقوق بین‌الملل، حقوق عمومی و رشته‌های جدیدی چون حقوق اقتصادی، حقوق تجارت بین‌الملل و حقوق ارتباطات را شکل داده است.

در حقیقت در جهان امروز هیچ علمی به‌صورت محض و مجزای از علوم دیگر چندان کاربردی نخواهد بود و باید عصر جدید در علوم را عصر علوم میان‌رشته‌ای توصیف کرد، علم حقوق نیز از این قاعده مستثنی نیست، چراکه قوانین و مقررات و چالش‌های حقوقی به سبب گسترش جوامع و روابط اجتماعی آن‌چنان گسترده شده است که دیگر یک حقوق‌دان نمی‌تواند بر همه‌ی حوزه‌های این علم احاطه داشته باشد و باید رشته‌ی خاصی را در حقوق انتخاب کند و عمق اطلاعات خود را در آن حوزه افزایش دهد.

در این میان حقوق ارتباطات از اهمیتی خاص و ویژه برخوردار است، چراکه با مهم‌ترین علم بشر یعنی ارتباطات که منشأ و مبنای علوم گوناگون است پیوند خورده است. برخی حقوق‌دانان حقوق ارتباطات را حقوق رسانه دانسته‌اند؛ اما حقیقت آن است که حقوق ارتباطات بسیار فراتر از حقوق رسانه است و همه‌ی حوزه‌های ارتباطی از قبیل مخابرات، ارتباطات رادیویی و... را نیز در بر می‌گیرد.

در جهان درحال‌توسعه‌ی امروز، ورود فناوری‌های نوین به علم ارتباطات روزبه‌روز بر نزدیکی مردم در این دهکده‌ی جهانی می‌افزاید؛ لکن این ارتباطات نیازمند چهارچوب و قاعده‌گذاری‌های خاصی برای جلوگیری از سوءاستفاده احتمالی و نظم بخشیدن به این ارتباطات است و این مهم تنها از عهده متخصصین خاصی برمی‌آید که هم بر حوزه علم حقوق احاطه داشته باشند و هم از علوم ارتباطات بهره‌مند باشند. تغییروتحول و دگرگونی در علم حقوق ارتباطات بیش از هرکدام از رشته‌های حقوق است، چراکه وسایل ارتباط هر روز پیشرفت می‌کند و دچار تغییر و تحولات گوناگون می‌شود و متخصص این علم را وادار می‌کند که دانش خود را به‌روز نگاه دارد.

متخصصان حقوق ارتباطات، به دنبال طبقه‌بندی پروفسور «فرنان ترو»، بنیان‌گذار و استاد فقید انستیتوی مطبوعات دانشگاه پاریس درباره قلمرو این رشته جدید، حقوقی، پنج زمینه یا بخش مربوط به آن را مورد بررسی قرار می‌دهند

الف) مقررات حقوقی تأسیس و اداره مؤسسات ارتباطی
ب) مقررات حقوقی حاکم بر محتوا و انتشار (مندرجات، برنامه‌ها و پیام‌های ارتباطی)
پ) مقررات حقوقی حرفه روزنامه‌نگاری و حرفه‌های ارتباطی دیگر
ت) مقررات حقوقی مالکیت معنوی

ث) مقررات حقوقی بین‌المللی ارتباطات (ما در این مقاله با این شاخه کار داریم)

در شاخهٔ پنجم حقوق ارتباطات که به وضعیت حقوقی بین‌المللی ارتباطات اختصاص دارد مقررات حاکم بر تکنولوژی‌ها و فعالیت‌های ارتباطی، مورد بررسی قرار می‌گیرند این مقررات از طریق ابزارهای حقوقی توسط نهادهای بین‌المللی و منطقه‌ای متفاوتی مانند مجمع‌عمومی سازمان ملل، اتحادیه بین‌المللی ارتباطات دور، یونسکو، سازمان جهانی مالکیت معنوی شورای اروپا اتحادیه اروپایی و ... وضع شده‌اند و زمینه‌های گوناگونی را در بر می‌گیرند [۹، معتمدنژاد ۱۳۸۸: ۳۰].

در میان مقررات مذکور اصول راجع به آزادی بیان و اطلاعات و محدودیت‌های آن، از اهمیت ویژه‌ای برخوردار است و به همین مناسبت به آن می‌پردازیم.

۴ آزادی بیان

آزادی بیان از حقوق اساسی افراد در جامعه بشری محسوب می‌شود و در چارچوب حقوق بشر از جایگاه ویژه سیاسی و اخلاقی برخوردار است. آزادی بیان ابزاری جهت رساندن اندیشه و عقیده به دیگران است. حق برخورداری از آزادی بیان ریشه و مبنای بسیاری دیگر از آزادی‌ها همانند آزادی مطبوعات، حق دسترسی آزادانه به اطلاعات، حق انتقال و انتشار اندیشه‌ها، حق انتقاد، حق استقلال و رهایی از سانسور است.

آزادی بیان به‌عنوان یک حق مبنایی در اسناد بین‌المللی و منطقه‌ای حقوق بشر تصریح شده است. در بعد بین‌المللی، حق آزادی بیان در ماده ۱۹ اعلامیه جهانی حقوق بشر و بند ۲ ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی مورد شناسایی قرار گرفته است. در هر دو سند، حق آزادی بیان به‌عنوان حق افراد برای داشتن و ابراز نظر بدون دخالت دیگران و همچنین حق جستجو، به‌دست‌آوردن و بهره‌وری از اطلاعات و ایده‌ها تعریف شده است.

۱.۴ محدودیت‌های آزادی بیان

در بند ۳ ماده ۱۹ میثاق بین‌المللی مقرر شده است که حق آزادی بیان می‌تواند موضوع محدودیت‌های قانونی قرار گیرد، محدودیت‌هایی که برای احترام به حقوق و شهرت دیگران یا برای تأمین امنیت ملی، نظم عمومی و سلامت جامعه ضرورت دارد.

مهم‌ترین سند درباره آزادی بیان، کنوانسیون اروپایی حقوق بشر است، مطابق ماده ۱۰ این کنوانسیون، تمامی افراد بشر برای بیان ایده‌ها و نظرات خود بدون هیچ‌گونه سانسور یا دخالت از طرف دولت آزادند. موضوع آزادی بیان به طور خاص بیان‌هایی که باعث آزار و تبعیض یا باعث تحریک خشونت و دشمنی در مقابل دیگر افراد و گروه‌ها به‌وسیله اشاره به نژاد آنها، باور مذهبی، جنسیت یا گرایش جنسی آنها می‌شود را در بر نمی‌گیرد. دیوان اروپایی حقوق بشر بارها آزادی بیان را به‌عنوان یکی از مبانی جامعه دموکراتیک توصیف کرده؛ زیرا این اصل، حق هر فرد برای تبادل اطلاعات، مباحثه ایده‌ها و بیان نظرات را تضمین می‌نماید و توسعه هنری، علمی و تجاری در جامعه را پایه‌ریزی می‌کند.

برخورداری افراد از حق آزادی بیان در قوانین ملی اکثر کشورهای جهان نیز به رسمیت شناخته شده

است. شاید قوی‌ترین حمایت از آزادی بیان در قانون اساسی ایالت متحده آمریکا آمده است. در قانون اساسی آمریکا، ارزش آزادی بیان بر دیگر ارزش‌های دموکراتیک مثل برابری، احترام به شأن انسانی و حریم خصوصی ارجحیت دارد به‌نحوی‌که دیگر حقوق و ارزش‌های دموکراتیک نبایستی آزادی بیان را محدود کند. حمایت قانونی ارائه شده به آزادی بیان در ایالات متحده آمریکا نسبت به کشورهای دیگر جهان کم‌نظیر و یا حتی بی‌نظیر است. دیدگاه آمریکایی نسبت به آزادی بیان همیشه سازگار با هنجارهای حقوق بشر بین‌المللی و همچنین حمایت از آزادی بیان در دیگر کشورهای دموکراتیک جهان نبوده است. اگرچه هنجارهای حقوق بشر بین‌المللی و قوانین اساسی دیگر کشورهای دموکراتیک جهان، آزادی بیان را به‌عنوان یک حق مهم مورد شناسایی قرار می‌دهند لیکن آنان بر این باورند که این حق بایستی در مقابل دیگر حقوق دموکراتیک متعادل شود. به‌عبارت‌دیگر این کشورها محدودیت‌های معینی را بر آزادی بیان به رسمیت می‌شناسند [۳، زاهدی ۱۴۰۰: ۱۰۳] که در ادامه بیان خواهد شد، پس می‌بینیم که مهم‌ترین مسائل مطرح شده حقوق بین‌الملل ارتباطات گاهی در یک سری چارچوب‌هایی قرار دارد که می‌تواند بنا بر قانون هر کشور تغییر کند.

۵ قوانین چین در مواجهه با رسانه‌های جدید

کشور چین دامنه وسیعی از قوانین و مقررات مرتبط با رسانه دارد که از مدت‌ها قبل وضع شده‌اند طی زمان آنچه تغییر کرده خود مقررات نبوده، بلکه درجه اجبار این مقررات تغییر کرده است همچنین این قوانین و مقررات محدودیت‌های واقعی رفتاری نیستند، بلکه ابزاری برای حکومت چین هستند که متناسب با شرایط سیاسی از آنها کند.

در محتوای آنلاین چین معیارهای محتوای اینترنتی (ICP) (۲۰۰۰) دارد: منع، تولید بازتولید یا توزیع محتوای اینترنت درصورتی‌که مغایر با اصول پایه قانون اساسی باشد یا امنیت کشور را به خطر اندازد، اسرار کشور را افشا کند یا ...

مقررات ۲۰۰۸ برای مدیریت سرویس برنامه‌های صوتی و تصویری اینترنت، منع مواردی مانند مغایرت با اصول پایه قانون اساسی به خطر انداختن اخلاق اجتماعی یا سنن فرهنگی ملت، تشویق کم سن و سالان به تبهکاری، خشونت زیاد، هرزه، قمار و آدم‌کشی و...؛ مقررات SAPPRFT برای کنترل محتوای برنامه‌های صوتی و تصویری در اینترنت (۲۰۰۹) این مقررات پیش‌تر عنوان شد علاوه بر مفاد، بالا، محتواهای زیر باید ویرایش یا حذف شوند آسیب به فرهنگ تاریخ و وقایع تاریخی چین، آسیب به تاریخ سایر کشورها بی‌احترامی به تمدن بشری و فرهنگ و سنت سایر کشورها، اولین و مهم‌ترین موضوع تلاش برای ایزوله کردن چین از جهان خارج است و کنترل محتوای وب، بزرگ‌ترین موضوع امروز چین در حوزه محتواست. چین از آن دست کشورهایی است که در آن اینترنت بیشترین سانسور و کنترل را دارد و شاخه‌های متعددی از حکومت سازوکار پیچیده‌ای را برای رگولاتوری سانسور و نظارت بر فعالیت‌های اینترنتی به کار می‌برند وزارت امنیت عمومی و نیروی پلیس بر اینترنت نظارت می‌کنند. گاهی اوقات وب‌سایت‌ها به‌کلی قطع می‌شود و کاربران به گزارش‌های خبری برون‌مرزی دسترسی ندارند. گاهی موتورهای جست‌وجو کلمات حساس را شناسایی می‌کنند، در این مورد، هیچ وب‌سایتی برای جست‌وجوی موضوعات حساس عمل نمی‌کند. بسیاری

اوقات حتی کاربران به آدرس وب‌سایت‌های حکومتی ارجاع داده می‌شوند. همچنین حکومت وب‌سایت‌هایی به‌عنوان توقیف «شهروند» برای تشویق مردم به گزارش‌دادن پیام‌های غیرقانونی یا غیراخلاقی در وب تأسیس کرده است. در زمینه سرویس OTT (محتوای ویدئوی اینترنتی قابل‌مشاهده روی تلویزیون) نیز چندین رگولاتور با هم‌پوشانی وظایف وجود دارند که مهم‌ترین آنها SAPPRFT (در نقش رگولاتور انتقال و انتشار برنامه‌های صوتی و تصویری روی اینترنت) و MIIT (مجوزدهی سرویس‌های ارتباطات راه دور ارزش‌افزوده اینترنتی)، SIIO (رگولاتوری اخبار در اینترنت و نظارت بر محتوای آنلاین) و MOC (ارسال آنلاین محصولات فرهنگی در اینترنت شامل موسیقی و بازی) هستند. در این سرویس‌ها، رعایت دستورالعمل محتوایی الزام شده و الزاماتی برای تأمین‌کنندگان محتوای آنلاین برای خودتنظیم گری قرار داده شده است. همچنین در این سرویس، سرمایه‌گذاری خارجی اسماً ممنوع بوده و همچنین تأمین برنامه توسط شرکت‌های خارجی ممنوع است. تأمین‌کنندگان بومی نیز مطابق سیستم بازنگری واردات SAPPRFT، تنها مجاز به تأمین محتوای خارجی مشخص مانند نمایش و فیلم خارجی هستند [۴، سعیدی ۱۴۰۱: ۳۹].

چین جزو کشورهایی است که در کنار استفاده از اینترنت، سال‌هاست شبکه ملی خود را راه‌اندازی کرده است. گفتنی است چین در برابر هجمه سایبری آمریکا بیشترین مقاومت بین‌المللی را تاکنون از خود نشان داده است. به‌طوری‌که تاکنون بیشترین تعداد بازی‌های ملی رایانه‌ای، موتور جستجوی ملی، میل سرورهای ملی و از همه مهم‌تر سیستم‌عاملی ملی را طراحی کرده است. اخیراً دفتر اطلاعات شبکه اینترنت ملی چین اعلام کرده که استفاده کاربران از وبلاگ‌ها و دیگر خدمات این شبکه با نام‌های مجازی ممنوع است و کاربران باید در فضای مجازی از نام و مشخصات حقیقی خود استفاده نمایند. پروژه سپر طلایی که به‌صورت عامیانه از آن به‌عنوان فایروال عظیم چین نیز یاد می‌شود، یک پروژه جهت کنترل و مراقبت از اینترنت است که توسط وزارت امنیت عمومی چین اجرا می‌شود. اجرای این پروژه از سال ۱۹۹۸ آغاز شد. کنترل اینترنت در چین به دلیل طیف وسیعی از قوانین و مقررات اداری بسیار شدید است. بیش از ۶۰ درصد مقررات اینترنتی مربوط به دولت چین، توسط ISPها، شرکت‌ها و سازمان‌های دولتی اجرا می‌شود. نام «پروژه سپر طلایی» به طور اختصاصی و منحصراً به سیستم حفاظت اینترنت چین اشاره داشته و به‌عنوان فایروال بزرگ چین نیز شناخته می‌شود. بااین‌حال، برخی از کارشناسان حوزه فضای مجازی معتقدند که سپر طلایی و فایروال بزرگ، دو موجودیت جداگانه هستند که فایروال بزرگ یکی از چندین مؤلفه سپر طلایی چین است. برخی نیز معتقدند که پروژه سپر طلایی «چیزی بیش از یک دیوار آتش نیست». یک سیستم نظارت پیشرفته که به دولت این امکان را می‌دهد تا درخواست‌های جستجوی خاص را نظارت کند، فعالیت‌های کاربران اینترنتی را رصد و ردیابی کند [۷، محمدی ۱۳۹۹: ۸].

۶ فرانسه رتبه اول محدودیت اینترنت در اروپا

در فرانسه به دنبال پیروی انقلاب کبیر این کشور که ریشه‌دارترین و گسترده‌ترین انقلاب آزادی‌خواهی و دموکراسی طلبی غربی به شمار می‌رود، آزادی مطبوعات موردتوجه فراوان قرار گرفته است. در اعلامیه حقوق بشر و شهروند انقلاب فرانسه که در ۲۶ آگوست ۱۷۸۹ در پاریس انتشار یافت، برای نخستین‌بار،

تعریف‌های حقوقی دقیقی از آزادی به معنای اعم و همچنین آزادی ارتباطات به‌صورت عام و آزادی مطبوعات به‌صورت خاص ارائه و حدود آنها نیز مشخص شدند.

ماده ۱۱ اعلامیه راجع به آزادی ارتباطات و از جمله آزادی مطبوعات چنین پیش‌بینی کرده است:

«انتقال و انتشار آزاد افکار و عقاید، یکی از گران‌بهاترین حقوق انسانی است، بنابراین هر شهروندی می‌تواند آزادانه سخن بگوید، بنویسد و چاپ کند، مگر در مواردی که برای مقابله با سوءاستفاده از این آزادی، در قانون مشخص شده‌اند و قابل‌تعقیب‌اند»، فرانسه از سال ۱۹۸۸ یک سری مقررات کیفری مخصوص مبارزه با جرائم رایانه‌ای را وضع کرده است. در واقع تا این تاریخ هیچ نوع جرم‌انگاری خاصی که شامل بزهکاری مربوط به رایانه باشد در فرانسه وجود نداشت. پیش‌ازاین رایانه نه به‌عنوان یک عنصر جرم‌زا، بلکه به‌عنوان وسیله‌ای در خدمت ادارات که امکان طبقه‌بندی مجموع کارهای انسانی را فراهم می‌کرد تلقی می‌شد؛ ازاین‌رو هنگامی که پارلمان فرانسه در ششم ژانویه ۱۹۸۷ برای اولین‌بار اقدام به وضع قوانین در خصوص رایانه کرد آن را به تعریف جامع مقررات حقوقی رایانه و تنظیم آنچه علمای حقوق آن را منشور بزرگ حقوق بشر در مورد انفورماتیک نامیدند اختصاص داد. در این قانون که به قانون «انفورماتیک آزادی» نیز معروف است فناوری رایانه‌ای فقط به‌عنوان وسیله‌ای که می‌توان با آن حقوق افراد، به‌ویژه حق رعایت حریم خصوصی آنان را مورد تجاوز قرارداد در نظر گرفته شده بود نه به‌عنوان وسیله‌ای برای آسیب رساندن به اموال و دارایی‌های مردم؛ بنابراین تنها مقررات کیفری در خصوص رایانه که تا پایان سال‌های دهه ۱۹۸۰ در حقوق موضوع فرانسه وجود داشت، به زیر پا گذاشتن مقررات مربوط به حمایت از داده‌های شخصی افراد مربوط می‌شد تنها در سال ۱۹۸۸ یعنی دقیقاً ۱۰ سال بعد از تصویب قانون «انفورماتیک و آزادی»، پارلمان فرانسه متن قانونی دیگری راجع به محیط انفورماتیک به تصویب رساند. قانون ۵ ژانویه ۱۹۸۸ بنابه‌درخواست منتخبان مردم فرانسه در پارلمان که امیدوار بودند خلأ حقوقی را که تا آن زمان در حقوق فرانسه وجود داشت، پر کنند، به تصویب رسید. این قانون به‌عنوان قانون «گودفرن» برگرفته از نام نماینده‌ای که این طرح دوم را به مجلس ملی ارائه و از آن دفاع کرد، معروف شد. نتیجه اینکه جرائم رایانه‌ای از این تاریخ به بعد در مواد بند ۳۳۳ قانون جزای فرانسه در یک مبحث تحت عنوان جرائم علیه سیستم‌های پردازش داده‌ها موردتوجه قرار گرفت. در پارلمان فرانسه این طرح به‌عنوان یک متن صریح کوتاه، ساده و پاسخگوی نیاز زمان معرفی شده بود؛ بنابراین قانون گودفرن بر خلاف قانون انفورماتیک و آزادی هیچ اشتیاقی به تنظیم مقررات درباره انسانی که فعالیت‌های او به‌صورت انفورماتیک ارائه می‌شود ندارد؛ ازاین‌رو به نظر می‌رسد که این قانون تا اندازه زیادی شبیه یک متن ساده و موردی است [۴، سعیدی ۱۴۰۱: ۱۱۰].

طبق بررسی‌ها در اتحادیه اروپا فرانسه شدیدترین نظارت‌های حکومتی بر فضای مجازی را دارد و شهروندان حق جست‌وجوی برخی عبارات را ندارند. پرونده حکمرانی فضای مجازی اینترنت در فرانسه از سال ۱۹۹۴ در دسترس عموم قرار گرفت و در ابتدا فقط در معدود شرکت‌ها و دانشگاه‌ها در اختیار تعداد کمی از کاربران قرار گرفت، عموم مردم از سال ۱۹۹۴ به اینترنت دسترسی پیدا کردند و از اوایل دهه ۲۰۰۰ با ظهور ADSL دسترسی به طور گسترده فراهم شد.

در اتحادیه اروپا، فرانسه شدیدترین نظارت‌های حکومتی بر فضای سایبری را دارد طبق قانون‌های هادوپی و لوپسی مصوب سال ۲۰۰۹، کاربران ناقض قوانین شبکه از دسترسی به آن محروم می‌شوند و علاوه بر فهرست

بلندی از تارنماهای غیراخلاقی یا ایدئولوژیک مسدود، شهروندان حق جست‌وجوی برخی عبارات را ندارند. اینترنت مدارس نیز بسیار محدود هستند [۴، سعیدی ۱۴۰۱: ۱۱۱].

۷ بخش روسی اینترنت

روسیه مدعی است که مدیریت و حاکمیت بخش روسی‌زبان شبکه جهانی اینترنت بر عهده این کشور است. این ادعا، مبنی بر ایجاد زیرساخت مستقل منابع شبکه، از جمله DNS برای جلوگیری از تحمیل حاکمیت بر زیرساخت‌های شبکه RUnet در عین حفظ سازگاری با بقیه اینترنت جهانی است. نوع بیان و ادعای روسیه در تعریف بخش روسی اینترنت، حفظ سازگاری و همکاری با اینترنت جهانی بوده و براین‌اساس، نهاد نظارت فدرال روسیه با موتورهای جستجو و شرکت‌های Sputnik، Yandex، Google و Mail.Ru درخواست برقراری ارتباط داشته است. این اپراتورها به‌استثنای گوگل، با سیستم ارتباط برقرار کرده و الزامات قانونی را رعایت کردند. RUnet فرصت توسعه قوانین مرتبط با زیرساخت‌های مهم اینترنت را فراهم کرده و تلاش می‌کند تا امکانی را فراهم آورد تا در شرایط اضطراری یا خاموشی (متوقف‌شدن سیستم‌ها توسط کشورهای متخاصم)، مستقل از اینترنت کار کند. برای کاربران عادی، اصطلاح RUnet به معنی، دسترسی به خدمات و محتوای وب‌سایت‌ها برای کاربران روسی، بدون نیاز به مهارت‌های زبان خارجی است. به‌عنوان‌مثال موتورهای جستجوگر، خدمات پست الکترونیکی، آنتی‌ویروس‌ها، فرهنگ لغت روسی و ارائه‌دهندگان خدمات آنلاین که دارای یک دفتر در روسیه هستند . (از جمله شرکت‌های خارجی مثل آمازون، یوتیوب، PayPal، eBay و غیره). با وجود بسیاری از وب‌سایت‌های بین‌المللی باکیفیت بسیار بالا و جستجوگر گوگل که حدود ۱۰ سال از ساختار روسی پشتیبانی کاملی داشته، امروزه برخی از کاربران روسی علاقه‌ای به استفاده از خدماتی مانند فیس‌بوک یا گوگل‌مپ ندارند، زیرا خدمات بومی دارای ویژگی‌های خاص کشور روسیه و دارای جامعه محلی هستند. علاوه بر این، بسیاری از مقامات دولت روسیه به طور فعال از این اصطلاح به‌عنوان مترادف اینترنت در قلمرو روسیه یعنی زیرساخت‌های اینترنتی که تابع قوانین روسیه است (از جمله قوانین سانسور روسیه، کپی‌رایت، شرکت‌های بزرگ، قوانین تبلیغ و غیره) استفاده می‌کنند. ایده اصلی RUnet، یک اینترنت مستقل بوده که با شبکه سراسری کره شمالی که کاملاً از اینترنت جهانی جدا است، متفاوت است. این سیستم‌های اینترنتی مستقل، شباهت‌هایی به «شبکه چین» دارد. به‌ویژه از نظر کنترل جریان داده‌ها از داخل و خارج از کشور و هدف آن‌ها صرفاً کنترل دسترسی به اینترنت در یک منطقه جغرافیایی خاص نیست. بلکه هدف واقعی، تأمین ابزارهای لازم برای اعمال سطح حاکمیتی در حوزه دیجیتالی است که در دنیای فیزیکی نیز صورت می‌گیرد. در چنین شرایطی، دولت، کنترل مستقیم زیرساخت‌های اینترنت را در خاک خود به عهده می‌گیرد و به آن اجازه دفاع از سیستم‌ها در برابر حمالت خارجی باهدف تضمین تمامیت ارضی مشابه حوزه فیزیکی را می‌دهد. در حال حاضر، انجمن غیردولتی مستقر در ایالات متحده (ICANN) زیرساخت‌های پایه اینترنت جهانی را مدیریت می‌کند. برای کشورهایی مانند ایران، روسیه و چین، این وضعیت پر ریسک است، زیرا این سازمان هرچند مستقل از دولت آمریکا بوده، می‌تواند در برابر مداخلات واشنگتن آسیب‌پذیر باشد. در نهایت، مفهوم حاکمیت اینترنت مطلوب این کشور، بر این ایده وابسته است که باید در

ایجاد پایه‌های عملکرد اصلی اینترنت از طریق کنترل مستقیم بر سرورهای DNS که اساساً همه ترافیک را به‌صورت آنلاین هدایت می‌کنند، بین کشورها برابری ایجاد شود. البته برای روسیه این صرفاً تلاشی برای ایجاد برابری در زیرساخت‌های اینترنت نیست. مسکو با درنظرگرفتن تغییراتی در عملکرد RUnet، اهداف عملی‌تری را در ذهن دارد. با وجود اختلافات فزاینده بین مسکو و غرب و به‌ویژه با افزایش تمرکز در حوزه سایبر، روسیه نگران آسیب‌پذیری زیرساخت‌های داخلی خود در برابر حملات سایبری بزرگ خارجی است. ضمناً یک زیرساخت مستقل‌تر و توانایی حفظ مقداری از کارکردهای داخلی در هنگام قطع ارتباط با دنیای خارج، می‌تواند دفاعی بیهوده و درعین‌حال مؤثر را در برابر چنین تهدیدهایی فراهم کند. درعین‌حال، امنیت اطلاعات برای تلاش‌های مسکو درباره RUnet از اهمیت اساسی برخوردار است. باتوجه‌به ماهیت ذاتی اینترنت، مکاتبات آنلاین بین شهروندان روسی و اشخاص، اغلب زیرساخت‌های داخلی روسیه را مدنظر قرار نداده و این خطر را از نظر مسکو ایجاد می‌کند که قدرت‌های خارجی می‌توانند از این طریق، این ارتباطات را پالایش کرده یا در آن اختلال ایجاد کنند؛ بنابراین، با طراحی مجدد زیرساخت‌های اینترنتی خود برای مقابله با این‌گونه تهدیدات، مسکو همچنین درصدد است تا اطمینان حاصل کند که ارتباطات دیجیتال یا انتقال داده‌ها بین روس‌ها، زیرساخت‌های داخلی این کشور را ترک نمی‌کند [۷، محمدی ۱۳۹۹: ۶].

۸ حق دسترسی به اینترنت در آمریکا

بی‌طرفی اصطلاحی است که نخستین‌بار در سال ۲۰۰۰ از سوی کمیسیون فدرال ارتباطات آمریکا در مورد بی‌طرفی نسبت به داده‌های در حال جریان به کار رفت و سپس با توسعهٔ مفهومی، به کل زنجیرهٔ ارزش در اینترنت تسری یافت.

به‌موجب این اصل باید با بسته‌های داده به نحو برابر و بدون تبعیض بر اساس نوع برنامهٔ کاربردی، محتوا و مقصد آنها رفتار شود به‌گونه‌ای که کاربران اینترنت حق جست‌وجو و گردش در شبکه و انتخاب وب‌سایت‌ها، برنامه و خدمات اینترنتی و بیشترین امکان دسترسی به محتوای اینترنت محور را داشته باشند.

اصل بی‌طرفی اعمال اصل کلی منع تبعیض در ارتباطات اینترنتی را دنبال می‌کند. طبق این اصل، کاربران باید بتوانند هر نوع فناوری و برنامهٔ کاربردی را به کار گیرند و به سرویس‌های موردنظر خود دسترسی داشته باشند، بدون آنکه ترافیک مربوط به آن برنامه یا خدمات از سوی اپراتورهای شبکه، موتورهای جست‌وجو و دیگر بازیگران اینترنت جهت‌دهی یا اولویت‌بندی شود. همچنین، ترافیک اینترنتی نباید به طور تبعیض‌آمیز مسدود شود، مگر اینکه برای حفظ امنیت شبکه لازم و متناسب باشد؛ تبعیض در دسترسی به اینترنت ممکن است به دلایل و توجیهات فنی (نبود پهنای باند و زیرساخت‌های فنی لازم برای اینترنت جهانی و پرسرعت)، اقتصادی (عدم تنظیم قواعد رقابت بین ارائه‌دهندگان خدمات دسترسی)، اجتماعی (عدم احترام به ترجیحات و انتخاب‌های مصرف‌کنندگان اینترنت و مواجه کردن آنها با انبوه اطلاعات خواسته و ناخواسته) و حقوقی (مدیریت قراردادهای ارائهٔ خدمات و نبود حمایت‌های لازم از کاربران در برابر شروط اجحاف‌آمیز) صورت گیرد.

براین‌اساس، اصل بی‌طرفی آثار و مزایای زیادی بر کاربران اینترنت دارد؛ از جمله اینکه به تحقق شفافیت،

تنوع و تکثر در اینترنت (در برابر تمرکز و انحصار) کمک می‌کند، از سانسورهای ساختاری و سیستماتیک آزادی بیان و اطلاعات پیشگیری کرده و انگیزه‌های لازم برای خلاقیت، نوآوری و رقابت را فراهم می‌کند [۲، انصاری ۱۳۹۹: ۶۷].

برخی از حقوقی که مصرف‌کنندگان اینترنت به‌موجب این اصل به دست می‌آورند و تعهداتی که متناظر با این حقوق برای دولت و ارائه‌دهندگان خدمات دسترسی ایجاد می‌شود در مصوبات اتحادیهٔ اروپا درباره اصل بی‌طرفی اینترنت و گزارش عمال آن در دولت‌های عضو اتحادیه، گزارش‌های گزارشگران آزادی بیان، قواعد کمیسیون فدرال ارتباطات آمریکا به‌صورت زیر آمده است:

۱. حق دسترسی به محتوای قانونی اینترنت انتخابی خود و ارسال هرگونه محتوای قانونی به انتخاب خود؛

۲. حق انتخاب و اجرای هرگونه نرم‌افزارهای کاربردی و استفاده از سرویس‌های صوتی و ویدئویی به انتخاب خود؛

۳. حق دسترسی به هرگونه موتور جست‌وجو به انتخاب خود؛

۴. حق اتصال دستگاه‌های انتخابی غیر آسیب‌رسان به شبکه؛

۵. حق برخورداری از رقابت در بین ارائه‌دهندگان شبکه، ارائه‌دهندگان سرویس و نرم‌افزارهای کاربردی و ارائه‌دهندگان محتوا؛

۶. حق دریافت اطلاعات واضح و آشکار به زبان ساده در مورد سرعت، قابلیت‌ها، محدودیت‌ها و قیمت‌گذاری تقریبی هرگونه سرویس عمومی اینترنت.

مسئولیت اصلی تحقق بی‌طرفی شبکه با دولت است که باید علاوه بر تصویب و انتشار عمومی ضوابط مربوط به این موضوع، گزارش اقدامات مرتبط با آن را نیز به‌صورت عمومی منتشر کند. دسترسی به اینترنت باید امن باشد بدین معنا که در نتیجهٔ دسترسی به اینترنت نباید تهدیدی متوجه افراد شود. بدین منظور، دولت‌ها علاوه بر اینکه باید حق بی نامی و استفاده از رمزگذاری را به رسمیت بشناسند، مکلف هستند با اتخاذ تدابیر لازم، اعم از فنی و قانونی، ارتکاب برخی اعمال از طریق اینترنت را منع و کنترل کنند. دولت‌ها باید فرایند جمع‌آوری، پردازش و استفاده از داده‌های مذکور را قانونمند کنند، همانند دولت آمریکا که با وضع قوانین متعدد به این سمت رفته‌اند امن بودن اینترنت ایجاب می‌کند که دولت‌ها از کودکان در برابر آسیب‌های ناشی از دسترسی به اینترنت حفاظت کنند. دسترسی کودکان به اینترنت را نظام‌مند کنند، ارتکاب خشونت و آزار علیه آنها را جرم‌انگاری کرده و از کودکان در برابر مطالب غیر سالم و زیان‌بار حفاظت کنند. آمریکا در این زمینه قانون خاصی تصویب کرده است [۲، انصاری ۱۳۹۹: ۶۸].

کشور آمریکا سردمدار جریان آزاد اطلاعات است، این کشور در کنفرانس بین‌المللی آزادی اطلاعات در ۱۹۴۸، با تمام قوا در برابر شوروی و کشورهای سوسیالیستی صف‌آرایی کرد؛ در کنفرانس ژنو، آمریکا برای

به کرسی نشاندن نظریه‌های خود به طور مستقیم طرح‌های مختلفی ارائه کرد. پیشنویس ماده ۱۹ اعلامیه جهانی حقوق بشر درباره آزادی اطلاعات با وجود مخالفتهای شدید کشورهای سوسیالیستی و فرانسه بر سر محدودیتهای این آزادی، تصویب شد. بدینگونه آمریکا و شوروی برای نخستین‌بار، در یک کنفرانس بینالمللی با یکدیگر برخورد کردند. آمریکایی‌ها از آزاد بودن کامل اطلاعات در سطح جهانی به‌منظور حفظ تفاهم بینالمللی و تحکیم صلح دفاع میکردند. شوروی‌ها در برابر مواضع آمریکا، اصل حاکمیت ملی کشورها و نظریه "خدمات عمومی" دولتی در مورد اداره وسایل ارتباط‌جمعی را عنوان کردند. آنها معتقد بودند که اداره وسایل ارتباط‌جمعی باید در کنترل دولت باشد و اگر در امور مربوط به ارتباطات و اطلاعات در سطح جهانی مداخله شود، در حاکمیت ملی آنها مداخله می‌شود [۸، معتمدنژاد، ۱۳۸۳: ۹۳]. اما می‌بینیم که آمریکا برای حفظ منافع خود پا روی این قانون گذاشته است که یکی از مصادیق آن استیضاح مدیرعامل تیک‌تاک است.

۱.۸ استیضاح مدیرعامل تیک‌تاک در فضای آزادی بیان و اهمیت نظارت بر فضای مجازی

استیضاح مدیرعامل تیک‌تاک مسئله‌ای هست که چالش‌هایی به دنبال داشته است، و ازآن‌جهت که مسئله جدیدی در نوع خود است نظرات ضدونقیضی را به دنبال داشته است، اما چیزی که مورد تأیید همگان است، این است که جمع این بازخواست و آزادی بیان کار دشواری است حتی با تمام دلایلی که دولت آمریکا برای آن بیان کرده است.

آمریکا تمام قوانین دنیا را بر پایه جریان آزادی اطلاعات پیاده کرده است و این به نفع آمریکا است که اطلاعات در آنجا تولید و در آنجا ذخیره می‌شود، ولی جایی که منافع آمریکا به خطر افتاد قوانین مقابل آزادی بیان وضع کردند؛ تنها دو کشور هستند که می‌گویند آزادی بیان جزء امور طبیعی انسان‌ها هست و بقیه کشورها می‌گویند جزء امور موضوعه هست، آمریکا که سردمدار آن بود که به‌هیچ‌عنوان نباید اطلاعات محدود شود وقتی گوشه‌ای از منافعش به خطر می‌افتد به تکاپو می‌افتد که جلوی آن را بگیرد برای همین قوانینی از جمله قانون «محدودکردن ظهور تهدیدات امنیتی (RESTRICT) که فناوری اطلاعات و ارتباطات را هدف قرار می‌دهد» وضع کردند و این قانون به دولت آمریکا اجازه می‌داد کاربران را برای استفاده از تیک‌تاک محدود کند، و قانون دیگری وضع‌کردن که نیروهای نظامی، انتظامی، امنیتی و اطلاعاتی آمریکا حق استفاده از هیچ پلتفرم غیرآمریکایی را ندارند؛ پس آن چیزی که در بطن این ماجرا مشخص است این است که استیضاح مدیرعامل تیک‌تاک برای این بود که در اول شاید اطلاعات آمریکایی‌ها در جای دیگر ذخیره شود و جلوی این را بگیرند و در مرحله بعد مدیریت افکار عمومی انجام داده و به اقناع مردم بپردازند، چون اگر مسائل اخلاقی مسئله موردنظر بود، در مورد بقیه پلتفرم‌ها مخصوصاً پلتفرم‌های آمریکایی هم همین موارد و اشکال وارد است. منشور سازمان ملل متحد بند ۱ و بند ۱۹ و قانون بشر دربند ۱۹ به‌صراحت تأکید می‌کند که آزادی بیان حق همه جامعه است و هیچ‌کس حق محدودکردن آن را ندارد، و آمریکایی‌ها پیرو و امضاکننده این طرح هستند و این پیگیری آمریکا درمورد تیک‌تاک طبق حقوق بین‌الملل ارتباطات خلاف قانون است و آمریکا حق چنین قانون‌گذاری‌هایی در مقابل حقوق بین‌الملل ندارد، چون قوانین حقوق بین‌الملل بالاتر از قوانین موضوعه در کشورهاست، ضمن اینکه این موارد در خود قانون اساسی آمریکا هم هست که هر نوع

محدودیتی علیه آزادی بیان نباید قانون‌گذاری شود و این قانون دیگر قوانین که وضع کردند برای این است که دولت برای دسترسی افراد، آزادی دریافت اطلاعات، انتشار اطلاعات، آزادی استفاده از هر وسیله برای انتشار و دریافت اطلاعات بتواند محدودیت اعمال کند که آزادی این موارد را حقوق بین‌الملل در برمی‌گیرد و قوانین دیگر قوانین موضوعه کشور آمریکا در مقابل حقوق بین‌الملل و مخالف آن است (اکبری. ک، نشست علمی استیضاح تیک‌تاک در آمریکا: بررسی محدودیت شبکه‌های اجتماعی در کشورهای مدعی دموکراسی، ۲۵ اردیبهشت ۱۴۰۲).

این نشست نشان از اهمیت فوق‌العاده فضای مجازی برای سیاست‌مداران و قانون‌گذاران ایالات متحده، اولین، بزرگ‌ترین و تنها سیاست‌گذار کلان این حوزه در جهان است و به‌وسیله آن ما دست یافتیم به اینکه بعضی از محدودیت‌ها که در جمهوری اسلامی برای بعضی پلتفرم‌ها انجام شد کاملاً مطابق قوانین بین‌الملل ارتباطات بود؛ چون این محدودیت‌ها برای این بود که این پلتفرم‌ها کانونی برای آموزش کاربرد سلاح علیه کشور، ایجاد جنگ داخلی، ایجاد خشونت در داخل کشور و ... بودند، و تمامی این موارد که اغلب در پلتفرم‌های آمریکایی ترویج می‌شد به‌صراحت مخالف حقوق بین‌الملل ارتباطات است پس در نتیجه و این محدودیت‌هایی که توسط کشور ایران بر روی برخی پلتفرم‌ها اعمال شد همه موافق حقوق بین‌الملل بود و همه اینها مطابق آزادی بیان است و همه اینها اهمیت تشکیل شبکه ملی اطلاعات را به ما گوشزد می‌کند.

۲.۸ شبکه ملی اطلاعات ایران

شبکه ملی اطلاعات طبق تعریفی که شورای‌عالی فضای مجازی در مصوبه جلسه پانزدهم خود در تاریخ ۳/۱۰/۹۲ ارائه داده است به‌عنوان زیرساخت ارتباطی فضای مجازی کشور، شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده‌ای است به صورتی که درخواست‌ها دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند به‌هیچ‌وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت و خصوصی و امن داخلی در آن فراهم شود، بحث شبکه ملی در کشور از اواخر سال ۱۳۸۴ مطرح و مهم‌ترین دلیل پیاده‌سازی این شبکه در آن سال کاهش وابستگی به شبکه جهانی اینترنت اعلام شد [۱۰، همایون و هاشمی، ۱۳۹۶: ۱۲].

شبکه ملی اطلاعات در یک نگاه کلی، همان اینترنت با مدیریت داخلی است که همه استانداردهای امنیتی، فرهنگی و فنی در آن رعایت شده است. یعنی، همه اطلاعات و ارتباطات، کارها، خریدها، بازی‌ها و ... در یک شبکه داخلی؛ مدیریت، نگهداری و محافظت می‌شود.

شبکه ملی اطلاعات که با نام‌های دیگری شامل «اینترنت ملی»، «اینترانت ملی ایران» و «شبکه ملی اینترنت» نیز، شناخته می‌شود، پروژه‌ای برای توسعه شبکه زیرساخت امن و پایدار ملی در ایران است.

در مجموع شبکه ملی اطلاعات یعنی برقراری ارتباطات و ارائه خدمات در فضای مجازی به شکل ارزان، پرسرعت، امن و سالم. در حقیقت این شبکه باید بتواند نیازهای واقعی و مشروع مردم را در بستری پرسرعت، قیمتی پایین، امنیتی جامع و پایدار و در عین برخورداری از بالاترین حد سلامت پاسخگوی نیازهای مشروع مردم در فضای مجازی باشد و زمینه ارتباط کاربران ایرانی با یکدیگر را از بستر داخلی و ارتباط با خارج از کشور را از بستر بین‌الملل مهیا کند [۵، کمالی ۱۳۹۸: ۳۶].

سازمان‌ها در عصر حاضر صاحب انبوهی از اطلاعات به‌عنوان دارایی خود هستند. اطلاعاتی که نیاز به حفاظت دارد تا در معرض خطر و آسیب قرار نگیرد. اشتراک اطلاعات، نظام مدیریت اطلاعات در سازمان‌ها باید دارای الگوی عمل و برنامه جامع باشد و از امکانات و تجهیزات اختصاصی بهره‌برداری کند. شبکه درون‌سازمانی واجد یک سری تمهیدات است که به طور معمول از سوی مدیریت‌های داخلی موردتوجه قرار می‌گیرد؛ اما هنگامی‌که در یک سپهر گسترده؛ یعنی کشور، امنیت سازمان‌ها مطرح می‌شود نمی‌توان اهمیت شبکه ملی اطلاعات را نادیده گرفت. برای ناامنی در فضای سایبر تنوع اهداف و انگیزه‌ها متفاوت است. برخی افراد در واقع به دنبال هیچ‌گونه منفعتی نیستند و برای سرگرمی و تفریح مبادرت به رفتارهای ناامن‌کننده و ضداجتماعی می‌کنند، کدنویسان خرد از جمله این افراد هستند که هک‌کردن اطلاعات و منابع پایگاه‌های شخصی و سازمانی از نمونه کارهای آنان است؛ یک بخش که قاطبه مهاجمان و ناامن‌کننده‌های فضای سایبر را تشکیل می‌دهند افراد انتقام‌جو و منفعت‌طلب هستند که بدنه اصلی مخاطرات و تهدیدهای سایبری را تشکیل می‌دهند. اینان به دلایل مختلفی از جمله پیشینه تجاربی که با دیگر افراد داشته‌اند و در یک سری مراودات و معاملات ناکام بوده‌اند به این جهت وارد عمل شده و اقدامات مخرب را انجام می‌دهند؛ بخش دیگری که کار حرفه‌ای در زمینه تهدیدهای سایبری را طراحی و دنبال می‌کنند برنامه‌نویسان خبره‌ای محسوب می‌شوند که با مقاصد و اهداف سازماندهی شده برای ضربه‌زدن به ساختارها و موقعیت‌های سرزمینی یا سازمانی برای احراز و ارتقای موقعیت خود از موضع برتری‌جویی اقدام می‌کنند که معمولاً دامنه فعالیتشان گسترده است و تبعات آن می‌تواند بسیار وخیم باشد از عملیات هکری، سرقت و دستبرد تا حملات تخریبی سایبری تأسیسات و پروژه‌ها و ایجاد اختلال در عملکرد سامانه‌ها و برنامه‌ها و جنگ‌های سایبری در سطوح مختلف سبک تا سنگین از این طریق به انجام می‌رسد [۵، کمالی ۱۳۹۸: ۳۷].

شبکه ملی اطلاعات دارای مزایایی است که باعث شده ایران، مانند بسیاری از کشورهای پیشرفته دیگر، به دنبال آن باشد. چند نمونه از این مزایا عبارت‌اند از:

۱. کاهش مراجعات بیهوده کاربران به اینترنت بین‌الملل و دریافت تکراری اطلاعات که به این معناست که هم در هزینه‌های ارزی صرفه‌جویی فراوانی صورت می‌گیرد و هم سرعت دسترسی به اطلاعات با افزایش بسیار زیادی مواجه خواهد شد؛

۲. با تشکیل ابر اطلاعات و استفاده شرکت‌ها، سرورهای خود را به داخل کشور منتقل می‌کنند؛ زیرا هم از جهت قیمت و هم از جهت سرعت، کاملاً به سود آن‌هاست. این موضوع به همین نسبت برای مصرف‌کننده داخلی با مزیت قیمت و سرعت همراه خواهد بود؛

۳. استفاده بیشتر کاربران از پهنای باند داخلی، به معنای کاهش قیمت اینترنت برای مصرف‌کنندگان خواهد شد؛

۴. بارگذاری اطلاعات (آپلود) برای تولیدکنندگان اطلاعات رایگان خواهد بود؛ بنابراین، راه‌اندازی سایت و سایر خدمات ازاین‌جهت هزینه‌ای در برنخواهد داشت. همچنین، تولیدکنندگان داخلی برای تولید ترافیک، از محل درآمد ترافیک اینترنت وجوهی را دریافت خواهند کرد، همانند شرکت‌های معروفی

مثل آمازون؛ بنابراین، غالب مردم به‌جای مصرف اطلاعات، به تولید اطلاعات علاقه‌مند خواهند شد. این موضوع موجب به‌وجودآمدن خودکار نهضت تولید محتوا خواهد شد. همچنین، وقتی تولید محتوا افزایش پیدا کند، مصرف‌کننده گزینه‌های زیادی برای انتخاب خواهد داشت و تحقیقاً به تولیدات فاخر مراجعه خواهد کرد. در نتیجه، گرایش افراد به تولید محصولات فاخر خواهد بود، نه غیرمفید و بی‌کیفیت؛

۵. تفاوت قیمت اینترنت بین‌المللی و ترافیک داخلی وجود دارد. به این معنا که اینترنت بین‌المللی با همین قیمت و ترافیک داخلی با یک‌دهم قیمت فعلی عرضه خواهد شد. این تفاوت فاحش در قیمت باعث می‌شود کاربران غالب نیازمندی‌های خود را با سرویس‌های خوب داخلی برطرف کنند و سرویس‌های خارجی با کاهش استفاده کاربران مواجه شوند (مانند اتفاقی که برای سرویس وبلاگ افتاد).

۶. شرکت‌های ارائه‌دهنده خدمات، باتوجه‌به افزایش فراوان سود حاصل از مراجعه کاربران داخلی، ملزم به رعایت پیوست فرهنگی می‌شوند، به این معنا که حق ندارند محتوای ناسالم و یا هر محتوایی که بافرهنگ اسلامی – ایرانی در تعارض است، نگهداری و در اختیار کاربران قرار دهند و در صورت تخلف، به‌راحتی با دیگر شرکت‌ها جایگزین می‌گردند.

۷. در این شرایط، می‌توان با شرکت‌های معروفی مانند گوگل مذاکره کرد؛ زیرا تا قبل از این، گفتگو با چنین شرکت‌هایی اصلاً عقلانی نبود و مزیت‌ها در میدان عمل کاملاً به سود این شرکت‌ها بود؛ اما در صورت داشتن شبکه ملی اطلاعات، وضعیت این شرکت‌ها در کشورمان مانند چین خواهد شد که به‌عنوان نمونه، گوگل هر ساله قرارداد فعالیت خود در چین را تمدید می‌کند و متعهد می‌شود که تمامی قوانین چین را مراعات و مطابق سیاست‌های چین اقدام به فعالیت نماید [۶، کهوند ۱۳۹۶: ۸۵].

باتوجه‌به مزایای فوق، شبکه ملی اطلاعات به‌عنوان یک پروژه مهم و استراتژیک برای توسعه کشور و ارتقای سطح فناوری و اطلاعات در جامعه، بسیار حائز اهمیت است؛ و ازآن‌جهت که کشورهایی همچون چین، روسیه و حتی آمریکا در این فضا پیشرفت‌های قابل‌توجهی داشته‌اند، باید به این نکته توجه کنیم که در حالت کلی تمام کشورهای پیشرفته یا برای تحقق سرعت و کیفیت بالا در ارتباطات داخلی و ایجاد امنیت سایبری خود اقدام به ایجاد شبکه‌های ارتباطی داخلی کرده‌اند یا اینکه همچون ایران در حال ایجاد و توسعه این شبکه هستند، اما به هر روی همان‌گونه که بیان شد، نحوه بهره‌گیری و به‌کارگیری از آن کاملاً به نگاه کلان حاکمیتی و دولتی هر کشور برمی‌گردد.

۹ نتیجه‌گیری

پیشرفت فناوری اطلاعات و ارتباطات، باعث تضعیف نقش حاکمیت‌های ملی در کنترل و نظارت بر مرزهای سیاسی، جریان داده و اطلاعات، کنترل و هدایت افکار عمومی و سایر موارد شده است. فضای سایبر به‌عنوان

یکی از اصلی‌ترین بسترهای درگیری و تقابل میان دولت‌ها شناخته می‌شود. با استفاده از فناوری‌های مبتنی بر اینترنت، مانند شبکه‌های اجتماعی و غیره، کشورها سعی در برتری‌جویی نسبت به رقبای خود دارند و به دنبال تغییر مواضع کشور هدف یا تغییر حکومت در کشور موردنظر هستند. تمرکز و ذخیره‌سازی اطلاعات ریزودرشت بخش‌های مختلف جهان، افزایش قدرت اطلاعاتی، سپس سلطه اطلاعاتی و در نهایت سلطه فرهنگی و سیاسی آمریکا بر دیگران را به دنبال داشته است. باتوجه‌به این مسائل، کشورها باید در پی اعمال حاکمیت در قلمروهای جدید مانند فضای مجازی باشند. اعمال حاکمیت در فضای مجازی در جهت جلوگیری از تهدیدها، موضوعیت حیاتی دارد. تحقق شبکه ملی اطلاعات، می‌تواند کلیه نیازهای حوزه فناوری اطلاعات و ارتباطات کشور را پوشش دهد و زمینه را برای تحقق دولت الکترونیک، سلامت الکترونیک، آموزش الکترونیک و خدمات عمومی الکترونیکی مانند بانکداری الکترونیکی و غیره، فراهم کند. همچنین، تحقق شبکه ملی اطلاعات، تضمین استقلال و امنیت کشور و تحقق حاکمیت جمهوری اسلامی در فضای سایبر را به دنبال دارد که به وابستگی کلیدی به تحقق شبکه ملی اطلاعات در سه بعد زیرساخت، سرویس و محتوی دارد.

پس باتوجه‌به رویه دیگر کشورها، از جمله کشورهای بنیان‌گذار و حامی حقوق بین‌الملل ارتباطات، داشتن فضای سایبری امن و شبکه ملی ارتباطات امری مهم و ضروری قلمداد شده و باتوجه‌به تبصره‌های قوانین دیگر کشورها در مورد تخصیص زدن حقوق بین‌الملل، اقدامات ایران هم دارای چهارچوب قانونی خود بوده، و نمی‌توان گفت ایران ناقض حقوق بین‌المللی ارتباطات است.

مراجع

[۱] اکبری، کمال، نشست علمی بررسی محدودیت شبکه‌های اجتماعی در کشورهای مدعی دموکراسی، دانشکده دین و رسانه دانشگاه صداوسیما، ۱۴۰۲.
https://qomirib.ac.ir/portal/newsview/67930

[۲] انصاری، باقر، «حق دسترسی به اینترنت؛ مبانی و محتوا»، مجله حقوقی دادگستری، ۱۳۹۹.

[۳] زاهدی، مهدی، «آزادی بیان و اصل دوگانگی ایده و بیان»، فصلنامه علمی پژوهش حقوق عمومی، انتشارات دانشگاه علامه طباطبایی، ۱۴۰۰.

[۴] سعیدی، رحمان، حقوق بین‌المللی تطبیقی ارتباطات (جلد دوم)، چاپ اول، انتشارات سیمای شرق، ۱۴۰۱.

[۵] کمالی، تقی، امنیت سایبری و حفاظت داده‌ها، چاپ اول، انتشارات پشتیبان، ۱۳۹۸.

[۶] کهوند، محمد، «شبکه ملی اطلاعات»، نشریه مبلغان، ۱۳۹۶.

[۷] محمدی، حافظ، «شبکه ملی اطلاعات و تحقق حکمرانی سایبری در جمهوری اسلامی ایران با رویکرد تجربه کشورها» دومین همایش ملی حکمرانی اسلامی، ۱۳۹۹.

[۸] معتمدنژاد، کاظم، ایران و اجلاس جهانی سران درباره جامعه اطلاعاتی، چاپ اول، مرکز پژوهش‌های ارتباطات، ۱۳۸۳.

[۹] معتمدنژاد، کاظم، حقوق ارتباطات، چاپ اول، دفتر مطالعات و توسعه رسانه‌ها، ۱۳۸۸.

[۱۰] همایون، محمدهادی؛ هاشمی، محمد ساجد، «بازنمایی شبکه ملی اطلاعات در رسانه‌های برون‌مرزی»، فصلنامه مطالعات رسانه‌های نوین، ۱۳۹۶.

ارائه الگوی به‌کارگیری رسانه‌های اجتماعی در ارتقای روابط عمومی (مورد مطالعه: شهرداری نهاوند)

مریم کرمعلی[۱]، علی جعفری[۲]

[۱] دانشجوی دکتری علوم ارتباطات، دانشگاه آزاد اسلامی واحد اردبیل، اردبیل، ایران
maryamk1366@yahoo.com
[۲] استادیار پژوهشگاه مطالعات آموزش و پرورش، سازمان پژوهش و برنامه‌ریزی آموزشی، تهران، ایران
alijafari.researcher@gmail.com

چکیده

هدف این پژوهش، بررسی تأثیر رسانه‌های اجتماعی بر روابط عمومی سازمان‌های خدماتی است. با پیشرفت رسانه‌های اجتماعی، بخش‌های مختلفی از جمله روابط عمومی نیز تحت تأثیر قرارگرفته‌اند. به‌همین دلیل، تخصصی‌های روابط عمومی باید توانایی سازگاری با محیط دیجیتال را داشته باشند تا با تغییرات چشم‌گیر این فضا همراهی کنند. این پژوهش با هدف طراحی یک الگوی استفاده از رسانه‌های اجتماعی در بهبود اثربخشی روابط عمومی سازمان‌های خدماتی به‌صورت آمیخته (کیفی و کمی) انجام شده است. روش تحلیل پژوهش به صورت کاربردی و با رویکرد اکتشافی آمیخته بوده است. در مرحله اول، با استفاده از تحلیل محتوا و مصاحبه‌های عمیق، مؤلفه‌های الگو شناسایی شدند. شرکت‌کنندگان این مرحله از بین ۱۶ نفر از خبرگان دانشگاهی و مدیران ارشد شهرداری نهاوند به‌صورت هدفمند انتخاب شدند. در مرحله دوم، با استفاده از روش مدل‌سازی معادلات ساختاری، الگوی طراحی‌شده بررسی شد. نمونه آماری این پژوهش شامل ۲۰۳ نفر از مدیران و کارشناسان شهرداری نهاوند بود که به‌صورت تصادفی طبقه‌ای انتخاب شدند. ابزار جمع‌آوری داده‌ها پرسشنامه بود که روایی و پایایی آن تأیید شده است. تحلیل داده‌ها با استفاده از نرم‌افزار لیزرل انجام شد. نتایج بخش کیفی نشان می‌دهد که رسانه‌های اجتماعی در سه جنبه ارتباطات رسانه‌ای، سهولت استفاده و اطلاع‌رسانی تأثیرگذار هستند. در بخش کمی نیز مشخص شد که استفاده از رسانه‌های اجتماعی با ارتقای روابط عمومی سازمان‌های خدماتی رابطه‌ای معنادار دارد و الگوی طراحی شده متناسب است. از این رو، مدیران و سیاست‌گذاران روابط عمومی سازمان‌های خدماتی می‌توانند با بهره‌گیری از نتایج این پژوهش و استفاده از ظرفیت‌های رسانه‌های اجتماعی، بستر مناسبی را برای توسعه و بهبود اثربخشی فعالیت‌های روابط عمومی سازمان فراهم کنند.

کلمات کلیدی: رسانه اجتماعی، روابط عمومی، سازمان خدماتی، شهرداری نهاوند.

۱ مقدمه

استفاده از رسانه‌های اجتماعی به عنوان یکی از محبوب‌ترین فعالیت‌های آنلاین، جایگاه خود را به‌عنوان یک ابزار ارتباطی مهم در جهان مدرن یافته است. در سال ۲۰۲۰، بیش از ۳ میلیارد و ۶۰۰ هزار نفر در سراسر جهان از رسانه‌های اجتماعی بهره‌مند بودند، و پیش‌بینی می‌شود که این تعداد تا سال ۲۰۲۵ به تقریباً ۴ میلیارد و ۴۱ هزار نفر افزایش یابد (استاتیستا[۱] ، ۲۰۲۱).

رسانه‌های اجتماعی، ابزارهای مبتنی بر فناوری هستند که به فعالیت‌ها و تعاملات فضای کاری نفوذ کرده و آنها را تغییر داده‌اند. این رسانه‌ها امکان پخش و مبادله گسترده‌ای از محتوای تولید شده توسط کاربران را فراهم می‌کنند (ساترلند و فربرگ، درایور و خطاب[۲] ، ۲۰۲۰). با افزایش تعداد کاربران، بخش روابط عمومی سازمان نیز از این تغییرات بهره‌مند شده و از فرصت‌های ارتباطی و تبلیغاتی جدید بهره‌می‌برد (کنت و لی[۳] ، ۲۰۲۰).

بعضی مطالعات (کنت و تیلور[۴] ، ۱۹۹۸) نشان داده‌اند که از اواخر دهه ۱۹۹۰، با پیشرفت فناوری‌های دیجیتال و تمرکز بر قابلیت تعاملی اینترنت، رسانه‌های اجتماعی به طور فزاینده‌ای رویه روابط عمومی را تغییر داده‌اند (الاگوی و بریسلو[۵]، ۲۰۱۶). این رسانه‌ها نه تنها به ارائه حجم زیادی از اطلاعات کمک می‌کنند، بلکه مشارکت و صدای سازمان را در مقابل عموم مردم بهبود می‌بخشند. رسانه‌های اجتماعی افراد را قادر می‌سازند تا روابط جدیدی بین افراد و سازمان‌ها ایجاد کنند (ال کندری و گایتر، الفهد، دشتی و السابر[۶] ، ۲۰۱۹).

در این سناریو، رسانه‌های اجتماعی به متخصصان روابط عمومی فرصت‌های متعددی ارائه می‌دهند تا با مردم در تعامل باشند و از آخرین شیوه‌های فناوری در کار خود بهره‌مند شوند (کورتیس و همکاران[۷] ، ۲۰۱۰). افزایش فرصت‌های مشارکت عمومی، روابط بین سازمان و مخاطبان را تقویت کرده و به بهبود خدمات یا سود سازمان کمک می‌کند. آمارها نیز نشان می‌دهد که متخصصان روابط عمومی بزرگترین قسمت از ارتباطات خود را به وسیله رسانه‌های اجتماعی مدیریت می‌کنند و به این عنوان به اهمیت این ابزارها اکیداً تاکید می‌کنند (ادمایر هربست[۸]، ۲۰۱۴).

با توجه به نقش محوری شهرداری نهاوند در رضایتمندی از حمل و نقل شهری شهروندان و ضرورت ارائه اطلاعات صحیح و دقیق، ایجاد الگوی روابط عمومی مناسب می‌تواند در بهبود کیفیت ارتباطات میان سازمان و جامعه مؤثر باشد. این پژوهش با هدف پاسخ به سؤال اصلی «الگوی به کارگیری رسانه‌های اجتماعی در ارتقای روابط عمومی سازمان‌های خدماتی چگونه است؟» اجرا شده است، تا متخصصان آینده روابط عمومی

[1] Statista
[2] Sutherland, Freberg, Driver and Khattab
[3] Kent and Li
[4] Kent and Taylor
[5] Allagui and Breslow
[6] Al-Kandari, Gaither, Alfahad, Dashti and Alsaber
[7] Curtis et al.
[8] Adlmaier-Herbst

درک درستی از نحوه استفاده از این ابزارها برای بهبود ارتباطات سازمانی به‌دست آورند.

۲ مبانی نظری پژوهش

۱.۲ روابط عمومی

انجمن بین‌المللی روابط عمومی (ایپرا)، که در سال ۱۹۵۵ تأسیس شده و از اعضای انجمن‌های ملی و کارشناسان روابط عمومی تشکیل شده است، در ماه می ۱۹۶۰ تعریف جامعی از روابط عمومی ارائه داد. ایپرا بر این باور است که روابط عمومی بخشی از وظایف مدیریت سازمان است، عملی است ممتد، مداوم و طرح‌ریزی شده که از طریق آن افراد و سازمان می‌کوشند تا پشتیبانی، تفاهم و همکاری کسانی را به‌دست آورند که با آنها سروکار دارند یا در آینده سروکار خواهند داشت و با اقدام‌های ارتباطی و تدابیر دیگر، به خلق گرایش‌های مطلوب بپردازند و گرایش‌های مخالف را از میان بردارند (رسولی و هدایتی، ۱۳۹۶: ۲۱۸).

۲.۲ رسانه‌های اجتماعی

رسانه‌های اجتماعی را می‌توان به عنوان ابزارهای گروهی آن‌لاین و فناوری‌هایی تعریف کرد که مشارکت، محاوره، آزاداندیشی و اجتماعی شدن را در گروهی از کاربران تشویق و میسر می‌کنند. رسانه‌های اجتماعی یک مجموعه از کاربردهای ابزارهای نرم‌افزاری آنلاین هستند و شامل سایت‌های شبکه‌های اجتماعی نظیر فیسبوک، مای‌اسپیس، توییتر، و همچنین سایت‌های اشتراک رسانه‌ای، وبلاگ‌ها، پادکست‌ها و غیره می‌شوند (زارعی و بیات، ۱۳۹۴: ۱۰۱).

۳.۲ پیشینه تجربی پژوهش

پیشینه‌های داخلی و خارجی پژوهش در جدول ۱ ذکر شده است.

۴.۲ روش شناسی پژوهش

این پژوهش از نظر هدف، کاربردی محسوب می‌شود و طرح تحقیق، آمیخته اکتشافی از نوع متوالی است؛ چرا که استفاده از روش آمیخته، به ارائه تصویری کاملتر و در کیفیت عمیق‌تر از پدیده‌های در دست مطالعه برای تحقق اهداف پژوهشی منجر می‌شود.

جامعه هدف در بخش کیفی، خبرگان دانشگاهی صاحب نظر و با تجربه و همچنین مدیران ارشد شرکت بهره‌برداری شهرداری نهاوند بود. برای تعیین حجم نمونه، از روش اشباع نظری استفاده شد. در این روش، فرایند نمونه‌گیری تا جایی ادامه می‌یابد که یافته‌های جدید از مصاحبه‌ها حاصل نشود. در این پژوهش، اشباع نظری پس از مصاحبه با ۱۶ نفر به دست آمد.

برای انتخاب نمونه‌ها از روش غیراحتمالی هدفمند استفاده شد. در این روش، محققان معیارهایی را برای انتخاب نمونه‌ها مدنظر قرار می‌دهند. در این پژوهش، معیار انتخاب نمونه‌ها داشتن مدرک دکتری در زمینه مدیریت رسانه، انتشار مقاله مرتبط با زمینه پژوهش و سابقه کار اجرایی در حوزه روابط عمومی بود.

جدول ۱: پیشینه‌های داخلی و خارجی پژوهش

محقق (سال)	عنوان	یافته‌ها
نرگسیان، هژبرافکن خلاری و معینی کربکندی (۱۳۹۴)	تأثیر رسانه‌های اجتماعی آن‌لاین بر شفافیت و اعتماد عمومی با اثر میانجی‌گری مشارکت عمومی (مطالعه موردی: دانشجویان دانشگاه نهاوند)	اثر رسانه‌های اجتماعی آن‌لاین بر مشارکت مدنی و سیاسی و همچنین، اثر این دو نوع مشارکت بر شفافیت و اعتماد عمومی معنادار است.
مرادی (۱۳۹۶)	بررسی تأثیر شبکه‌های اجتماعی در دنیای روابط عمومی (مطالعه موردی: شهرداری بابل)	به‌کارگیری شبکه‌های اجتماعی مجازی (تلگرام) در روابط عمومی بر توسعه خدمات اطلاع‌رسانی، توسعه دسترسی به منابع خبری دسته اول، انگاره‌سازی مثبت و کارایی و بازده روابط عمومی الکترونیک در شهرداری بابل تأثیر دارد.
زینلی، سلطانی‌فر و مظفری (۱۳۹۷)	بررسی نقش شبکه‌های اجتماعی موبایلی بر توسعه مشارکت اجتماعی	شبکه‌های اجتماعی موبایلی بر توسعه مشاکت اجتماعی تأثیر دارد.
محمدی و همکاران (۱۳۹۸)	مدیریت جریان‌سازی خبری در روابط عمومی سازمان‌های دولتی	با تغییرات تکنولوژیکی ایجادشده، تبدیل شدن روابط عمومی به سازمان‌های رسانه‌ای و نیز، استفاده از قالب‌های ژورنالیستی، روابط عمومی‌ها در جریان‌سازی خبری جامعه نقش فعال‌تری دارند و به‌تبع آن، باعث پیشبرد اهداف سازمانی می‌شوند.
کریمی راهجردی، قوام، خرازی، آذر و گرانمایه‌پور (۱۳۹۸)	جایگاه شبکه‌های اجتماعی مجازی و پیام‌رسان موبایلی در شکل‌گیری خرد جمعی	رسانه‌های مبتنی بر موبایل، به‌سبب فرامرزی و کم هزینه بودن و گسترش آزادی بیان، محلی برای تبادل افکار عمومی شده‌اند و امکان اشاعه افکار عمومی از طریق مشارکت مستقیم شهروندان را فراهم آورده‌اند.

ابزار گردآوری داده‌ها در بخش کیفی نیز مصاحبه‌های نیمه‌ساختار یافته بود. مصاحبه‌ها به صورت جلسات فردی و مدت زمان میانگین ۴۵ دقیقه‌ای انجام شد. در ابتدای هر جلسه، هدف پژوهش به روشنی توضیح داده شد و پس از مطرح کردن سؤالات مصاحبه، پاسخ‌های افراد ضبط شد. بیانات و اظهارات مشارکت‌کنندگان پس از اتمام هر مصاحبه به متن نوشتاری تبدیل و جهت کدگذاری وارد نرم‌افزار مکس کیودا شد. تحلیل یافته‌ها با استفاده از روش تحلیل تم انجام گرفت. به زعم بویاتزیس[۹] (۱۹۸۹) تحلیل تم روش مناسبی برای برقراری انتقال مفاهیم بین پژوهشگران با جهت‌گیری‌های متفاوت و ارتباط بین رویکردهای فلسفی مختلف میان نظریه‌پردازان و مجریان است. این روش به تسهیل فرایند انتقال مشاهده‌ها و یافته‌ها و تفسیرهای محققان به دیگران کمک می‌کند.

[9] Boyatzis

برای بررسی پایایی کدگذاری، از روش پایایی بازآزمون استفاده شد. در این روش سه مصاحبه انتخابی در دو بازه زمانی سه هفته‌ای کدگذاری شدند. در هر کدگذاری، کدهای مشابه به نام توافق و کدهای غیرمشابه به نام عدم توافق مشخص شده و پایایی بین کدگذاری‌ها محاسبه شد. نتایج پایایی بازآزمون برای سه مصاحبه، ۰/۸۷، ۰/۸۲ و ۰/۸۵ درصد تعیین شد که نشان‌دهنده پایایی قابل قبول کدگذاری هاست.

در مرحله دوم، به منظور ارزیابی برازش یافته‌های کیفی، از روش کمی و رویکرد مدل سازی معادلات ساختاری استفاده شد. جامعه آماری در این بخش مدیران و کارشناسان روابط عمومی در شهرداری نهاوند بود. موضوع مهم در بحث مدل‌یابی معادلات ساختاری تعیین حداقل حجم نمونه است ، (کلاین[10]، ۱۹۹۰) کلاین (۲۰۰۵) توصیه می کند که از ۵ تا ۱۰ برابر هر متغیر، برای تخمین حجم نمونه استفاده شود و ۲۰۰ مورد را برای اندازه نمونه، متوسط توصیف می‌کند. بر این اساس، از آنجایی که ۳۰ گویه در مدل اندازه‌گیری وجود دارد، حداقل ۱۵۰ نمونه و حداکثر ۳۰۰ نمونه لازم است. بدین ترتیب با استفاده از فرمول کوکران، ۲۰۰ نفر برای حجم نمونه کفایت می‌کند. با توجه به امکان ریزش پرسش‌نامه‌ها، ۲۵۰ پرسشنامه توزیع و در نهایت، ۲۰۳ نسخه تکمیل شده بازگشت داده شد.

جهت انتخاب نمونه‌ها، از روش طبقه‌ای تصادفی نسبی استفاده شد؛ به این ترتیب که جامعه به دو طبقه مدیران و کارشناسان تقسیم شد، سپس با توجه به نسبت جامعه در هر طبقه، نمونه‌گیری به صورت تصادفی انجام گرفت. ابزار گردآوری داده‌ها در این بخش، پرسش‌نامه‌ای بود که بر اساس یافته‌های بخش کیفی طراحی شد و با استفاده از روش‌های اعتبارسنجی به تأیید رسید. برای بررسی روایی، از شاخص روایی محتوا استفاده شد. برای تعیین ضریب نسبی روایی محتوا از متخصصان درخواست شد تا هر یک از سؤال‌ها را بر اساس مقیاس سه بخشی لیکرت و بر اساس این گزینه‌ها طبقه‌بندی کنند: ۱. ضروری است؛ ۲. مفید است ولی ضرورتی ندارد؛ ۳. ضرورتی ندارد.

سؤال‌هایی که مقدار CVR محاسبه شده برای آن‌ها، کمتر از میزان مدنظر (با توجه به تعداد خبرگان ارزیابی‌کننده سؤال) باشد، باید از آزمون کنار گذاشته شوند. در این بخش ۸ نفر از خبرگان برای روایی‌سنجی مشارکت کردند. نتایج نشان داد که مقدار CVR متوسط به دست آمده برای هر گویه پرسش‌نامه، بیش از ۰/۷۵ است که روایی محتوای پرسش‌نامه را تأیید می‌کنند. جهت سنجش پایایی پرسش‌نامه نیز، از ضریب آلفای کرونباخ استفاده شد و نتایج نشان داد پرسش‌نامه از پایایی قابل قبولی برخوردار است. در نهایت، تحلیل داده‌ها در بخش کمی با استفاده از روش مدل سازی معادلات ساختاری با نرم‌افزارهای SPSS و لیزرل صورت گرفت.

۳ یافته‌های پژوهش

در بخش کیفی، تحلیل یافته‌ها با استفاده از روش تحلیل تم در شش مرحله انجام شد. در مرحله نخست، جهت آشنایی محقق با عمق و گستره محتوایی داده‌ها، غوطه‌ورسازی در داده‌ها آغاز شد. در مرحله دوم، کدگذاری باز به صورت پاراگراف به پاراگراف انجام گرفت. در کدگذاری باز که نخستین مرحله در اجرای

[10] Kline

شکل ۱: الگوی مفهومی اولیه مستخرج از بخش کیفی

راهبرد تحلیل تم است، نکات کلیدی مصاحبه‌ها شناسایی و کدگذاری شد. در این مرحله ۹۶ کد از مصاحبه‌ها به دست آمد.

مرحله سوم، شامل دسته‌بندی کدهای گوناگون در قالب کدهای گزینشی و مرتب کردن همه خلاصه داده‌های کدگذاری شده است. در واقع، پژوهشگر تحلیل کدهای خود را آغاز می‌کنند و در نظر می‌گیرد که چگونه کدهای گوناگون را برای ایجاد یک تم کلی ترکیب کند. در این مرحله ۳۰ کد گزینشی به دست آمده است.

در مرحله چهارم، پژوهشگر مجموعه‌ای از تم‌ها را ایجاد کرده و آن‌ها را بازبینی می‌کند. این مرحله شامل دو مرحله تصفیه و شکل دهی به تم‌های فرعی است. مرحله نخست بازبینی در سطح خلاصه‌های کدگذاری شده است. در مرحله دوم، اعتبار تم‌های فرعی در رابطه با مجموعه داده‌ها در نظر گرفته می‌شود. در این مرحله، پژوهشگران به ۵ تم فرعی دست یافتند.

۱.۳ یافته‌های بخش کمی

در این بخش، ۲۰۳ پرسش‌نامه به طور کامل جمع‌آوری شد. از این تعداد، ۶۴ درصد پاسخ‌گویان مرد و ۳۶ درصد زن بودند. از نظر گروه سنی، ۱۱٫۸ درصد پاسخ‌گویان زیر ۳۰ سال، ۳۷٫۴ درصد بین ۳۰ تا ۴۰ سال، ۳۹٫۹ درصد بین ۴۰ تا ۵۰ سال و ۱۰٫۸ درصد بالای ۵۰ سال داشتند.

جدول ۲: نتایج آزمون نرمال بودن توزیع داده‌ها

متغیر	آزمون کایزر- مایر- اولکین	نتیجه
قابلیت های رسانه های اجتماعی	۰/۸۷۰	کفایت نمونه تأیید شد.
ارتقای فعالیت های روابط عمومی	۰/۸۵۴	کفایت نمونه تأیید شد.

جدول ۳: KMO آزمون بارتلت و آزمون

متغیرهای اصلی پژوهش	کولموگروف- اسمیرنف		
	آماره	معناداری	نتیجه
قابلیت های رسانه های اجتماعی	۰/۶۹۵	۰/۷۱۹	نرمال است
ارتقای فعالیت های روابط عمومی	۱/۱۱۵	۰/۱۶۷	نرمال است

از نظر سابقه کاری، ۱۳/۸ درصد پاسخ‌گویان زیر ۵ سال، ۲۹/۷۶ درصد بین ۵ تا ۱۰ سال، ۳۴/۵ درصد بین ۱۰ تا ۲۰ سال و ۲۲/۲ درصد بالای ۲۰ سال سابقه کاری داشتند. در زمینه تحصیلات، ۶۵ درصد افراد کارشناسی، ۳۰ درصد کارشناسی ارشد و ۵ درصد دکتری داشته‌اند.

۱.۱.۳ آزمون نرمال بودن داده های آماری

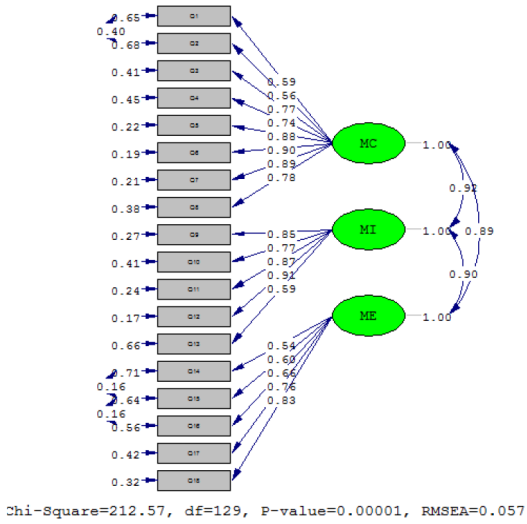
جهت بررسی نرمال بودن داده ها از روش آزمون کولموگروف اسمیرنف (S-K) استفاده شد که نتایج آن با استفاده از نسخه ۲۴ نرم‌افزار اس پی اس اس محاسبه و در جدول ۲ گزارش شده است. با توجه به نتایج جدول ۲ مقادیر سطح معناداری مؤلفه‌های مدل بالاتر از مقدار خطای ۰/۰۵ است. در نتیجه داده‌های آنها توزیع نرمال دارند.

۲.۱.۳ شاخص KMO

با استفاده از این آزمون می‌توان از کفایت نمونه‌گیری اطمینان حاصل کرد. این شاخص در دامنه صفر تا یک قرار دارد. اگر مقدار شاخص نزدیک به یک باشد داده‌های مدنظر چندان مناسب نیست؛ در صورتی که مقدار KMO کمتر از ۰/۰۵ باشد، داده‌ها برای تحلیل عاملی مناسب نخواهد بود؛ اگر مقدار آن بین ۰/۵۰ تا ۰/۶۹ باشد، می‌توان با احتیاط بیشتر به تحلیل عاملی پرداخت؛ ولی در صورتی که مقدار آن بزرگتر از ۰/۷۰ باشد همبستگی‌های موجود در بین داده‌ها برای تحلیل عاملی مناسب خواهد بود. با توجه به نتایج جدول ۳ ،تکنیک تحلیل عاملی برای متغیرهای تحقیق امکان پذیر است (KMO > ۰/۵).

۴ مدل‌سازی معادلات ساختاری

مدل معادله ساختاری ترکیبی از مدل‌های مسیر (روابط ساختاری) و مدل‌های عاملی تأییدی (روابط اندازه‌گیری) است. در مرحله اول محقق باید از کیفیت ابزارهای اندازه‌گیری اطمینان پیدا کند. به این منظور، با استفاده از روش تحلیل عاملی تأییدی، برازش مدل اندازه‌گیری پژوهش را بررسی می‌کند. در این بخش، به کمک تحلیل عاملی تأییدی، روابط بین نشانگرها و سازه‌ها یا صفت‌های مکنون بررسی می شود تا



شکل ۲: مدل اندازه‌گیری تحقیق (تخمین استاندارد)

مشخص شود که نشانگرها (شاخص‌های) هر سازه با چه دقتی آن سازه را اندازه‌گیری می‌کنند. مالک مناسب بودن ضرایب بارهای عاملی ۰٫۴ است (عاقلی و آجرلو، ۱۳۹۷: ۱۴۳)

روایی با استفاده از روایی هم‌گرا و پایایی از طریق ضرایب آلفای کرونباخ و پایایی ترکیبی (CR[11]) سنجیده می‌شود. همچنین روایی هم‌گرا به این اصل بر می‌گردد که شاخص‌های هر سازه با یکدیگر همبستگی میانه‌ای داشته باشند. طبق نظر مگنر، ولکر و کمپبل[12] (۱۹۹۶) معیار هم‌گرابودن روایی، این است که میانگین واریانس‌های استخراجی (AVE) بیشتر از ۰٫۵ باشد. ضریب پایایی ترکیبی نیز میزان همبستگی سؤال‌های یک بعد به یکدیگر را برای برازش کافی مدل‌های اندازه‌گیری مشخص می‌کند. مقدار آلفای کرونباخ و ضریب پایایی ترکیبی باید بالاتر از ۰٫۷ باشد. نتایج مربوط به روایی و پایایی پرسش‌نامه پژوهش توسط معیارهای یاد شده در جدول ۴ نشان داده شده است. همچنین شکل‌های ۲ تا ۵ مدل‌های اندازه‌گیری تحقیق در حالات تخمین استاندارد و ضرایب معناداری را نشان می‌دهند.

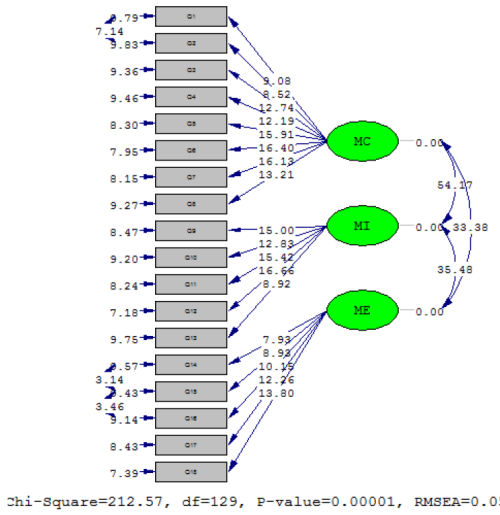
جهت ارزیابی برازش مدل این تحقیق، از شاخص‌هایی همچون کای دو بر درجه آزادی (χ^2/df) آماره شاخص ریشه میانگین مجذور خطا (RMEA[13]) P-Value و شاخص CFI استفاده شده است.

جذر برآورد واریانس خطای تقریب[14] که به‌صورت اعشاری گزارش می‌شود، بر پارامتر غیر مرکزی[15] مبتنی است. این شاخص برای مدل‌های خوب، برابر با ۰٫۰۵ یا کمتر است. مدل‌هایی که خطای تقریب آنها ۰٫۱۰ یا

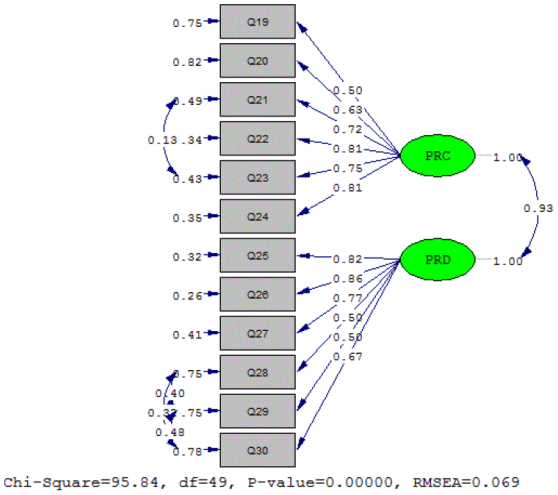
[11] Composite Reliability
[12] Magner, Welker & Campbell
[13] Root Mean Square Error of Approximation
[14] RMSEA
[15] Non centrality Parameter

جدول ۴: تحلیل عاملی متغیرهای مشاهده‌گر

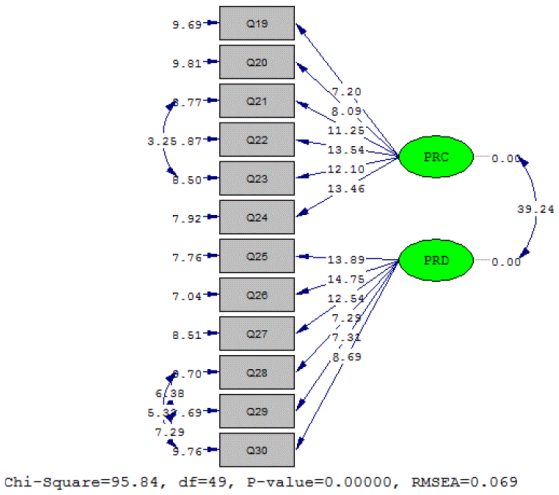
متغیر	نماد	ضریب عاملی	میانگین واریانس استخراجی (AVE)	پایایی ترکیبی (CR)
ارتباطات رسانه ای	MC۱	۰/۵۹	۰/۵۹۸	۰/۹۲۱
	MC۲	۰/۵۶		
	MC۳	۰/۷۷		
	MC۴	۰/۷۴		
	MC۵	۰/۸۸		
	MC۶	۰/۹۰		
	MC۷	۰/۸۹		
	MC۸	۰/۷۸		
اطلاع رساني رسانه هاي اجتماعي	MI۱	۰/۸۵	۰/۶۴۹	۰/۹۰۰
	MI۲	۰/۷۷		
	MI۳	۰/۸۷		
	MI۴	۰/۹۱		
	MI۵	۰/۵۹		
سهولت كاربري رسانه هاي اجتماعي	ME۱	۰/۶۴	۰/۵۰۰	۰/۸۲۸
	ME۲	۰/۶۰		
	ME۳	۰/۶۶		
	ME۴	۰/۷۶		
	ME۵	۰/۸۳		
ارتباطات در روابط عمومي	PRC۱	۰/۵۰	۰/۵۰۶	۰/۸۵۷
	PRC۲	۰/۶۳		
	PRC۳	۰/۷۲		
	PRC۴	۰/۸۱		
	PRC۵	۰/۷۵		
	PRC۶	۰/۸۱		
توسعة روابط عمومي	PRD۱	۰/۸۲	۰/۵۰۰	۰/۸۴۸
	PRD۲	۰/۸۶		
	PRD۳	۰/۷۷		
	PRD۴	۰/۵۰		
	PRD۵	۰/۵۰		
	PRD۶	۰/۶۷		



شکل ۳: مدل اندازه‌گیری تحقیق (ضرایب معناداری)



شکل ۴: مدل اندازه‌گیری تحقیق (تخمین استاندارد)



شکل ۵: مدل اندازه‌گیری تحقیق (ضرایب معناداری)

بیشتر باشد برازش ضعیفی دارند. شاخص برازندگی تطبیقی (CFT[۱۶]) اگر بزرگتر از ۰/۱ باشد، برابر با ۰/۱ و اگر کوچکتر از صفر باشد، برابر با صفر قرار داده می شود و همانند شاخص‌های قبلی چنانچه مقدار این کسر بین ۹۰ تا ۹۵ درصد باشد، قابل قبول تلقی می‌شود.

شاخص برازش، کای اسکوئر بهنجار یا نسبی از تقسیم ساده مقدار کای اسکوئر بر درجه آزادی مدل محاسبه می‌شود که اغلب مقادیر بین ۲ تا ۳ را برای این شاخص قابل قبول می‌دانند (عاقلی و آجرلو، ۱۳۹۷: ۱۴۵). شاخص‌های ارائه شده در این تحقیق برای مدل اندازه‌گیری رسانه‌های اجتماعی عبارت است از: $\chi^2/df = ۱/۶۷۴$، $RMSEA = ۰/۰۵۷$، $CFI = ۰/۹۹$، $NFI = ۰/۹۸$ که برازش مناسب مدل را نشان می‌دهد.

شاخص‌های مدل اندازه‌گیری روابط عمومی نیز به ترتیب عبارت است از: $\chi^2/df = ۱/۹۵۶$، $RMSEA = ۰/۰۶۹$، $CFI = ۰/۹۷$، $NFI = ۰/۹۶$ گویای برتزش مناسب مدل است.

پس از اطمینان از مقبول بودن مدل‌های اندازه‌گیری در مدل معادله ساختاری تدوین شده می‌توان به برآورد و آزمون مدل مفهومی پژوهش، از طریق مدل‌یابی معادلات ساختاری اقدام کرد. برای تعیین میزان تناسب مدل‌های ساختاری پژوهش شاخص‌های برازش محاسبه شدند که عبارتند از: $\chi^2/df = ۲/۱۴$، $RMSEA = ۰/۰۷۵$، $CFI = ۰/۹۹$، $NFI = ۰/۹۹$ که از برازش مناسب مدل حکایت می‌کند.

۵ بحث، نتیجه‌گیری و پیشنهادها

پژوهش حاضر با هدف طراحی الگوی به‌کارگیری رسانه‌های اجتماعی در راستای ارتقای فعالیت‌های روابط عمومی سازمان‌های خدماتی با رویکرد آمیخته صورت گرفت. بر اساس یافته‌های به‌دست آمده از مرحله

[16] Comparative Fit Index

کیفی، مضمون اصلی قابلیت‌های رسانه‌های اجتماعی سه مضمون فرعی ارتباطات رسانه‌ای، سهولت کاربری رسانه‌های اجتماعی و اطلاع‌رسانی رسانه‌های اجتماعی را شامل می‌شود و مضمون اصلی ارتقای فعالیت‌های روابط عمومی سازمان، مشتمل است بر دو مضمون فرعی ارتباطات در روابط عمومی و توسعه روابط عمومی.

به‌طور کلی، سازمان شهرداری نهاوند، به‌عنوان سازمان خدمات عمومی، نیازمند پاسخ‌گویی مداوم و آگاهی‌رسانی در زمینه‌های مختلف از جمله نقص‌های فنی حوادث و مسائل اجتماعی رخ داده در محیط خدمت‌رسانی این سازمان است. این موضوع با افزایش مطالبه‌گری و نیاز اطلاعاتی مخاطب امروز، برجسته‌تر شده است. از این رو، توسعه و ارتقای فعالیت‌های روابط عمومی شرایطی را برای شناسایی آسیب‌های احتمالی پیش‌بینی و بهره‌گیری از فرصت‌های محیطی فراهم می‌آورد. با عنایت به نتایج این پژوهش قابلیت‌های رسانه‌های اجتماعی با بهره‌مندی از ارتباطات رسانه‌ای اطلاع‌رسانی و سهولت کاربری می‌تواند در تحقق این امر یاری‌رسان روابط عمومی شهرداری نهاوند باشد. این قابلیت‌ها به عنوان پل ارتباطی و دیده‌بان نظام اجتماعی در انتقال مطالبات و انتظارات مردم و بیان دستاوردها و اقدام‌های سازمان‌های خدماتی نقش مهمی را ایفا می‌کند. از این رو بخش‌های خدمات عمومی همچون شهرداری نهاوند و حومه می‌بایست با بهره‌گیری از رسانه‌های اجتماعی شرایطی را در راستای توسعه ارتباطات و اطلاع‌رسانی دقیق فراهم کند تا ضمن تقویت تعاملات با مخاطبان توانایی پیش‌بینی مشکلات را داشته باشد و توان مقابله با تهدیدها را در خود تقویت کند. از این رو بازنگری فرایندهای ارتباطی در حوزه روابط عمومی جهت انعکاس خبری مؤثر فعالیت‌های متنوع سازمان و پاسخگویی مداوم در عرصه‌های مختلف به‌ویژه در راستای تحقق مأموریت روابط عمومی سازمان‌های خدماتی مورد انتظار است. این موضوع نشان‌دهنده ضرورت بهره‌گیری همه‌جانبه از ظرفیت‌های ارتباطی و ابزاری رسانه‌های اجتماعی و خلاقیت‌های مبتکرانه رسانه‌های اجتماعی با توجه به نیازها و تحولات مخاطبان امروز است.

در ادامه، بر اساس یافته‌های پژوهش، پیشنهادهای کاربردی ارائه می شود.

پیشنهاد می‌شود که شهرداری نهاوند و سازمان‌های فعال در بخش خدمات عمومی، با مشارکت در بحث‌ها و به اشتراک‌گذاری مسائل اجتماعی حال حاضر جامعه، ارتباطات قویتری را با مخاطبان ایجاد کنند. سازمان‌های خدمات عمومی می‌توانند با پرداختن به مسائل اجتماعی در کنار اخبار و اطلاعات مربوط به سازمان خود همدلی خود را با مخاطبان نشان دهند و ارتباطات اثربخشی را با آنها ایجاد کنند.

پیشنهاد می‌شود که شهرداری نهاوند حضور فعالانه و پاسخگویی در فضای رسانه‌های اجتماعی داشته باشد، به اتفاقات و مسائل رخ داده در محیط شهرداری واکنش مسئولانه نشان دهد و در رسانه‌های اجتماعی خود با شفافیت کامل اطلاع رسانی کند.

مراجع

[۱] رسولی، محمدرضا و هدایتی، محمدرضا (۱۳۹۶). نقش خلاقیت و عوامل مؤثر بر آن در کارایی روابط عمومی سازمان تأمین اجتماعی. ابتکار و خلاقیت در علوم انسانی، ۷(۲): ۲۱۷ – ۲۴۲.

[۲] زارعی، عاطفه و بیات، محمدکریم (۱۳۹۴). کارایی رسانه‌های اجتماعی در کتابخانه‌های دانشگاهی: مطالعه موردی دانشگاه‌های دولتی تهران. کتاب مهر، ۱۷ – ۱۸، ۹۸ – ۱۲۱.

[۳] نرگسیان، عباس؛ هژبرافکن خلاری، حسن؛ معینی کربکندی، محمدرضا (۱۳۹۴). مطالعه تأثیر رسانه‌های اجتماعی آن‌لاین بر شفافیت و اعتماد عمومی با اثر میانجی‌گیری مشارکت عمومی (مطالعه موردی: دانشجویان دانشگاه تهران). مدیریت دولتی، ۷(۳): ۶۳۷ – ۶۵۶.

[۴] مرادی، فاطمه (۱۳۹۶). بررسی تأثیر شبکه‌های اجتماعی در دنیای روابط عمومی (مطالعه موردی: شهرداری بابل). کنفرانس ملی رویکردهای نوین روابط عمومی ایران، اصفهان.

[۵] زینلی، حنانه؛ سلطانی‌فر، محمد و مظفری، افسانه (۱۳۹۷). بررسی نقش شبکه‌های اجتماعی موبایلی بر توسعه مشارکت اجتماعی. مطالعات توسعه اجتماعی ایران، ۱۰(۴): ۹۷ – ۱۰۸.

[۶] محمدی، افشین؛ مظفری، افسانه و خرازی، زهرا (۱۳۹۸). مدیریت جریان‌سازی خبری در روابط عمومی سازمان‌های دولتی. مطالعات رسانه‌ای، ۱۴(۱): ۲۳ – ۳۷.

[۷] کریمی راهجردی، اشرف؛ قوام، عبدالعلی؛ خرازی آذر، رها و گرانمایه‌پور، علی (۱۳۹۸). جایگاه شبکه‌های اجتماعی مجازی و پیام‌رسان موبایلی در شکل‌گیری خرد جمعی. مطالعات رسانه‌های نوین، ۵(۱۷): ۱ – ۳۴.

[۸] عاقلی، میثم و آجرلو، فاطمه (۱۳۹۷). اثر روزنامه‌نگاری برند بر قصد حمایت مشتریان از کسب‌وکارهای نوپای داخلی. فصلنامه علمی پژوهشی مدیریت برند، ۵(۱): ۱۳۵ – ۱۶۸.

[9] Statista (2021). Number of social network users worldwide from 2017 to 2025. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users

[10] Sutherland, K., Freberg, K., Driver, C. & Khattab, U. (2020). Public relations and customer service: Employer perspectives of social media proficiency. Public Relations Review, 46(4), 101954.

[11] Kent, M. L. & Li, C. (2020). Toward a normative social media theory for public relations. Public Relations Review, 46(1), 101857.

[12] Kent, M. L. & Taylor, M. (1998). Building dialogic relationships through the world wide Web. Public Relations Review, 24(3), 321–334.

[13] Allagui, I. & Breslow, H. (2016). Social media for public relations: Lessons from four effective cases. Public relations review, 42(1), 20-30.

[14] Al-Kandari, A. A., Gaither, T. K., Alfahad, M. M., Dashti, A. A. & Alsaber, A. R. (2019). An Arab perspective on social media: How banks in Kuwait use instagram for public relations. Public Relations Review, 45(3), 101774.

[15] Curtis, L., Edwards, C., Fraser, K. L., Gudelsky, S., Holmquist, J., Thornton, K. & Sweetser, K. D. (2010). Adoption of social media for public relations by nonprofit organizations. Public Relations Review, 36(1), 90–92.

[16] Adlmaier-Herbst, D. G. (2014). Public relations in the digital world: Global relationship management personal information. Digital media and social inclusion. Retrieved from https://www.researchgate.net/publication/270281374_Public_Relations_in_the_Digital_World_Global_Relationship_Management_Personal_information

[17] Boyatzis, R. E. (1998). Transforming qualitative information: Thematic analysis and code development. SAGE.

[18] Kline, M. (1990). Mathematical thought from ancient to modern times. (Vol. 2). Oxford University press.

[19] Magner, N., Welker, R. B. & Campbell, T. L. (1996). Testing a model of cognitive budgetary participation processes in a latent variable structural equations framework. Accounting and Business Research, 27(1), 41-50.

بازخوانی کارکرد دوسویه قوه خیال در سلطه‌ی سایبری بر مبنای علم النفس فلسفی

زهرا حبیبیان[۱]، عذرا جعفری موحد[۲]

[۱]دانش‌آموخته سطح سه فلسفه اسلامی جامعة الزهرا سلام‌الله علیها، قم و دانشجوی کارشناسی ارشد فلسفه و کلام اسلامی، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
habibian213@gmail.com
[۲]دانش‌آموخته سطح سه فلسفه اسلامی جامعة الزهرا سلام‌الله علیها، قم و فارغ‌التحصیل دکتری کلام امامیه، دانشگاه قرآن و حدیث، قم
jafarimovahed97@gmail.com

چکیده

در طول تاریخ، کنترل و سلطه بر دیگران دغدغه‌ی اصلی سلطه‌جویان بوده است. دانش سایبرنتیک محصول علم مدرن، با خاستگاه اومانیستی، به‌معنای کنترل و حاکمیت از طریق جریان اطلاعات است که در انسان با محوریت خیال رقم خورده و بستری نرم و نوین در اعمال سلطه محسوب می‌شود. قوهٔ خیال به تحلیل علم‌النفس فلسفی دو ساحت سلطه‌پذیر و سلطه‌گریز دارد. از یک سو سلطهٔسایبری با تخدیر خیال، ذائقه‌شناسی و ذائقه‌سازی در انسان، فاعلیت عقلانی نفس را زایل ساخته و نفس آدمی را با ایجاد کثرت در ارضای امیال شهوانی تا سر حد تسخیر در جهت اهداف سلطه پیش می‌برد. از سوی دیگر خیال در جنبه سلطه‌گریز خود پلی برای استقرار عقل بوده و در پرتو هدایت تکوینی و تشریعی، با قدرت زیبایی‌شناختی، عامل اصلی عزم، طریقی ضروری در سلوک و سپری در مقابل اعمال سلطه‌ی سایبری به شمار می‌رود. در سلطه‌ی سایبری، نوعی تسخیر باطل ایجاد می‌شود که به‌نحو علّی بر انسان مؤثر نبوده و به فاعلیت بالقصد او ضربه‌ای وارد نمی‌سازد؛ بلکه مسیر اختیار را با بازداشتن تمسک به تفکر و تعقل، یک‌طرفه ساخته و در مسیری خلاف مصلحت او سوق می‌دهد. بر این مبنا روش کنترل در سلطه‌ی سایبری با تعالی انسان در تقابل است. شناخت ساحت دوگانه‌ی خیال در سلطه‌ی سایبری، در پیشگیری و دفاع در برابر آسیب‌های نظام سلطه و نیز تنظیم نظامی متعالی مبتنی بر مبانی اسلامی، مؤثر است.

کلمات کلیدی: کنترل، سلطه‌ی سایبری، اومانیسم، خیال، فاعلیت بالتسخیر، زیبایی‌شناسی، هدایت.

۱ مقدمه

سلطه‌گری و نظام مبتنی بر آن یکی از انواع نامطلوب حکمرانی است که دیرینه‌ای به قدمت حیات بشر دارد و سایبر، ابزار و روشی نوین در اعمال آن محسوب می‌شود.

دانش سایبرنتیک، محصول نظریات نوربرت وینر در سال ۱۹۴۸ میلادی، هم‌زمان با پیشرفت علم مدرن و رشد فنّاوری، در فضای فکری – فلسفی ضدیت باخدا و رغبت به اومانیسم[1]، به‌عنوان دانش کنترل جریان اطلاعات در ماشین‌ها، سیستم‌ها و موجودات زنده شکل گرفت. وینر در تبیین سایبر از واژه‌ی کنترل و فرمان، بهره برده است. سایبر بعدها در مطلق فرمان و کنترل موجودات، اعم از طبیعی و مصنوعی کاربرد یافت. ترکیب سلطه و سایبری و اعمال آن بر انسان، روشی نرم در کنترل انسان را فراروی قدرت‌ها قرار داد.

قوه خیال ازجمله قوای مؤثر در فعل و انفعالات اختیاری انسان است که ظرفیت‌های بی‌نظیری در تنوع انگیزش و کنش و نیز پذیرش سلطه و نفی آن دارد؛ از این‌رو حلقه واسط سلطه‌سایبری و انسان محسوب می‌شود. بازخوانی تفسیری که علم النفس فلسفی در کارکردی دوسویه از خیال به‌عنوان مثال متصل و ارتباطش با مثال منفصل و عوالم بالاتر ارائه داده‌است، در روشن ساختن تناسبی که میان خیال انسانی و سلطه‌سایبری وجود دارد، راه‌گشا است. به علاوه، این بازخوانی به هدف پاسداری از سلطه‌پذیری انسان، شناخت ریشه‌ها و راه‌های نفوذ دشمن از طریق کنترل خیال و ایجاد خطای شناختی در آن و نیز ارائه‌ی راهکارهای ساحت سلطه‌گریز خیال در مقابل سلطه‌ورزی سایبری، ضروری است.

پژوهش‌های مرتبط با مسئله این جستار در چهار حالت صورت‌بندی شده است: برخی به نحو ممتاز به بررسی سلطه، سایبر و خیال پرداخته‌اند؛ دسته‌ای ارتباطشان با این مسئله در حد اشتراک در پاره‌ای از مباحث است؛ شماری نیز تمرکز بر تبیین جزئی اخص از آن داشته و جمله‌ای نیز تحلیلی ضمنی در حواشی تحقیق‌اند و هیچ‌کدام به نحو مبسوط بر خیال در نسبت سلطه‌سایبری، متمرکز نشدند.

در مسیر حل مسئله این تحقیق، با روش توصیفی – تحلیلی، به تحلیل مفاهیم کلیدی عنوان پرداخته، سپس پس از ترسیم جایگاه خیال در علم النفس فلسفی، کارکرد دوگانه‌ی خیال با تأکید بر بعد سلطه‌پذیر آن در نسبت سلطه‌سایبری تبیین می‌شود و در پایان ترسیمی که علم النفس فلسفی از بعد سلطه گریز خیال داشته و راهکاری که در سلوک و نفی سلطه ارائه می‌دهد، تقریر می‌شود.

۲ تحلیل مفاهیم

عمده مباحث فلسفی در زمینه‌ی خیال، محض و بنیادی است؛ از این‌رو پیشروی در سیر راهبردی موضوع جستار حاضر، به تحلیل ماهوی و متناظر عناصری نظیر سلطه، سایبری و خیال، نیازمند است.

۱.۲ معناشناسی سلطه و انواع آن

سلطه در لغت به معنای قهر و چیرگی (ابن منظور، ۱۴۰۸: ۶/۳۲۶) و از منظر جامعه‌شناختی، به رابطه‌ای مقرون باقدرت میان دو شخص و یا دو دولت اطلاق می‌شود (علی‌بابایی، ۱۳۶۹: ۱۲۶).

[1] Humanism

سلطه در نظر ماکس وبر یعنی: «گردن‌نهادن گروهی از افراد به احتمالی که محتوای مشخصی دارد» (راسل، ۱۳۶۷: ۵۵) و در دیگر تعابیر، قدرت از آن حیث که «امکان تحمیل اراده خود بر رفتار دیگر افراد است» سلطه نامیده می‌شود. (راش، ۱۳۷۷: ۵۸) براین‌اساس سلطه قدرتی مقید است و قدرت در معنا، توانمندی افراد و گروه‌ها در به کرسی نشاندن منافع و امیال خود، علی‌رغم مخالفت دیگران است (صولتی، ۱۳۹۰: ۵۳) و می‌توان آن را به سه دسته‌ی الهی، ماشینی و انسانی تقسیم کرد.

سلطه در قرآن به معنای حجت و برهان و در برخی موارد، به سیطره شیطان بر بندگان اطلاق شده است (خالقی بایگی و همکاران، ۱۳۹۸: ۱۵۹). در برخی تعابیر نیز، هم‌تراز با حکمرانی و سلطنت قلمداد شده و ناظر به بعد کمالی آن، برداشتی مثبت از آن شده است (مصباح یزدی، ۱۳۸۲: ۱۱۴)؛ درحالی‌که در معنای سلطه نوعی تحمیل نفسانی برتری‌جویانه وجود دارد؛ از این‌رو ارزش معنایی آن منفی است و حکمرانی بر اساس آن در زمره حکمرانی نامطلوب قرار می‌گیرد.

سلطه و استخدام در تعابیر فلسفی، روحیه‌ی غلبه و به استخدام درآوردن دیگری و استثمار آن به هدف رفع نیازهای خود است و با توسعه در معنا، استخدام به هدفی متعالی، ازجمله گرایش‌های غریزی و فطری آدمی است (طباطبایی، ۱۳۶۴: ۲۰۲-۲۰۴) که شکل جبر و تحمیل قدرت در آن، معنای سلطه را می‌سازد. استخدام در انسان با هدفی خردورزانه و متکی بر عقلانیت ابزاری رخ می‌دهد (مطهری، ۱۳۶۳: ۱۹۹) لذا ارزشی خنثی دارد. ولی چنانچه مبدأ آن صرفاً امیال نفسانی باشد؛ نظیر سلطه، بار منفی داشته و اگر ناشی از عقلانیت الهی و فطری باشد جلوه‌ای متعالی می‌یابد (مدقق، شرف‌الدین، ۱۳۹۸: ۶۳)؛ از این‌رو سلطه، استخدام مقیدی است که برخاسته از نفسانیت و تحمیل اراده رخ می‌دهد و تفاوتی در فاعلیت انسانی و غیرانسانی آن نیست؛ بلکه هر موجود واجد تصمیم‌گیری را شامل می‌شود.

بنابراین تمایز سلطه و استخدام، در کاربرد و عدم کاربرد جبر و تحمیل است.

گونه‌های سلطه در دو دسته مادی و معنوی ترسیم می‌شود. سلطه مادی، غلبه قدرت انسان بر انسان به روش‌های مختلفی مانند توسل به خشونت، ایجاد وابستگی و ضعیف‌سازی متعلقِ سلطه است. فرمان و کنترل جریان اطلاعات در سیستم‌ها و موجودات زنده نیز که با نام سایبرنتیک اطلاق می‌شود، به‌روزترین معنا از روش‌های اعمال سلطه مادی است که محصول مدرنیته و عصر روشنگری تلقی شده و امروزه در مباحث سیاسی و حکمرانی جایگاهی ویژه یافته است. این سلطه نوین، با درگیر ساختن امیال و ادراکات و در بستر خیال، بدون قطع ارتباط با ادوات مادی، اراده خود را به فاعلیت نفس انسانی تحمیل می‌سازد.

سلطه در روش معنوی، تحمیل اراده بر خلاف خلقت تکوینی و تشریعی بوده و غیرالهی است و در مصادیقی نظیر فاعلیت تسخیری اجنه، شیاطین و در سطح نازل آن، در سلطه‌های روانی و به اصطلاح کاریزماتیک جریان دارد و وابسته به میزان قدرت وجودی و مثالی سلطه‌گر و ضعف مثالی متعلق سلطه، اراده او را دچار اختلال می‌سازد.

از منظر نظام توحیدی و ولایی، سلطه مطرود است. چرا که در تمام مصادیق آن، تحمیل اراده و یک‌طرفه‌سازی مسیر اختیار متعلق سلطه بوجود می‌آید؛ در گونه‌های مادی آن، در روش اعمال زور با کاربرد خشونت، در روش تضعیف سازی با تأثیر و تحریک روانی، و در روش سایبرنتیک با مسدودسازی مسیر انتخاب عقلانی در نتیجه غلبه شهوانی وهمانی و در گونه‌های معنوی آن نیز، یک‌طرفه سازی همراه با تسخیر در

مرتبه‌ای از مراتب مثالی و وجودی فرد رخ می‌دهد.

جایگزین سلطه در نظام توحیدی، هدایت است که در جهت‌دهی به متعلق خود، دو بستر تکوین و تشریع را شامل می‌شود. در بستر تکوین، با عنوان هدایت تکوینی، به نحو احاطی و علّی، اصل وجود متعلق خود را در بر دارد و به نوعی خود اراده و وجود متعلق است؛ نه تحمیل آن و در بستر تشریع نیز با عنوان هدایت تشریعی، به معنای سنگین‌تر کردن کفه‌ی انتخاب عقلانی (ر.ک به حدیث: مجلسی، بیتا: ۴۳ /۳۶۳) با ارزش‌گذاری‌های مکرر و اعمال انذار و تبشیرها است و نمونه آن برانگیزی و احیای عقول توسط انبیا[۲]، هدایت مردم تا سرحد رسیدن به قدرت برپاداری عدالت[۳] و همچنین هدایتی است که در امر به معروف و نهی از منکر وجود دارد؛ در حالی که در تمام این بسترها، جهت دهی به متعلق، بدون اعمال جبر و تحمیل اراده رخ می‌دهد.

۲.۲ سلطه در کاربست سایبری

سلطه پیش از عصر مدرنیته و عصر روشنگری به شیوه سنتی و مرسوم نظیر خشونت و ارعاب اعمال می‌شد؛ اما با ظهور مدرنیته، در قالب نظریات جامعه‌شناسانه و فلسفی، ساختار نوینی یافت.

در این عصر در واکنش به فلسفه و مذهب در ساختار منحرفش، بنیاد دنیوی – تجربی، جانشین بنیاد دینی – عقلانی شده و از آن، نگره اومانیسم، پوزیتیویسم، سکولاریسم و سوبژکتویسم زاده شد (صولتی، ۱۳۹۰: ۱۴ و ۱۵).

با تکیه‌بر عقل خود بنیاد، خردورزی هم‌تراز عقلانیت و عقلانیت به‌مثابه رفتار محاسبه‌پذیر تلقی و بر محور منافع، مفهوم «جامعه بازار» ارائه شد (همان: ۱۹) و مفاهیمی نظیر توسعه، صرفاً تقریر کمی یافت و بنیاد ارزش‌ها بر اقتصاد بنا گردید.

در همین بستر قدرت اصالت یافت و پایه‌های تمدن مدرنیته، بر مبنای سلطه‌جویی و سرمایه‌داری شکل گرفت و اساس حکمرانی، دانش و فرهنگ آن را سامان داد (مصباح یزدی، ۱۳۷۶: ۳۷). درحالی‌که محتوای بنیاد چنین نظامی را دیگر نه وحی؛ بلکه خرد خود بنیاد بشری می‌ساخت (سید محمد حکاک، ۱۳۸۰: ۶).

اراده معطوف به قدرت[۴]، نظریه معروف نیچه، هم‌راستا با تعابیر هابز و فرانسیس بیکن بر گسترش و تثبیت بنیاد اصالت قدرت افزود.

محصول چنین بنیادی در غرب، غارت ثروت، تجاوز و تصاحب مملکت، تحریف تاریخ و فرهنگ و سانسور وقایع مثبت تاریخی کشورهای دیگر را به نفع نظام سلطه به دنبال داشت. (مصباح یزدی، ۱۳۷۶: ۳۷) در دل تحول عصر مدرن در بنیاد، عقاید، نگره به مذهب، فلسفه و علم، دانش سایبرنتیک در پوشش جدید اعمال سلطه، متولد شد.

سایبرنتیک[۵] در زبان یونانی به معنای «هنر هدایت‌کردن» (بابایی و همکاران، ۱۴۰۰: ۲۲) و در برخی

[۲] ویثیروا لهم دفائن العقول (نهج البلاغه، خطبه ۱)
[۳] لِيَقُومَ النَّاسُ بِالْقِسْطِ (حدید/۲۵)

[4] Will to Power
[5] Cybernetics

تعابیر معادل کوبرنتیس[۶] به معنای «سکان‌دار» است که در ترجمه لاتین، گاونر[۷] یا حکمران معنا می‌شود (وینر، ۱۳۶۶: ۱).

سایبرنتیک دانشی است که به مطالعه‌ی مفاهیم کنترل و ارتباطات در موجودات هوشمند و سیستم‌ها باهدف فهم و ساخت سیستم‌هایی که بتوانند به اهدافشان برسند (بابایی و همکاران، ۱۴۰۰: ۳۶)، پرداخته و با بررسی نحوه‌ی پردازش سیستم‌ها (دیجیتالی، مکانیکی یا بیولوژیکی) درصدد کنترل و هدایت آن برمی‌آید (همان: ۲۴).

نخستین بار نوربرت وینر، ریاضیدان آمریکایی – لهستانی، در سال ۱۹۴۸ متأثر از دوران مدرن و فرهنگ مدرنیته با نگرش ماشینی و اومانیستی به انسان، ضمن طرح نظریه سایبرنتیک به تدوین دانش آن همت گماشت. فرمان، کنترل و سیستم از واژگان کلیدی دانش اوست که در معنایی عام، سلطه را در ساختاری نوین کاربردی ساخته است و امروزه به زیرشاخه‌های متعددی نظیر بایوسایبرنتیک[۸] و به‌اختصار، اکو[۹]، سایکو[۱۰] و سوسایوسایبرنتیک[۱۱] تقسیم شده و نیز در دسته علوم سیاسی وجه‌اشتراک یافته است.

نظریه وینر بر ساحت ادراکی و جنبه ظریف موجود هوشمندی نظیر انسان، یعنی جریان اطلاعات و آگاهی تکیه دارد. سایبرنتیک برخاسته از تحلیل شباهت‌های صوری میان انسان و سیستم، وی و جامعه انسانی را به مثابه ماشین قابل‌کنترل می‌داند (همان:۲۶).

سلطه‌سایبری، ترکیب سلطه در بستر سایبری، اشراف بر جامعه و انسان‌ها و کنترل آن‌ها از طریق جریان آگاهی در قالبی نامحسوس است و از جایی‌که تنها راه اعمال سلطه بر انسان با محور ادراکی و احساس رقم می‌خورد، خیال نقش برجسته‌ای در آن ایفا می‌کند. این نظریه، راهبردی برای تحمیل سلطه در بستری نرم در نظام سلطه ایجاد کرده و در قالب رسانه، تکنولوژی، هوش مصنوعی، متاورس، گیم و غیره کاربرد یافته است.

اعمال قدرت در غرب بر اساس نوع رویکرد به آن، چهره‌های مختلفی مانند تک‌بعدی، دوبعدی و سه‌بعدی و ... دارد. در عرصه سلطه‌سایبری رویکرد سه‌بعدی قدرت مدنظر است. قدرت در این معنا می‌تواند بر افکار و امیال قربانیانش نفوذ کند، بدون اینکه آن‌ها از این تأثیر آگاهی یابند (هیندس، ۱۳۸۰: ۶و۷).

فضای سایبر به‌عنوان بستر سلطه‌سایبر، محیطی مصنوعی، الکترونیکی و غیرفیزیکی در نظام‌های رایانه‌ای است که از مسیر آن اطلاعات ایجاد، ارسال، دریافت، ذخیره، پردازش و حذف می‌شوند (کامران دستجردی و محمدی، ۱۳۹۳: ۱۴۵). ارکان سلطه‌سایبری را انسان، فضای سایبر، عامل سلطه، محتوای سلطه و محور اعمال قدرت، ظرف ادراکی و احساسی آدمی یعنی خیال، تشکیل می‌دهد.

---

[6] Kubernetes
[7] Governor
[8] Biocybernetics
[9] Ecocybernetics
[10] Psychocybernetics
[11] Sociocybernetics

۳.۲ ماهیت و ابعاد خیال

خیال در لغت به معنای گروه اسبان (خلیل جر، ۱۳۶۷: ۱/ ۹۴۸)، ظن و گمان (قریشی، بی‌تا: ۳/ ۳۲۰ و ابن‌منظور، ۱۴۰۸: ۱۱/ ۲۲۶)، تلوّن و رنگارنگی (احمدبن فارس، ۱۴۰۴: ۲/ ۲۳۵)، پنداره‌ای برساخت از رؤیا و بیداری (طریحی، بی‌تا: ۵/ ۳۶۷) و حالتی مؤثر در تفاخر و عجب (حسن مصطفوی، ۱۳۶۰ : ۳/ ۱۶۴)، به‌کار رفته است و در اصطلاح فلسفی فارغ از اختلافات و با تکیه‌بر نظر صدرالمتألهین، بستری مثالی – تجردی است که در سه ساحت هستی شناختی، معرفتی و انسان‌شناختی، در سه معنای مثال منفصل، مثال متصل و نفس مثالی، اشتراک داشته و ناظر به هرکدام کارکردی مخصوص دارد.

مثال یا «خیال منفصل» در ساحت هستی شناختی، یکی از مراتب عالم هستی و محور وصل عالم عقل و طبیعت بوده (قیصری، ۱۳۷۵: ۹۷) و منفصل و مستقل از عالم محسوسات و ابتدای عالم روحانی است (شیرازی، ۱۳۹۰: ۴۹۵).

مثال یا «خیال متصل» با اطلاق «قوه خیال» بر آن، در ساحتی معرفتی، مخزن صور و معانی جزئیه برگرفته از خارج و نیز خالق صور و معانی ابداعی حسی و خارجی است (جوادی آملی، ۱۳۸۶: ۲۰/ ۳۱۳).

«نفس مثالی» یا خیالی در ساحت انسان‌شناختی، مرتبه مثالی نفسانی انسان است که باقابلیتی دوگانه، به همراهی خیال متصل و دیگر قوای نفس، نظیر واهمه و متخیله، نقشی فعلی و انفعالی در بستر مثال ایفا می‌کند و در آغاز تکوین تکاملی نفس، پس از گذار از جسمانیت، اولین مرتبه ادراکی و روحانی نفس را ایجاد می‌نماید (شیرازی، ۱۳۹۳ : ۸/ ۲۱۳؛ مصباح یزدی، ۱۳۹۳: ۱/ ۴۰۱ و۴۰۲).

در این پژوهش، مقصود از قوه خیال با کارکرد دوسویه، بستر مثالی نفس در ارتباط با مثال متصل است که ظرف سلطه‌پذیری و سلطه‌گریزی انسان را فراهم ساخته است.

۳ جایگاه خیال در علم النفس فلسفی

در علم النفس فلسفی، خیال، برزخ حس و معنا (جوادی آملی، ۱۳۸۶: ۱۹/ ۴۸۵-۴۸۷) و ابزار مثالی نفس است. با وجود اشتراک انسان و حیوان در وجدان این قوه و اثرش در فاعلیت، این قوه در انسان به جهت اختصاص او به مصوره، مفکره، عاقله و نیز قوت بیشترش، از حیوان تمایز می‌یابد (ابن عربی، ۱۲۹۳: ۳/ ۳۸-۴۶).

علاوه بر این با قدرت شگرفی که در دستگاه ادراکی نفس دارد، تأثیر مستقیمی در فاعلیت آن داشته و با کارکردی دوسویه مبتنی بر غلبه هر یک از قوای حیوانی و انسانی، به سمت سلطه‌پذیری و سلطه‌گریزی جهت می‌گیرد. در واقع از جهت مجرد خود، بابی به ملکوت دارد و می‌تواند با اطاعت از فرامین عقل، سرمایه‌های فطری خویش را شکوفا و حقایق را در قلب منعکس سازد و از جهت مادی خود، بابی به عالم طبیعت دارد و می‌تواند با سرپیچی از فرمان عقل، ظرف کثرات و متعلق سلطه گشته و به ناتوانی و فساد ادراکی و تعطیلی عقل منجر شود.

۱.۳ خیال و فاعلیت

در حکمت متعالیه علم و شوق به‌منزله‌ی مبادی علمی؛ و قوای عامله و اراده به‌مثابه مبادی عملی، خاستگاه ضروری فاعلیت نفسِ ذی‌شعور محسوب می‌شوند (سبزواری، ۱۹۸۱، ۶/ ۳۸۸). مبادی علمی که با ایجاد مبادی شوقی منجر به ظهور مبادی رفتاری شده است، به دو قسم عقلی و خیالی تقسیم می‌شوند.

ازنظر صدرا تمامی فعالیت‌های عقلی و خیالی در مبدأ علمی و تمامی غایت اندیشی‌ها در مبدأ شوقی، مستقیم و بی‌واسطه، با استعانت از خیال صورت می‌گیرد (شیرازی، ۱۳۶۳: ۵۷۵ به نقل از: وفاییان، ۱۳۹۵: ۱۲۹) و هرگونه فعلی هرچند با مبدأیت علمیِ عقلی، نظیر تفکر و ادراک کلیات، در ظرف خیال و با استعانت از الفاظ و کلام ذهنی حاصل می‌شود (شیرازی، ۱۳۵۴: ۳۰۷)؛ از این‌رو نفوذ خیال در افعال انسانی به حدی گسترده است که رفتارهای عبادی انسان را نیز شامل شده و به دلیل وسعت فراگیری آن در عالم طبیعت و مثال، رفتار عقلی محض از انسان را ممتنع ساخته است.

علاوه بر این، تفاوت فعل با مبدأیت عقلی از فعل با مبدأ خیالی در این است که فعل خیالی دیگر از همراهی عقل برخوردار نیست، هرچند که فاعلیت عقلی همواره همراه و در بستر خیال رخ می‌دهد (همان: ۱۵۴).

در فرآیند فاعلیت ارادی انسان، ابتدا صورتی علمی مشتمل بر تصور و تصدیق به‌فایده آن بوجود می‌آید. این صورت یا از او صادر شده یا درنتیجه انفعال از خارج به دست می‌آید؛ پس از تصور غایت و تصدیق به‌فایده آن بر مبنای عقل یا خیال، اشتیاقی انفعالی به‌سوی انجام فعل، برآمده از قوای شهویه، غضبیه یا قوه عقل عملی در او پدید می‌آید (طباطبایی، ۱۴۰۲: ۱۲۱-۱۲۲).

در مبدأیت علمی، به میزان لطافت و طهارت خیال و نفس مثالی، قوای عقل عملی انسانی فرصت بروز و غلبه می‌یابد.

در نظر بوعلی اولین مبدأ تحریک بدن در انسان قوه خیال و دومین آن قوه عاقله است؛ حتی در حیوانات که در جنس مثالی هم‌ردیف انسان هستند قوه خیال مبدأ تحریک است (طوسی، ۱۳۷۵: ۱۷۲).

این تحریک از مجرای در اختیار قرار دادن صور خیالی در خدمت واهمه، متصرفه، حسّ مشترک و به‌نوعی عقل عملی است و در مرحله شکل‌گیری شوق در انسان، صور خیالی نقش اساسی را ایفا می‌کنند (ابن‌سینا، ۱۳۶۳: ۱۸۴).

علاوه بر همراهی خیال در مبدأیت عقلی، از مجاری دیگر تحریکِ قوه خیال در افعال انسان، لذت‌جویی آن است؛ چنانچه صدرا در برخی آثار خود ذیل بحث سعادت حقیقی تصریح کرده است که هرکدام از قوا، لذّت خویش را دارا است و آن را می‌طلبد (شیرازی، ۱۳۶۰: ۲۴۹؛ همان، ۱۳۶۳: ۵۸۶).

بر همین اساس در تخیل برخلاف تصدیق، لذت‌جویی مبدأیت دارد و همین امر به قبض و بسط نفس در بستر خیال کمک می‌کند (چمن‌خواه ۱۳۸۴: ۲۵).

از این‌رو خیال و صور خیالی در پرتو خیال‌انگیزی و تحریک قوا می‌توانند نفس را منفعل ساخته و فاعلیت آن را تحت‌تأثیر قرار دهند.

۲.۳ خیال و قوای حیوانی

نفس حیوانی با قوای ادراکی و تحریکی، از نفس نباتی متمایز می‌شود. قوای ادراکی نفس دو قسم‌اند: حواس ظاهر و قوای باطن. حواس ظاهر عبارت‌اند از: باصره، سامعه، ذائقه، شامه، لامسه. قوای باطن عبارت‌اند از: حس مشترك، خیال، وهم، حافظه و قوه متصرفه (شیرازی، ۱۳۶۰: ۱۹۳). قوای تحریکی نیز شامل قوای نزوعیه (شهویة و غضبیة) و فاعله می‌شود.

خیال متصل در بستر مثالی نفس از یک‌سو عهده‌دار حفظ محصولات حس مشترک است که از محسوسات به‌دست آمده و از دیگر سو مدرَک حس مشترک می‌باشد. داده‌های خام خیال در راستای تحقق افعال خارجی و ذهنی، توسط قوه واهمه، متصرفه و متخیله مورداستفاده قرار می‌گیرد. قوه متصرفه گاه به ترکیب و تفصیل صور موجود در خیال پرداخته (شیرازی، ۱۳۸۷: ۱۷۶۴-۱۷۶۵) و قوه متخیله نیز عهده‌دار تکثیر و تجسیم مفاهیم است (شیرازی، ۱۹۸۱: ۳/ ۳۶۷).

وهم نیز در نسبتی اعم مطلق از خیال متصل که مدرک صور جزئی است، مدرک معانی جزئیه است و با مراجعه به خزانه‌ی صور خیالی از آن بهره می‌جوید (خمینی، ۱۳۸۹: ۲/ ۴۳۵).

قوه واهمه برای ادراک فعلی که مبتنی بر صورتی خیالی باشد، وارد عمل می‌شود و از این‌رو در خدمت خیال است (شیرازی، ۱۹۸۱، ۸/ ۲۱۵).

ملاصدرا قوه متصرفه را نیز در خدمت وهم دانسته و وهم را رابط میان عقل و متصرفه برشمرده است و همواره تأکید می‌نماید که قوه عاقله، در افعال خود، دیگر قوا را از مجرای قوه واهمه به خدمت می‌گیرد. (همان) واهمه با انجام تصدیق، واسطه عقل با محسوسات می‌گردد؛ زیرا عقل در بستر خود تنها مفاهیم ضروری فطری را دارد و جز با وساطت تصدیق وهمانی، مفاهیم و تصدیقات غیرضروری را نمی‌پذیرد (فتوحات، ۱۲۹۲ق: ۳/ ۳۶۴). از این‌رو وهم گاهی با تصدیقات نابه‌جا و سرایت حکم محسوسات به غیرمحسوسات، عقل را به خطا وامی‌دارد (سهروردی، ۱۳۷۵: ۲/ ۴۲).

ضعف یا قوت نفس مثالی در مشاهدات عالم مثال منفصل و نیز ضعف یا قوت ادراکات معنوی در عبور آن از مسیر وهم، متصرفه، متخیله و ضبط آن در خزانه خیال و ایجاد شوق در تداعی حافظه و ذاکره در برجسته ساختن خواطر مؤثر است. از دیگر سو، خیال متصل در بستر نفس مثالی در جذب یا دفع قوای محرکه نزوعیه مؤثر است. قوه شهویه به‌محض دریافت و تصور صُور لذت‌بخش خیالی، نفس را به‌سوی جذب آن تشویق می‌کند (صمدی آملی، ۱۳۹۰ :۶۶۱)؛ زیست بدنی – حیوانی انسان، در این دنیا منوط به این قوه و طمع، میل به فساد و تمامیت‌خواهی شهوانی ازجمله امیال آن می‌باشد. تحریک خیالی این قوه، هیجانات آن را غالب ساخته و در مقابل قوه عقل عملی می‌شوراند (نراقی، ۱۳۹۰: ۳۹).

قوه غضبیه به‌محض درک صور مضر و بی‌فایده خیالی، نفس را به دفع آن وادار می‌سازد (صمدی آملی، ۱۳۹۰: ۶۶۱). دفع مضرات و دفاع از خویشتن، منوط به این قوه و شرارت، طلب ظلم و عداوت‌جویی از امیال ذاتی آن است و نظیر قوه شهویه با تکیه‌بر تمامیت‌خواهی، در مقابل عقل قرار داشته و به غلبه بر نفس مایل است (نراقی، ۱۳۹۰: ۴۰). از ویژگی‌های شاخص این دو قوه تربیت‌پذیری است که در ظرف خیال امکان تحقق دارد.

همان‌گونه که پیداست، از میان قوای حیوانی، ارتباط نفس خیالی و خیال متصل با قوای تحریکی شهویه و غضبیه و قوه ادراکی واهمه و متخیله، سبب ایجاد و غلبه اشتیاق و درنتیجه تحت‌تأثیر قرار دادن فاعلیت شده و از این طریق، امکان یا ممانعت از سلطه را فراهم می‌سازد.

۳.۳ خیال و قوای ناطقه، فطرت و عقل منور

قوای حیوانی، محل کثرت، هیجانات و بی‌ثباتی و قوای ناطقه، محل وحدت، ثبات و رسیدن به حد خودکنترلی است.

منظور از قوای ناطقه، عقل عملی و نظری است. عقل عملی موطن تشخیص حسن و قبح بوده و در بستر خیال با ذخیره‌ی صور فطری، نفس را به سمت تصدیقات فطری – الهی سوق می‌دهد. عقل نظری نیز موطن ادراک ضروریات بوده و در صورت صفای قلب (نفس خیالی)، بستر انفعال و ادراک از عوالم بالاست.

فطرت به معنای سرشت نیز بینش و گرایش‌هایی عالی است که هم‌زمان با خلقت تکوینی در وجود انسان نهاده می‌شود (مطهری، ۱۳۹۱: ۳/ ۴۴۵). تشخیص مصادیق تمایلات فطری بسته به خاستگاه مبدأ علمی افعال (خیالی یا عقلی) تعیین می‌شود.

عقل منور یا عقل الهی نیز لایه‌ی سومی غیر از نفس مثالی و بعد حیوانی انسان است؛ خودِ خودِ خود او تفسیر شده و امانت نهان الهی و ناشناخته‌ترین بعد آدمی است. عقل الهی که در لسان شریعت «روح» نامیده شده است، ودیعه الهی و حکمران حقیقی نفس آدمی است. خیال، بستر میانی و واسطه ارتباط این لایه‌ی وجودی نفس، با طبیعت اوست (جوادی آملی، ۱۳۹۳ : ۹۲).

نقش خیال در ارتباط با قوای ناطقه، فطرت و عقل الهی بیشتر انفعالی است تا فعلی؛ هرقدر خیال در تبعیت این قوا درآید، خیال‌انگیزی‌ها و معارف عالی و از این بستر طهارت قلب و وهم، مجال می‌یابد.

در غیر این صورت، انسان به میزان ضریبی که در گزینش امیال دارد، بستر مثالی نفس که جایگاه قلب است را در جهت حاکمیت یکی از قوا فراهم می‌سازد.

۴ کارکرد خیال در سلطه‌سایبری

همان‌گونه که در معناشناسی سلطه‌سایبری بیان شد، کنترل و فرمان سیستم‌های هوشمند و غیرهوشمند، محور سایبرنتیک است. همچنین سلطه‌سایبری، حاکمیت بر جریان آگاهی انسانی و مقهورسازی اوست و این امر در بستر خیال میسر است.

از نظر وینر، سیستم‌های زنده و غیرزنده می‌توانند دارای هدف (در اصطلاح سایبر) باشند؛ یعنی: قابل پیش‌بینی، کنترل و برنامه‌ریزی باشند (بابایی و همکاران، ۱۴۰۰: ۲۴ و ۹۳) و تبیین رفتارهای سیستمی پیچیده نظیر انسان، نیازمند عامل بیرونی نبوده و می‌توان آن‌ها را با خوانشی مکانیستی تفسیر کرد (همان: ۳۳).

بر مبنای نگرشی که وینر بر انسان و امکان کنترل او از طریق جریان آگاهی داشت، آندره امپرماری ارتباط علوم سیاسی و سایبرنتیک را برای نخستین بار طراحی کرد (همان:۳۵) و پای سلطه و حکمرانی را

به‌طور رسمی به جریان نرم ذهن، با محوریت خیال کشاند.

خیال همان زبان و عنصر مشترکی است که فارغ از تمام محدودیت‌ها و شاخصه‌های جغرافیایی، مذهبی، فرهنگی – اجتماعی و قومی – قبیله‌ای می‌تواند انسان را تحت سیطره و نفوذ خاموش و پنهانی قرار دهد.

امروزه آثار سلطه رسانه، نمونه و مصداقی ملموس از اعمال سلطه‌سایبری در ظرف خیال است.

مک لوهان، از افراد شاخص مطالعات رسانه معتقد است: تأثیر رسانه به قدری عمیق است که هیچ تلاشی از جسم و روانمان را دست‌نخورده باقی نمی‌گذارد. ابزار و وسایل ارتباطی، نه تنها رابطه انسان و طبیعت بلکه طبیعت انسان مدرن هستند (مک‌لوهان، ۱۳۷۷: ۱۲۲).

جهان فناورانه امروز دیگر نه با ابزارهای سخت و قابل رؤیت، بلکه به شکلی نرم، در حال تغییر بینش‌ها، گرایش‌ها، کنش‌ها و سبک زندگی کاربران آن است (بابایی و همکاران، ۱۴۰۰: ۴۵).

ژان بودریار نیز معتقد است، رسانه‌ها ابزاری برای بی‌ثبات‌سازی واقعیات هستند؛ ولی انسان، به ندرت به تأثیرپذیری نگرش خود توسط رسانه‌ها، توجه دارد (حسینی، ۱۳۸۸: ۱۷۴–۱۸۱). این سخنان، شاهدی بر تأثیرپذیری و امکان سیطره بر خیال هستند.

در این میان اهمیت و کارکرد قوه خیال کاملاً دوسویه بوده و مرزی میان سعادت و شقاوت انسان است. از یک سو خیال قابلیت‌هایی کیهانی و فراکیهانی، نظیر کشف و مشاهده اسرار، نیل به عالم قدسی و هنر و جذبه‌های متعالی، تلقی وحی و الهام داشته و از سوی دیگر با سیر در امور شهوت‌انگیز، قوی‌ترین ابزار شیطان و وجوه مختلف سلطه در جهت پرورش آرزوها و و نیل به پستی‌ها است. وجود تمایز و تقابل میان این قابلیت‌ها، نمایانگر همین دوسویگی است که در دو جنبه تحریکی و شناختیِ فاعلیت نفس، اثر می‌گذارد.

در نظر بوعلی، نزد خیال کثرت، شناخته‌شده‌تر از وحدت است (شیرازی، بی‌تا: ۹۳) و از طرفی اکثر انسان‌ها نیز به لحاظ طبیعت در حد مراتب پایینی خیال و در حقیقت به مثابه حیواناتی هوشمند هستند (حسن زاده آملی، ۱۳۸۵ : ۱/ ۲۰۶–۲۰۸)؛ از این‌رو خیال در مراحل اولیه، ظرف کثرت و تحقق امیال طبیعی و حیوانی است.

۱.۴ ترفندهای اعمال سلطه‌سایبری

بر اساس آنچه در بحث جایگاه خیال در علم النفس فلسفی و نقش آن در فاعلیت و ارتباط با قوای حیوانی و قلیان امیال نفسانی، در دو قوه شهویه و غضبیه و نیز ظرفیت خیال، وهم و متخیله در ایجاد خطای معرفتی و از این طریق، منحرف شدن مسیر انتخاب عقلانی بیان شد؛ سلطه‌سایبری در اشکالی نظیر تکثیر، تشتت و سرگرم‌سازی، تخدیر و معتادسازی، کنترل و شرطی‌سازی و معنویت نوین، در فاعلیت نفس انسانی تأثیر می‌گذارد.

توضیح مختصر هر یک از اشکال فوق درادامه بیان می‌گردد.

تکثیر، تشتت و سرگرم‌سازی در بستر خیال: نظام سلطه در مسیر اهداف خود، با ایجاد صور خیالی پرشمار و مبتنی بر امیال شهوانی و غضبیه و گاهی با ایجاد بستر خیالی در ارضای آن، (به‌طور مثال، فضای گیم یا متاورس) حرص و تمایلات دانی او را شدت داده و به کثرت تعلقات و غفلت انسان از خواسته‌های عالی و خودفرمانش منتهی می‌شود. در این حالت مبادی شوقیه تحت فرمان امیال تنوع‌طلب حیوانی بوده و مبدأ

علمی نیز مجال اندیشیدن ندارد.

متاورس و گیم‌های وابسته به خیال به عنوان نمونه ابزارهای سلطه‌سایبر، فرصت زیادی برای پیشرفت و بهره‌برداری استعماری فراهم آورده است. سلطه در بستر سایبر و با محوریت خیال آدمی، قدرت دارد با ایجاد یک زندگی در ابعاد مجازی، فرصت اشباع نیازهای خیالی برای انسان را صدچندان ساخته و با استفاده از علوم اعصاب و علوم شناختی بستری مبتنی بر احساسات کاذب ایجاد کند، تا حدی که فرد امیال دانی خود را با حواس پنج‌گانه می‌چشد، لمس می‌کند و می‌بوید و ....

همچنین قدرت دارد مرز میان واقعیت و مجاز را برداشته شده و معیار صدق و کذب در متعلقش را بر مطلوب خود تعریف کند.

تخدیر و معتادسازی: سلطه از طریق استمرار و تکرار تحریک مبادی شوقی حیوانی و تضعیف مبادی علمی، تخدیر و اعتیاد نفس را حاصل می‌کند.

کنترل و شرطی‌سازی: سلطه‌سایبر با ایجاد موقعیت‌های تشویق و تنبیه هدایت‌شده و نیز با ایجاد مغالطات ذهنی و احساسی، ذهن و احساس را در بستر خیال، شرطی ساخته و تحت‌تأثیر خطای شناختی، به عملکرد و فاعلیتی وهمانی و خیالی وامی‌دارد.

به عنوان نمونه با ایجاد بستر بازخوردهای مثبت و منفی هدایت‌شده، فرد را به انتخاب‌هایی وابسته به آن‌ها مبدل ساخته و معیار صحت و خطای واقعی را از او زایل می‌سازد.

معنویت نوین: جریان سلطه، در راستای اعمال و تقویت استیلای خود، میل فطری معنویت‌خواهی بشر را با ایجاد و معرفی ایسم‌ها، مکاتب و معنویت‌های نوظهور و خطای معرفتی – شناختی در بستر وهم و خیال پاسخ می‌دهد و از این طریق متعلقش را بر مدار خود کنترل می‌کند.

به‌فضا کلی، فضای سایبر مزایایی را برای سلطه‌جویان ایجاد کرده است؛ نظیر قدرت فریفتن بالا با جعل عمیق ازطریق ایجاد بستر اشتراک اذهانی و دستیابی به اعماق ذهن انسان، ذخیره داده‌های انسانی و بهره‌برداری از آن به نفع نظام سلطه، وجود بستر کنترل، تبدیل کردن فضای سایبر به فضای زندگی و طبیعتی جداناپذیر، میل محور بودن و کم‌هزینه بودن، همه و همه با محوریت خیال و تسخیر آن در فضای کنترل‌شده رقم می‌خورد. نظام سلطه با اشکال فوق و استفاده از ابزارهایی چون سحر می‌تواند در بستر سایبر، ذهن متعلق خود را نیز به معنای واقعی تسخیر کند.

۲.۴ کنترل سایبری و فاعلیت بالتسخیر

فاعل بالتسخیر، فاعلی است که خود و فعلش در تسخیر قوای برتر از اوست و مبتنی بر رابطه‌ای احاطی، تحت تسخیر فاعل دیگر کار می‌کند (طباطبایی، ۱۴۰۲: ۱۷۲).

فاعلیت انسان در اثر فرمان و کنترل در سلطه‌سایبرنتیک، تا حدودی به این معنا نزدیک می‌شود؛ البته در این سلطه، اراده به کلی از بین نمی‌رود بلکه تحت تحمیل نرم، دچار اختلال شده و یک‌طرفه می‌شود. متعلق سلطه، به قدری در امیال دانی غوطه‌ور می‌شود که مجالی برای انتخاب عقلانی نمی‌یابد و به مثابه حیوانی وابسته و وحشی در افسار نظام سلطه درمی‌آید و رام آن می‌شود.

تسخیر، به دو وجه حق و باطل صورت می‌گیرد. به عبارت دیگر نفوذ علّی بر غیر، یا در مسیر مصلحت تکوینی و لازمه تکوین اوست و یا دخالت و خللی منفعت‌طلبانه در مسیر تکوین اوست.

سلطه، از سنخ تسخیر باطل است و سلطه‌سایبری، از این جهت با سایر تسخیرهای باطل، مشترک است؛ با این تفاوت که حد نفوذ و تسخیر در آن، در محدوده خیال و دستگاه فکری ادراک است و اثری علّی و تکوینی ندارد؛ بر خلاف تسخیرهای باطل مثالی که در آن نوعی دخالت تکوینی و علّی رخ می‌دهد؛ از این‌رو ضعف محدوده تسخیر و علّی نبودن آن از ویژگی‌های تسخیر سایبری است.

سلطه‌سایبرنتیک با ذائقه‌سازی برای انسان، موجب می‌شود که او بر اساس انگیزه‌ها، علایق و با اختیار خویش به سوی معانی خیالی حرکت کند؛ از این‌رو این فاعلیتِ به ظاهر بالتسخیر، به فاعلیت بالقصد او، به معنای: فعلی که در آن فاعل دارای علم و اختیار است و در انجام فعل، علم و اختیارش دخالت دارد (طباطبایی، ۱۴۰۲: ۱۷۲)؛ ضربه‌ای نمی‌زند؛ بلکه با کثرت خیال و غلبه یافتن امیال، فاعلیت عقلانی‌اش مختل می‌شود؛ اما فعل همچنان ارادی، ولیکن ضعیف و نفسانی است؛ بنابراین کنش‌هایی که از متعلق سلطه‌سایبر رخ می‌دهد در حقیقت منسوب به اوست، هر چند در سیطره اهداف و فریب سایبر تحقق یافته باشد.

جهت‌گیری حرکت خیال در اثر نفوذ و تسخیر کنترل سایبری، بر اساس اتحاد عالم و معلوم به اتحاد نفس انسانی با صور معنایی مورد اقبال او می‌انجامد؛ بعد از اتحاد، آن معانی وارد جایگاه دوم یعنی عرصه ذهن و اندیشه انسان می‌شوند؛ از آنجا که نفس انسان در عین وحدت خود، دارای مراتب و مشتمل بر همه قوای ادراکی و تحریکی است بعد از اتحاد با صور مجرد علمی، رفتار خود را بر اساس آن سامان می‌دهد. در مرتبه سوم، معانی با خروج از زاویه ذهن افراد وارد متن زندگی و رفتارهای اجتماعی آنان شده و به تبع آن، باورها، عادات، نهادها و کنش‌های اجتماعی را تسخیر می‌کند. به تعبیری وهم، خیال و حس در مسیر اهداف نظام سلطه، بر این جامعه حکم‌فرمایی می‌کند.

۵ کارکرد خیال در سلوک و اعراض از سلطه‌پذیری

بر اساس آنچه بیان شد جنس خیال در سنخ خواطر و تداعی مؤثر است و به دلیل گذر عقل از مسیر وهم، هر اندازه خیال، لطیف‌تر بوده و از غلبه امیال حیوانی مصون باشد، لطافت ظهور می‌یابد؛ به علاوه، به دلیل قابلیت تربیت‌پذیری، ظرف انفعال از قوای ناطقه، فطرت و عقل الهی در مسیر هدایت‌پذیری می‌گردد؛ به نحوی که انسان با غلبه بر امیال دانی و سیطره عقلانیت بر نفس خود، نیل به کمالات، زیبایی‌شناسی و حق‌جویی را انعکاس می‌دهد و با تداعی خواطر و لذایذ عالم مثال منفصل و ارتقا ادراک نظری به کمالات حقیقی و تکاملی خود، شوق یافته و بستر سلوک و سلطه‌گریزی او فراهم می‌شود.

در این مسیر آنگاه که قوای بدنی و حیوانی تحت تدبیر عقل عملی فاعلیت داشته باشند و حاصل ادراک عقل عملی برگرفته از عقل نظری به عنوان هادی و رسول باطنی، بر خیال و متخیله عارض شده و ایجاد شوق کند، نفس انسان به جهت حاکمیت عقل در مبدأ فاعلی، از سلطه ابا خواهد داشت.

در این میان فطرت نیز که ساختار ویژه‌ی بشری است و در تصدیق مفاهیمی نظیر استحاله اجتماع و

ارتفاع نقیضین، قرین عقل نظری بوده و در نیل گرایشاتی نظیر زیبایی دوستی، کمال‌طلبی، حق‌جویی و میل به پرستش، قرین عقل عملی است و تبدیل ناپذیری و عدم انحراف از ویژگی‌های آن است؛ با ممانعت از غلبه امیال حیوانی شکوفا شده و با گرایشات سلوکی و خیال‌انگیز متعالی خیال را تحت‌تأثیر قرار می‌دهد (مطهری، ۱۳۷۰: ۱۹). از این‌رو حاکمیت بر خیال، شرط سلوک و تعالی بستر زیبایی‌شناختی آن است.

در مسیر افزایش قدرت انعکاس خیال از هدایت عقل و فطرت، آگاهی به وجود خطرات سلطه و نیز مجهز شدن به هشیاری‌ها و توانمندی‌های مقابله با سایبر و محدودیت بهره از آن و نیز بهره از هدایت‌های ولایت و شریعت لازم است؛ چرا که آگاهی خود مبدأیی علمی برای ایجاد شوق در مقابله با اشتیاقات کاذبی است که گاهی از طریق سلطه‌سایبر و مسیرهایی نظیر آن اعمال می‌شود.

۱.۵ خیال، زیبایی‌شناسی و هنر

هنر و حس زیبایی‌شناسی از امیال فطری و الهی آدمی و خیال بستری برای تجلی آثار هنری است.

خلاقیت تصویرگری و خلق صورت توسط قوه خیال و (یوسفی‌سوته، ۱۳۹۸: ۳۲۲) صورت‌های خیالی، منشأ آثار هنری هستند.

نسبت خیال و هنر دوسویه است؛ خیال هنر آفرین و هنر نیروبخش خیال است؛ بر این اساس ایجاد اثری هنری مبتنی‌بر نقش‌بندی خیالی آن است (برقعی، ۱۳۹۵: ۱۷۹).

ایده فیلسوفان اسلامی در باب هنر، بازنمایی و محاکات توسط خیال است؛ بر این مبنا با وجود کمال‌گونگی هنر، به میزانی که تصاویر متعالی در ظرف خیال ثبت شود، بازنمایی و خلاقیت هنر الهی جلوه کرده و به میزانی که از تصاویر منفی، مستهجن، وهمی و آلوده به شهوات و مادیت اشباع شود؛ هنر و خلاقیت متدانی و بلکه شیطانی بروز می‌یابد (هاشم‌نژاد، ۱۳۸۵ :۳۳۱) .

هنر پرمخاطب عصر حاضر، هنری تکنولوژیک است و با غلبه نگاه سکولار به جهان و نگرش اومانیستی به انسان، با محور قرار دادن سوبژکتیویته هنرمند، هدفی بیش از ارضای هواهای نفسانی نداشته و تعهدی به تجلی زیبایی حقیقی در آثار خویش ندارد. این هنر با جذابیت‌های بصری خود به سرعت در همه‌ی جوامع رخنه کرده و حرکت به سمت اضلال را موجب شده است و مخاطب خود را با سرپوشی بر فطرت و غرقه‌ساختنش در نفسانیات از درک زیبایی‌های معقول دور کرده است به نحوی که بر اساس آیه ۴۵ سوره زمر[۱۲] زیبایی حقیقی برای آن‌ها مشمئزکننده شده است.

بر خلاف آن، هنر اسلامی که طلایه‌دار هدایت و حیات است؛ با الهام از مبانی اسلامی، قادر به ایجاد فضایی است که انسان به باطن اشیا و مفاهیم متوجه شود و این امر همان نیاز انسان معاصر و روزنه‌ای به سمت سلوک، احیای عقل و فطرت نهفته و مسیر منع از سلطه است.

انتقال صور خیالی و از مسیر آن خلق هنر متعالی، به دلیل ظرافت بستر خیال و شوقی بودنش، تابع برهان و تجویز عقلی نیست؛ بلکه تابع معنویت است که با تسلط بر خیال حاصل شده و چنین تسلطی با مراقبت از اشتغال به مادیات و نیز ممانعت از توجه بیش از حد به مفاهیم انتزاعی و هجوم خیالات متشتت حاصل

[۱۲] وَإِذَا ذُكِرَ اللَّهُ وَحْدَهُ اشْمَأَزَّتْ قُلُوبُ الَّذِينَ لَا يُؤْمِنُونَ بِالْآخِرَةِ (زمر/ ۴۵)

می‌شود.

۲.۵ خیال و هدایت الهی

هدایت، راهبرد علم النفس فلسفی در سیر سلوک و تعالی خیال است؛ چرا که انسانیت انسان و تمایزش با حیوان، به واسطه سیطره عقل وعقلانیت به عنوان نبی و هادی درونی بر قوا، افعال و تصمیمات اوست.

هدایت به دو نوع تکوینی و تشریعی در عالم سریان دارد (جوادی آملی، ۱۴۰۰: ۱۶/ ۴۸-۶۰)، هدایت عقل و فطرت در راستای هدایت تکوینی و در احاطه وجودی خداوند و علل طولیه است و هدایت انبیا، اولیا الهی و نیز در امتداد آن، ولایت فقیه و ولایت مؤمنین بر یکدیگر، در قالب امر به معروف و نهی از منکر، از سنخ هدایت تشریعی و در مسیر رهایی از سلطه‌پذیری انسان است.

امر و فرمان در این نوع هدایت، متفاوت از کنترل و فرمان در سلطه‌سایبری است و همان‌گونه که در معناشناسی سلطه بیان شد، در سلطه، استخدام بر اساس اعتبارات نفسانی و توأم با جبر بوده و در بستر آلوده‌شدن خیال و عدم تبعیت نفس از ندای عقل و فطرت و نیز ولی حقانی رخ می‌دهد.

ولی در ولایت الهی هر گونه توصیه و نهی، مبتنی بر تشریع الهی، عقلانیت توحیدی و فطرت الهی است.

فرمان و اراده‌ای که در جریان هدایت و ولایت صورت می‌گیرد، در نوع تکوینی‌اش ضامن وجود و حیات انسان و در نوع تشریعی‌اش مستلزم هدایت و ارتقا سطح عقلانیت و آزادی از سلطه‌های غیرالهی است. علاوه بر این به میزان ولایت‌پذیری عقل، در بستر خیال، خیال نیز مطهر شده و شوق و اشتیاق سلوکی را توأم با توصیه عقلانی و فطری انعکاس می‌دهد.

۶ دستاوردهای بحث

- سلطه، قدرت مقید به تحمیل اراده و نوعی استخدام مبتنی بر اعتباریات نفسانی است که پس از عصر مدرنیته با نظریه سایبرنتیک، در کاربست سایبری، بر محور خیال انسانی اعمال شد.

- از آنجا که از منظر علم النفس فلسفی، تمامی فاعلیت‌های عقلی، خیالی و تمامی انگیزش‌های امیال نفسانی و الهی با استعانت از خیال صورت می‌گیرد، حاکم شدن سایبر بر خیال و آلوده کردن آن، نفوذ استعماری در تمام فعالیت‌های علمی و عملی انسان است. جریان سلطه‌سایبری با شناسایی این وادی گسترده به عنوان عنصر مشترک در تمام انسان‌ها، راهبرد نفوذ خاموش را پیش گرفته است.

- سلطه با دو روش مادی و فرامادی، بر انسان غالب می‌شود. سلطه‌سایبری یکی از انواع نرم و نافذ اعمال سلطه مادی است که از طریق ادوات مادی با محوریت کنترل و فرمان جریان آگاهی، برآمده از مبانی اومانیستی و بر مبنای اصالت قدرت و سرمایه، با ایجاد انحراف در صفحه بینش و گرایش نفس مثالی که بستری دوسویه و تربیت پذیر دارد، با اشکالی نظیر سرگرم‌سازی، اعتیاد، شرطی‌سازی، پاسخ به معنویت‌خواهی نفس، فاعلیت آن را با تحمیل اراده خود، تحت‌تأثیر قرار می‌دهد. سلطه معنوی نیز

با اعمال تسخیر به میزان احاطه وجودی سلطه‌گر و ضعف متعلق سلطه، به غرض نفسانی و غیرالهی، در جهت خلاف کمال او رخ می‌دهد.

- ولایت و هدایت تشریعی فرآیند استخدام بدون تحمیل اراده و با هدف ارتقای سطح عقلانیت و نیل به کمالات انسان رخ می‌دهد.
- انحراف و شدت‌یافتن تمایلات قوای حیوانی و آلودگی خیال به وهم و کثرت‌ها، مانع از انعکاس و بروز عقلانیت و امیال فطری بوده و نفس را به مثابه افساری در دست قدرت‌های غیرالهی قرار می‌دهد.
- طهارت نفس خیالی در موطن قلب و تبعیت آن از عقل به عنوان حجت درون و نیز ولایت تشریعی به عنوان حجت بیرون، ضامن رهایی و بروز امیال سلوکی، هنر متعالی و بستر ایجاد اشتیاقات متعالی است.
- از آنجا که فاعلیت انسان مبتنی بر بینش و گرایش‌ها است؛ از بایستگی‌های حکمرانان متعالی می‌توان اشاره کرد به:

- اولاً؛ ایجاد بستر مناسب جهت مطالعه دقیق برای استفاده از ظرفیت خیال‌انگیزی خیال در بستر زیبایی‌شناسی و جهت‌دادن هنر به بعد متعالی آن است.
- ثانیاً؛ با توجه به گستره‌ی خیال، اصلی‌ترین راه جلوگیری از آسیب‌های سایبر، ایجاد بینش نسبت به خطرات سلطه‌سایبری، با اعمال تبیین در بسترهای متنوع ادراکی و نیز مسدودسازی بسترهای تحریکی اعمال سلطه‌سایبری و مقابله با آن از طریق ایجاد شرایط لازم برای رشد فطرت و عقل در سایه‌ی اتصال با ولایت الهی و طهارت خیال است.

مراجع

[۱] قرآن کریم
[۲] نهج البلاغه
[۳] ابن‌سینا، حسین ابن عبدالله، مبدأ و معاد، تهران، مؤسسه مطالعات اسلامی، ۱۳۶۳ ش.
[۴] ابن عربی، محی‌الدین، الفتوحات المکیة، مصر، بولاق، ۱۲۹۲ ق.
[۵] ابن منظور، لسان العرب، تعلیق و تصحیح علی شیری، بیروت دار احیاء التراث العربی، ۱۴۰۸ ق.
[۶] احمدبن فارس، معجم مقاییس اللغة، تحقیق و تصحیح عبدالسلام محمد هارون، قم، مکتب الأعلام الإسلامی، ۱۴۰۴ق.
[۷] اردبیلی، عبدالغنی، تقریرات فلسفه امام خمینی. قم، مؤسسه تنظیم و نشر آثار امام، ۱۳۸۱ ش.
[۸] بابایی، سعیده و همکاران، نظریه سایبرنتیک و تحقق آن در فضای مجازی، تهران، مرکز ملی فضای مجازی، ۱۴۰۰ ش.
[۹] جوادی آملی، عبدالله، تفسیر موضوعی قرآن کریم (هدایت در قرآن)، قم، اسرا، ۱۴۰۰ ش.

[۱۰] جوادی آملی، عبدالله، رحیق مختوم، قم، اسراء، ۱۳۸۶ ش.
[۱۱] جوادی آملی، عبدالله، حق و تکلیف در اسلام، تحقیق مصطفی خلیلی، قم، اسراء، ۱۳۹۳ش.
[۱۲] جوادی آملی، عبدالله، هنر و زیبایی از منظر دین، مجله هنر دینی، ش۲۱ و ۲۲، ۱۳۸۵ ش، صص۴۳-۵۲.
[۱۳] چمن خواه عبد الرسول، صور خیال در نهج‌البلاغه و تجلی آن در ادب فارسی، شیراز، نوید، ۱۳۸۴ ش.
[۱۴] حسن‌زاده‌ی آملی، حسن، اتحاد عاقل به معقول، قم، بوستان کتاب، ۱۳۶۴ ش.
[۱۵] حسینی، سیدحسن، زیبایی‌شناسی و فلسفه رسانه، تهران، مهر نیوشا، ۱۳۸۸ ش.
[۱۶] حکاک، محمد، تحقیق در آراء معرفتی هیوم، تهران، مشکوه، ۱۳۸۰ ش.
[۱۷] خالقی بایگی، عزیز و همکاران، نفی سلطه‌گری و سلطه‌پذیری در آیات ۲۷۹ بقره، ۱۴۱ نساء و ۱۸۹ قصص، آموزه‌های قرآنی دانشگاه علوم اسلامی رضوی، دوره شانزدهم، شماره ۳۰، پاییز - زمستان ۱۳۹۸ ش، ۱۵۵-۱۸۰.
[۱۸] خلیل جر، فرهنگ لاروس، ترجمه سیدحمید طبیبیان، تهران، امیرکبیر، ۱۳۶۷ ش.
[۱۹] راسل، برتراند، قدرت، ترجمه نجف دریابندری، چاپ دوم، تهران، انتشارات خوارزمی، ۱۳۶۷ ش.
[۲۰] راش، مایکل، جامعه و سیاست؛ مقدمه‌ای بر جامعه‌شناسی سیاسی، ترجمه منوچهر صبوری، تهران، سمت، ۱۳۷۷ ش.
[۲۱] سبزواری، ملاهادی، شرح اسفار، بیروت، دار احیاء تراث، ۱۹۸۱ م.
[۲۲] سهروردی، یحیی، مجموعه مصنفات شیخ اشراق، تهران، مؤسسه مطالعات و تحقیقات فرهنگی، ۱۳۷۵ش.
[۲۳] شیرازی، صدرالدین محمد، الحاشیه علی الهیات الشفاء، قم، انتشارات بیدار، بی‌تا.
[۲۴] شیرازی، صدرالدین محمد، الحکمة المتعالیة فی الأسفار العقلیة الأربعة، قم، منشورات طلیعة النور، ۱۳۹۳ ش.
[۲۵] شیرازی، صدرالدین محمد، الحکمة المتعالیة فی الأسفار العقلیة الأربعة، بیروت، داراحیاء التراث العربیه، ۱۹۸۱م.
[۲۶] شیرازی، صدرالدین محمد، الشواهد الربوبیه في مناهج السلوکیه، مشهد، مرکز جامع نشر، ۱۳۶۰ ش.
[۲۷] شیرازی، صدرالدین محمد، المبدأ و المعاد، تهران، انجمن حکمت و فلسفه، ۱۳۵۴ ش.
[۲۸] شیرازی، صدرالدین محمد، مفاتیح الغیب، تهران، مؤسسه تحقیقات فرهنگی، ۱۳۶۳ ش.
[۲۹] شیرازی، صدرالدین محمد، مبدأ و معاد، ترجمه جعفر شانظری، قم، انتشارات دانشگاه قم، ۱۳۹۰ ش.
[۳۰] صمدی آملی، داود، شرح مراتب طهارت، قم، روح و ریحان، ۱۳۹۰ش.
[۳۱] صولتی، مهران، جامعه‌شناسی سلطه، تهران، انتشارات جامعه‌شناسان، ۱۳۹۰ ش.
[۳۲] طباطبایی، محمد حسین، اصول فلسفه و روش رئالیسم، تهران، صدرا، ۱۳۶۴ ش.
[۳۳] طباطبایی، محمد حسین، نهایة الحکمة، قم، مؤسسة النشر الإسلامي، ۱۴۰۲ ق.
[۳۴] طریحی، احمد، مجمع البحرین، تهران، نشر فرهنگ اسلامی، بی‌تا.
[۳۵] طوسی، نصیرالدین، شرح الاشارات و التنبیهات، قم، نشرالبلاغه، ۱۳۷۵ ش.
[۳۶] علی بابایی، غلامرضا، فرهنگ علوم سیاسی، تهران، شرکت نشر و پخش ویس، ۱۳۶۹ ش.
[۳۷] قریشی، علی اکبر، بی‌تا، قاموس قرآن، تهران، دارالکتب الاسلامیه.
[۳۸] قیصری، محمد داوود، شرح فصوص الحکم، به کوشش سید جلال‌الدین آشتیانی، تهران، انتشارات علمی و فرهنگی، ۱۳۷۵ ش.

[۳۹] کامران دستجردی، حسن، محمدی، زهرا، فضای سایبری و تعاریف جدید در جغرافیای سیاسی، فصلنامه علمی – پژوهشی و بین المللی جغرافیای ایران، سال دوازدهم، شماره ۴۳، زمستان ۱۳۹۳ ش.

[۴۰] مدقق، محمد داود، شرف‌الدین، سید حسین، تبیین سلطه و رهایی در حکمت اسلامی با تأکید بر اندیشه آیت الله جوادی، حکمت اسرا، شماره ۳۴، ۱۳۹۸ ش، ۳۵-۶۷.

[۴۱] مجلسی، محمدباقر، بحارالانوار، تهران، دارالکتب الاسلامیه، بی تا.

[۴۲] مصباح یزدی، محمد تقی، تهاجم فرهنگی، قم، مؤسسه آموزشی و پژوهشی امام خمینی، ۱۳۷۶ ش.

[۴۳] مصباح یزدی، محمد تقی، شرح جلد هشتم اسفار اربعه، تحقیق و نگارش محمد سعیدی‌مهر، قم، مؤسسه آموزشی و پژوهشی امام خمینی، ۱۳۹۳ ش.

[۴۴] مصباح یزدی، محمد تقی، نظریه حقوقی اسلام، قم، مؤسسه آموزشی و پژوهشی امام خمینی، ۱۳۸۲ ش.

[۴۵] مصطفوی، حسن، التحقیق فی کلمات القرآن الکریم، تهران، بنگاه، ۱۳۶۰ ش.

[۴۶] مطهری، مرتضی، نقدی بر مارکسیسم، تهران، صدرا، ۱۳۶۳ ش.

[۴۷] مطهری، مرتضی، مجموعه آثار، تهران، صدرا، ۱۳۹۱ش.

[۴۸] مطهری، مرتضی، فطرت، تهران، صدرا، ۱۳۷۰ ش.

[۴۹] نراقی، ملااحمد، معراج السعاده، قم، نوید ظهور، ۱۳۹۰ش.

[۵۰] نقی‌زاده، محمد، نیاز انسان امروز به هنر دینی، مجله هنر دینی، ش۱۵ و ۱۶، ۱۳۸۲ ش، صص ۵۷-۷۴.

[۵۱] مکلوهان، مارشال، برای درك رسانه، ترجمه سعید آذری، تهران، مرکز تحقیقات صدا و سیما، ۱۳۷۷ ش.

[۵۲] وفاییان، محمد حسین، فرامرز قراملکی، احد، تبیین جایگاه و کارکرد قوه خیال، در صدور رفتار و افعال عاقلانه از انسان با تأکید بر مبانی نفس–شناسی صدر المتألهین، اخلاق وحیانی، شماره اول، پیاپی ۱۱، ۱۳۹۵، صص ۱۱۶-۱۳۴.

[۵۳] وینر، نوربرت، استفاده‌ی انسانی از انسان: سیبرنتیک و جامعه، ترجمه مهرداد ارجمند، تهران، سازمان انتشارات و آموزش انقلاب اسلامی، ۱۳۶۶ ش.

[۵۴] هاشم‌نژاد، حسین، درآمدی بر فلسفه هنر، قبسات، سال یازدهم، ۱۳۸۵، صص۳۱۳ -۳۳۲.

[۵۵] هیندس، باری، گفتارهای قدرت از هابز تا فوکو، ترجمه مصطفی یونسی، تهران، پردیس دانش، ۱۳۸۰ ش.

[۵۶] یوسفی سوته، رقیه، بررسی تحلیلی نقش قوه خیال در تعالی انسان بر مبنای حکمت متعالیه، قم، دانشگاه باقرالعلوم، ۱۳۹۸ش.

مدل فرآیندی تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی

محمدرضا مرادی[۱]، محمدرضا ولوی[۲]، متین مرادی[۳]

[۱] دکتری مدیریت راهبردی فضای سایبر، دانشگاه عالی دفاع ملی، تهران
mr.moradi@sndu.ac.ir
[۲] دانشیار دانشگاه صنعتی مالک اشتر، تهران
valavi@mut.ac.ir
[۳] دانشجوی مهندسی نرم‌افزار کامپیوتر، دانشگاه شاهد ، تهران
matinmoradi1401@gmail.com

چکیده

دکترین در حقیقت، فلسفه را که اغلب ابهام‌آلود و نظری است، می‌گیرد و آن را عملیاتی می‌کند تا از دل آن، سیاست‌هایی خاص بیرون بیاید. در خصوص مفهوم دکترین در دنیا، تفاوت دیدگاه وجود دارد. رویکرد ج.ا.ا. به دکترین نیز، با دو رویکرد غالب شرقی و غربی تا حدودی متفاوت است. دکترین عمدتاً در امور دفاعی-امنیتی به‌کار می‌رود. کشورهای دنیا، برای تدوین دکترین از مدل‌های مشخصی بهره می‌برند که عموماً نیز این مدل‌ها به‌صورت واضح تشریح نمی‌گردند. فضای سایبر، پدیده نوظهوری است که دارای ویژگی‌های خاص خود می‌باشد. این فضا چند سالی است که رسماً به‌عنوان یکی از عرصه‌های جنگ تعریف گردیده است. بنابراین چنانچه در نظر داشته باشیم برای این فضا در حوزه دفاعی-امنیتی دکترین تدوین نماییم، نیازمند یک مدل خاص‌منظوره می‌باشیم. مدل فرآیندی معرفی شده، مختص فضای سایبر جمهوری اسلامی ایران است و برگرفته از یک کارپژوهشی گسترده (با بهره‌گیری از نظر خبرگان و تعیین اعتبارسنجی آن) است که نتیجه آن ارائه شده است. هدف این پژوهش که برگرفته از یک رساله دکتری می‌باشد آن است که مدل فرآیندی تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی-امنیتی احصا شود.

کلمات کلیدی: دکترین، فضای سایبر، دفاعی امنیتی، تدوین مدل.

۱ مقدمه

در اداره امور یک کشور مهم‌ترین مسأله، حاکمیت است و حاکمیت نیازمند یکپارچگی است. پس از تدابیر منسجم متولیان حکومتی، سایرین در هر سازمان و دستگاهی می‌توانند به‌صورت هماهنگ و هم‌افزا اقدام نمایند. دکترین گفتمان مشترک ایجاد می‌نماید و این گفتمان مشترک می‌تواند به اقدامات هم‌سویی منجر شود

که ثمرات آن در اثر هم‌افزایی به‌صورت تصاعدی افزایش می‌یابد. سازمان‌های دفاعی-امنیتی در جمهوری اسلامی ایران پس از ورود عرصه سایبری به حوزه دفاع و امنیت، تلاش‌های فروانی در راستای مدیریت راهبردی این فضا به انجام رساندند. لیکن نقصان‌ها و چالش‌هایی در مدیریت کلان این فضا مشاهده می‌شود. تدوین دکترین در این حوزه امکان ایجاد وحدت رویه را فراهم می‌نماید؛ از آن جایی که تدوین دکترین، نیازمند یک الگو می باشد در این مقاله سعی داریم الگوی فرآیندی تدوین دکترین سایبری جمهوری اسلامی ایران را در حوزه دفاعی امنیتی ارائه نماییم. بدین منظور ابتدا به تبیین مفهوم دکترین می‌پردازیم سپس نگاهی گذرا به برخی مدل های تدوین دکترین سایبری در داخل و خارج از کشور می اندازیم در ادامه دکترین سایبری دفاعی امنیتی را تشریح می نماییم و در انتها به معرفی مدل می پردازیم. این مقاله بر اساس تعاریف مفاهیم زیر[۱] به‌وسیله محققین بنا شده است.

۲ دکترین

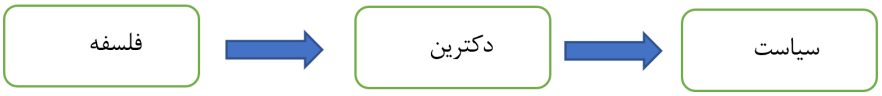
۱.۲ مفهوم دکترین

دکترین در معنای عام به معنای اعتقادات یا اندیشه‌هایی است که در یک مکتب فکری جایگاه برجسته‌ای دارد (دکترین مهدویت در شیعه). معنای خاص آن به معنای اصول و قواعدی است که در یک علم خاص همچون سیاست و اقتصاد جنبه کاربردی داشته باشد و باید در مقام عمل به‌کار بسته شود (دکترین چماق و هویج در سیاست [۲]). از میان معانی یادشده آنچه مدنظر محققان به‌عنوان تعریف عملیاتی است معنای دوّم دکترین است.

شناخت دکترین، از آنجایی شروع می‌شود که هر فلسفه و نظام شناختی، الزاماً برای پیاده شدن در متن اجتماع و بیان چگونگی حیات انسانی، نیاز به‌واسطه‌ای دارد. بر این اساس، دکترین موضوعیت پیدا می‌کند که غبار ابهام را از چهره آن می‌زداید تا بتواند به سیاست‌های مشخصی جهت اداره انسان تبدیل شود. از این حیث، دکترین حاکم، ضرورتاً یک ایدئولوژی و مجموعه‌ای سازمان‌یافته درباره بهترین شیوه زندگی مردم و درباره مناسب‌ترین ترتیبات نهادی برای جوامعشان می‌باشد؛ بنابراین، دکترین (قاعدة القواعد) تبیین و تشریح قواعد ذاتی حاکم بر خلقت، طبیعت و قواعد ذاتی حاکم بر اعمال موجودات، به‌ویژه بشر است. تبیین این قواعد مبتنی بر، «باید» برای جامعه‌سازی الزامی است.لذا موضوع این رویکرد، مطالعه جامعه از حیث قواعد ذاتی حاکم بر خلقت، طبیعت و رفتار موجودات و انسان است [۳].

دکترین، عبارت است از یک نیروی واسطه‌ای میان فلسفه و سیاست [۳] فلسفه همواره در ابتدا می‌آید و دکترین از آن ناشی می‌شود. سیاست نیز به‌نوبه خود از دکترین نشئت می‌گیرد [۳] در حقیقت دکترین، فلسفه را که اغلب ابهام‌آلود و نظری است، می‌گیرد و آن را عملیاتی می‌کند تا از دل آن، سیاست‌هایی خاص

[۱] الف-فضای مجازی: فضای مجازی، امتزاجی از فضای حقیقی می‌باشد که به ابزاری جهت بسط و تحکیم حاکمیت ملی در مناسبات جهانی و کشوری مبدل شده است. ب-دکترین: اصول و قواعدی است که در یک علم خاص و به‌منظور هدایت‌گری و کاربست عملی به کار می‌رود. ج-دکترین سایبری دفاعی امنیتی جمهوری اسلامی ایران: به‌عنوان راهنمای نظری و عملی راهبردی نیروهای دفاعی امنیتی (در شرایط امنیتی صلح، بحران و جنگ)، فلسفه حاکمیتی واحد برای عملیات نرم و سخت و حکمرانی روابط بین‌المللی سایبری؛ مورداستفاده قرار می‌گیرد [۱۰].



شکل ۱: تبیین الگوی سیاست‌گذاری بر مبنای رهیافت دکترینی [۳]

بیرون بیاید [۳]. به تعبیر دیگر، دکترین تعیین‌کننده سیاست است و یک سیاست عمومی، عبارت است از اجرای زیرمجموعه‌ای از یک دکترین حاکم [۳] و تمامی سیاست‌های عمومی، ریشه در یک دکترین مشخص دارند آن‌ها برای تبیین الگوی سیاست‌گذاری بر مبنای رهیافت دکترینی نمودار زیر را ارائه می‌نمایند و با تأکید بر کاربردی بودن این الگو می‌گویند: نکته مفید در خصوص این‌گونه تصویرسازی ما این است که آن‌ها را می‌توان در مورد همه انواع سیاست‌ها به کار برد.

تعریف دکترین از منظر برخی سازمان‌های حقوقی به شرح زیر می باشد:

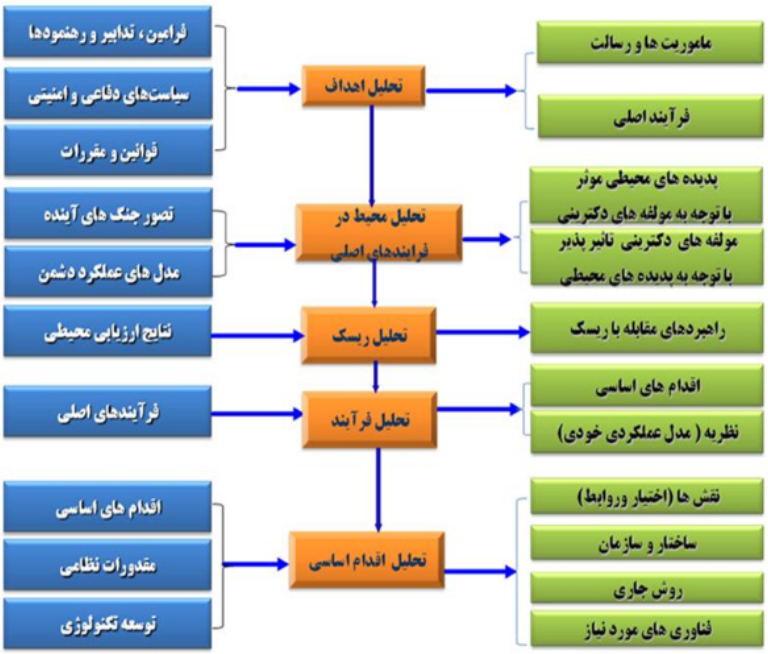
ستاد کل نیروهای مسلح: مجموعه‌ای از قواعد نسبتاً پایدار و کاربردی که چگونگی انجام مأموریت و اجرای عملیات را ترسیم می‌کند و مبنا و راهنمای برنامه‌ریزی‌های اقدامات است. رهنامه (دکترین) ایده‌ای است کلی معطوف به راه و روش برای رسیدن به اهداف. معمولاً دکترین متأثر از چهار مقوله است: ۱. نوع سازمان و مأموریت آن. ۲. محیط (به‌ویژه تهدیدات) ۳. قدرت نظامی و دفاعی ۴. علم و فناوری [۴].

فرهنگ اصطلاحات نظامی وزارت دفاع آمریکا: اصول بنیادینی که نیروهای نظامی و وابستگان آن‌ها توسط آن، فعالیت‌های خود را در راستای تأمین اهداف ملی هدایت می‌کنند(۲۰۲۰).

فرهنگ اصطلاحات دفاعی ناتو: اصول بنیادینی که نیروها و فعالیت‌هایشان را جهت نیل به اهداف هدایت می‌کند. این اصول دستوری بوده لیکن اجرای آن‌ها قضاوتی (منوط به رأی) می‌باشند (۲۰۱۹).

۲.۲ ماهیت‌شناسی دکترین

دکترین شیوه‌ای است که می‌گوید چگونه باید برای پیروزی بجنگیم و شامل سه عنصر اساسی نظریه، فرهنگ و اقتدارمی‌شود. اول از همه، دکترین باید برمبنای تلقیات از کار انجام‌شده و چیزی که باعث پیروزی در آن محیط می‌شود، قرار گیرد. به‌عبارت دیگر یک دکترین به یک عنصر نظریه نیاز دارد.باید بدانیم که چرا چیزی صادق است تا اثر آن را بگذارد. به‌علاوه این دکترین است که دلیل آن را توضیح می‌دهد. ثانیاً یک دکترین باید عوامل فرهنگی را موردتوجه قرار دهد.سرانجام، دکترین به‌نوعی اقتدار رسمی نیاز دارد چون در غیر این صورت اثر یکپارچه‌سازی و «هماهنگ‌کننده فکر» را نخواهد داشت. متعادل کردن سه عنصر فوق، یعنی نظریه، فرهنگ و اقتدار، می‌تواند به طرق مختلف انجام شود و با این کار می‌توان سه نوع دکترین ایده‌آل را تولید کرد: دکترین به‌عنوان ابزاری برای فرماندهی، تغییر و آموزش [۱۱].



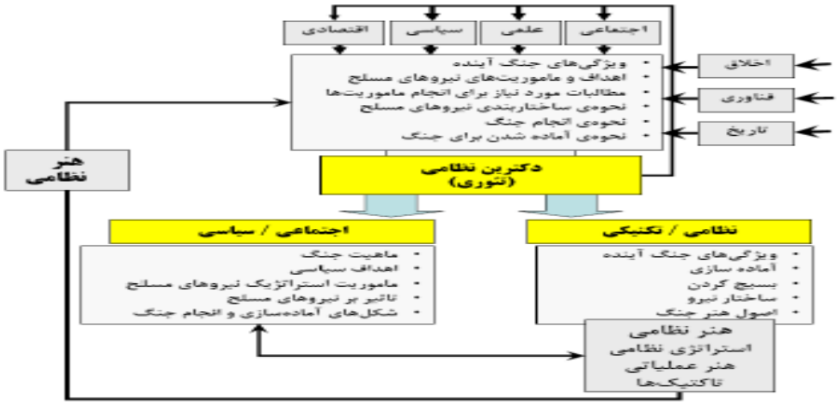
شکل ۲: فرآیند پنج مرحله‌ای تدوین دکترین [۵]

۳ برخی از مدل‌های تدوین دکترین

طبق بررسی‌های به‌عمل آمده تاکنون جهت تدوین دکترین سایبری در ج.ا.ا. روشی تدوین شده‌ای وجود ندارد، لیکن به‌صورت کلی جهت تدوین دکترین چندین الگو پیشنهاد شده است که در زیر به‌صورت مختصر مرور می‌گردد.

مدل سیستمی: این مدل توسط هیأت عالی آئین‌نامه‌های ن.م. ارائه شده است. در این مدل، خلق یا تجدید نظر در یک دکترین جدید در طی پنج مرحله به شرح ذیل انجام می‌پذیرد. از ویژگی‌های منحصر به فرد این مدل آن است که باعث می‌گردد تا فعالیت‌های انجام‌شده در تیم‌های تدوین‌کننده دکترین از چارچوب واحدی پیروی کرده و ضمن ایجاد یکنواختی، امکان ارزیابی را برای اطمینان از توجه همه‌جانبه به اجزای دکترین فراهم‌نماید [۵].

مدل دکترین نظامی: دکتر دانش آشتیانی در مقاله «اصول و روش تدوین دکترین نظامی»، یک روش پنج مرحله‌ای برای تدوین دکترین نظامی معرفی نموده‌اند. مرحله اول: شناسایی مناقشه (جنگ) و ماهیت آن؛ مرحله دوم: بررسی نقطه نظرات دشمن (نیات دشمن)؛ مرحله سوم: توسعه راهبرد ملی؛ مرحله چهارم: توسعه راهبرد نظامی (ملّی)؛ مرحله پنجم: توسعه و تدوین دکترین نظامی (ملّی) [۶].



شکل ۳: مدل تدوین دکترین در روسیه [۷]

مدل تدوین دکترین در روسیه: عبدالرسول دیو سالار در مقاله خود به تشریح روش تدوین دکترین در روسیه می پردازد و بیان می کند که مفهوم دکترین در ادبیات شرق و غرب از تفاوت قابل توجهی برخوردار است. در ادبیات شرقی دکترین نقش محوری در انتقال دیدگاه ها و باورهای رسمی نسبت به جنگ آینده ومحیط امنیتی پیش رو دارد. در حالی که در غرب دکترین شعور ناپیدای حاکم بر بکارگیری نیروهای مسلح در صحنه نبرد تعبیر می شود که بر پایه مفاهیم عملیاتی شکل گرفته و ارتباط میان فناوری، ساختار، تئوری و تجربه رزمی را برقرار می‌سازد در شرق دکترین برداشت مشترکی از مطالبات دفاعی ملی است [۷].

مدل دکترین جنگ سایبری: لچ جی. جانشکی و آندره ام. کلاریک در مقاله ای با عنوان «ایجاد دکترین جنگ سایبری» مدلی را جهت تدوین دکترین جنگ سایبری پیشنهاد می دهند.به طور خلاصه، چارچوب پیشنهادی برای توسعه دکترین جنگ سایبری ملی مبتنی بر چندین اصل اساسی است. اولین مورد این است که چنین فرآیندی در حیطه اختیارات دولت انجام می‌شود، هم در مورد شروع روند دکترین جنگ سایبری و هم در مورد پذیرش نهایی آن. توسعه دکترین جنگ سایبری باید به متخصصان غیرنظامی دولت، کارکنان حوزه دفاعی-امنیتی و سازمان‌های حرفه‌ای مرتبط با فناوری اطلاعات واگذار شود. پیشنهادهای نهایی به شورای امنیت در سطح ملی (یا نهاد دیگری با مسئولیت‌های مشابه) ارائه شود و در نهایت توسط رئیس دولت پذیرفته می‌شود. در نهایت دکترین جنگ سایبری در معرض عموم قرار می‌گیرد [۱۲].

۴ مفهوم‌شناسی دکترین سایبری در حوزه دفاعی امنیتی

موضوع تدوین دکترین سایبری یک موضوع فرا سازمانی و ملی است که تدوین آن مستلزم شناخت مؤلفه‌های مرتبط با آن در سیاست‌های ابلاغی، قانون اساسی و اسناد بالادستی این حوزه است. سایبرنتیک واژه پرکاربرد حوزه کنترل و ارتباطات در نیمه دوّم قرن بیستم میلادی است. این واژه از لغت یونانی Κυβερνήτης به

معنای سکان‌دار والی اخذ شده است[۲]. سکان‌دار در ناوبری کشتی کسی است که با رصد سرعت و جهت وزش باد و تأثیر آن بر امواج دریا و با در نظر گرفتن سمت و جهت مقصد، سکان کشتی را به چپ و راست می‌چرخاند.سایبرنتیک حضور حسگرها، اطلاعات، تصمیم‌سازی و تصمیم‌گیری و اعمال قدرت در ناوبری است و عدم وجود هر یك ناوبری را دچار مشکل خواهد کرد [۸]. برخی از تعاریف فضای سایبر عبارتند از:

شورای عالی فضای مجازی: فضای مجازی جمهوری اسلامی ایران فضایی در امتداد فضای واقعی، سالم، ایمن، مفید، پیشران پیشرفت سایر حوزه‌ها است (۱۳۹۷).

پیمان آتلانتیک شمالی (ناتو): فضای مجازی مجموعه‌ای وابسته به زمان از سیستم‌های اطلاعاتی به‌هم‌پیوسته و کاربران انسانی است که با این سیستم‌ها در تعامل هستند (۲۰۱۷).

تعریف مشترك روسیه و آمریکا: یک رسانه الکترونیکی که از طریق آن اطلاعات تولید، منتقل، دریافت، ذخیره، پردازش یا حذف می‌شوند (۲۰۱۴).

نیروهای مسلّح عملیات فضای مجازی و جنگ الکترونیکی را در محیط اطلاعاتی انجام می‌دهند. محیط اطلاعاتی مجموعه‌ای از افراد، سازمان‌ها و سیستم‌هایی تشکیل‌شده است که اطلاعات را جمع‌آوری، پردازش، انتشار یا طبق آن عمل می‌کنند. سهولت دسترسی به شبکه‌های فنی باعث کمک به اشتراک‌گذاری اطلاعات می‌شود و جنبه‌های اجتماعی محیط اطلاعاتی را تقویت می‌کند.ابعاد محیط اطلاعاتی عبارت‌اند از فیزیکی، اطلاعاتی و شناختی. عملیات اطلاعاتی، چه در داخل و چه در خارج از فضای مجازی، می‌تواند بر روی عملیات دوستانه، خنثی و تهدیدی در فضای مجازی تأثیر بگذارد [۱۳].

قدرت بازدارندگی: هر کشوری که بخواهد تحت سلطه نباشد، برای حفظ استقلال و هویت باید توان مقابله با حملات دشمنان را داشته باشد و بتواند به بهترین شکل از خود دفاع کند. جمهوری اسلامی ایران از ابتدای تشکیل با انواع گوناگونی از توطئه‌های مستکبرین روبه‌رو بوده و تهدید به حمله نظامی یکی از گزینه‌های روی میز دشمنان است. با توجه به این چالش، تدارک نیروهای مسلّح مقتدری که از حداکثر توانایی برخوردار بوده و توان مقاومت در برابر انواع دشمنی‌ها را داشته باشند، ضروری است.این همان چیزی است که در ادبیات سیاسی از آن به‌عنوان قدرت بازدارندگی تعبیر می‌شود و یکی از مهم‌ترین اهداف قرآنی نظام اسلامی است [۱].

ده استنباط از دیدگاه‌های مقام معظم رهبری (مد ظله العالی): ۱- عدم انکار فضای مجازی در انقلاب اسلامی. ۲- فضای مجازی پایه‌گذار تمدن اسلامی. ۳- واقعیت فضای مجازی در مقابل رویکرد دوجهانی. ۴- رویکرد مبتکرانه و فرصت‌آفرین و هوشمند در مواجهه با فضای مجازی. ۵- فضای مجازی ابزار بسط حاکمیت ملی در مناسبات جهانی و کشوری. ۶- چالش دوقطبی‌سازی سیاسی کاذب در توسعه کشور. ۷- چالش تسلط کمپانی‌های بزرگ تحت سلطه آمریکا. ۸- چالش شکاف توسعه در مقایسه با روند

[۲] لفظ Governor به‌معنای فرماندار با سایبرنتیک هم‌ریشه است.

پیشرفت و شتاب فناوری. ۹- توان و ظرفیت زیرساختی بالقوه (مردم - نخبگان - فناوری - ساختار- اقتصاد). ۱۰- ضرورت تدوین نقشه راه حکمرانی در فضای مجازی [۹].

قانون اساسی: برخی از اصول مهم قانون اساسی عبارتند از: اصل(۹) اصول تفکیک‌ناپذیر: آزادی، استقلال، وحدت، تمامیت اراضی کشور

اصل(۲۶) اصول ج. ا. ایران: استقلال، آزادی، وحدت ملی، موازین اسلامی

اصل(۱۷۶) اصول شورای عالی امنیت ملی: تأمین منافع ملی، پاسداری از انقلاب اسلامی، تمامیت ارضی، حاکمیت ملی

اصل(۱۵۲) سیاست خارجی ج.ا.ا: نفی هرگونه سلطهجویی و سلطهپذیری؛ حفظ استقلال همه‌جانبه و تمامیت ارضی کشور؛ دفاع از حقوق همه مسلمانان؛ عدم تعهد در برابر قدرتهای سلطهگر؛

برخی از مهم ترین اسناد بالادستی در مورد دکترین سایبری جمهوری ا. ایران در حوزه دفاعی و امنیتی به شرح زیر می‌باشند. علاوه بر اسناد یادشده فوق، سایر اسناد سیاستی که دارای ماهیت دفاعی امنیتی و فناوری اطلاعات می‌باشند، به‌طور کامل مدنظر قرار می‌گیرند.

- سند چشم‌انداز ۱۴۰۴ ساله (۱۳۸۲): ایران کشوری است: امن، مستقل و مقتدر با سامان دفاعی مبتنی بر بازدارندگی همه‌جانبه و پیوستگی مردم و حکومت؛ آزادی‌های مشروع، حفظ کرامت وحقوق انسان‌ها و بهره‌مند از امنیت اجتماعی و قضایی؛ الهام‌بخش، فعال و مؤثر در جهان اسلام؛ دارای تعامل سازنده و مؤثر با جهان بر اساس اصول عزت، حکمت و مصلحت.
- حکم مقام معظم رهبری (مد ظله‌العالی) دوره دوّم شورای عالی فضای مجازی (۱۳۹۴): ۳-ارتقای جمهوری اسلامی ایران به قدرت سایبری در طراز قدرت‌های تأثیرگذار جهانی و برخورداری از ابتکار عمل و قدرت تعامل با دیگر کشورها در جهت شکل‌دهی به قواعد و قوانین مرتبط با فضای مجازی در عرصه جهانی با رویکرد اخلاق‌مدار و عادلانه. ۱۰- تدوین و تصویب نظام‌های امنیتی، حقوقی، قضایی و انتظامی موردنیاز در فضای مجازی.
- گام دوّم انقلاب۱۳۹۷: توصیه‌هایی اساسی به‌منظور جهاد بزرگ برای ساختن ایران ا. بزرگ (ایجاد تمدّن عظیم اسلامی هدف نهایی جمهوری اسلامی ایران، امید و نگاه خوش‌بینانه به آینده، برپا کردن تمدّن اسلامی منتها با روح اسلامی و معنویّت)

۵ نتیجه‌گیری

پس از بررسی مدل‌های مختلف تدوین دکترین در دنیا، نظریه‌های دفاعی امنیتی جمهوری اسلامی ایران و ویژگی‌های فضای سایبر، محققین به یک مدل فرآیندی جهت تدوین دکترین سایبری ج.ا.ا به شرح زیر دست یافتند. در ادامه با برگزاری جلسه گروه کانونی، متشکل از تعدادی از خبرگان در این حوزه مدل به نقد و بررسی گذاشته شد و اشکالات مدل احصاء و تصحیح گردید. سپس مدل تصحیح شده در قالب پرسش‌نامه

شکل ۴: مدل فرآیندی تدوین دکترین سایبری ج.ا.ا

نیمه ساختاریافته به خبرگان ارائه و مجدداً نظرات جمع‌آوری گردید. در راستای اعتبارسنجی مدل، نسبت به تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی اقدام گردید. با اعتبارسنجی دکترین به‌دست آمده ، روایی مدل تدوین‌شده نیز احصاء گردید [۱۰].

مراجع

[۱] امام خامنه‌ای (مدظله‌العالی)، مجموعه بیانات، قابل‌دسترسی در: www.farsi.khamenei.ir

[۲] خسروپناه، عبدالحسین و یزدانی‌فر، صالحه (زمستان ۱۳۹۵)، نظام مدیریتی فقه و فرآیند سیاست‌گذاری و طرح‌ریزی، فصلنامه راهبرد فرهنگ، دوره نهم، شماره ۳۶، صفحات: ۴۱-۷.

[۳] بوریک، کریستوفرپی، شافریتز، جی.ام (۱۳۹۰)، سیاست‌گذاری عمومی در ایالات‌متحده آمریکا، ترجمه حمیدرضا ملک محمدی. تهران: دانشگاه امام صادق.

[۴] ستاد کل نیروهای مسلّح ج.ا.ایران (۱۳۸۹)، اصطلاحات و واژگان.

[۵] ثروتی، محسن و همکاران (۱۳۹۱)، راهنمای آموزشی تدوین دکترین، تهران، انتشارات دبیرخانه هیئت عالی آئین‌نامه‌های نیروهای مسلح.

[۶] دانش آشتیانی، محمدباقر (۱۳۸۸)، اصول و روش تدوین دکترین نظامی. فصلنامه نظم و امنیت انتظامی، شماره سوم سال دوم.

[۷] مؤسسه آموزشی و تحقیقات صنایع دفاعی (۱۳۸۶)، ارزیابی ابعاد گوناگون دکترین‌های امنیتی- دفاعی روسیه، تهران.

[۸] کیانخواه، احسان (۱۳۹۷)، تبیین ماهیت و مؤلفه‌های فضای سایبر بر اساس تفکر اسلامی، رساله دکتری، تهران: دانشگاه و پژوهشگاه عالی دفاع ملی.

[۹] ولوی، محمدرضا (۱۳۹۲)، طرح تحقیق دفاع سایبری آینده.

[۱۰] مرادی، محمدرضا (۱۴۰۱)، تدوین دکترین سایبری جمهوری اسلامی ایران در حوزه دفاعی امنیتی، رساله دکتری، تهران: دانشگاه و پژوهشگاه عالی دفاع ملی.

[11] Harold Hoiback (2015), The Anatomy of Doctrine and Ways to Keep It Fit , Journal of Strategic Studies.

[12] M. Colarik, Andrew, Janczewski, Lech (2012), Establishing Cyber Warfare Doctrine, Journal of Strategic Security, Volume 5, Number 1 Volume 5, No. 1: Spring 2012.

[13] Department of the Army (2017), FM 3-12, cyberspace and electronic warfare operation. Available at: http://www.apd.army.mil

واکاوی آسیب‌های فضای سایبر و شبکه‌های اجتماعی بر جامعه ایرانی (با تأکید بر بلاگرها)

محبوبه موسیوند[۱]، فائزه ساکی[۲]

[۱] استادیار گروه مطالعات علوم اجتماعی و توسعه، پژوهشکده زنان، دانشگاه الزهرا، تهران، ایران
m.moosivand@alzahra.ac.ir
[۲] کارشناسی ارشد مطالعات زنان، دانشگاه الزهرا، تهران، ایران
sakifaezeh7@gmail.com

چکیده

فضای سایبر و شبکه‌های اجتماعی علیرغم مزایای قابل توجه و بی‌شمار، آسیب‌ها و مشکلاتی را هم برای کاربران به‌دنبال داشته است که نیازمند بحث و بررسی است، به‌همین منظور این پژوهش با هدف واکاوی آسیب‌های فضای سایبر و شبکه‌های اجتماعی بر جامعه ایرانی (با تأکید بر بلاگرها) با استفاده از روش توصیفی-تحلیلی انجام شده است که نتیجه این پژوهش بدین شرح است که ترویج سبک زندگی متعارض با سبک زندگی ایرانی-اسلامی و ترویج تفکر کسب درآمد و شهرت از فضای سایبر و شبکه‌های اجتماعی به هر طریقی، دو آسیب عمده در این حوزه به‌شمار می‌رود. در مجموع به‌منظور کاهش آسیب‌های فردی و اجتماعی فضای سایبر و شبکه‌های اجتماعی به‌ویژه در حوزه بلاگرها پیشنهاد می‌شود که علاوه بر ارتقا دانش رسانه افراد، سیاست‌گذاری‌ها و اقدامات مناسبی جهت مقابله با بعضی آسیب‌های فضای مجازی انجام شود.

کلمات کلیدی: فضای سایبر، فضای مجازی، شبکه‌های اجتماعی، آسیب، بلاگر.

۱ مقدمه

«شبکه‌های وابسته به همدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های کامپیوتری، پردازنده‌های تعبیه شده، کنترل کننده‌های صنایع مهم، محیط سایبری اطلاعات و تاثیر متقابل بین شخص و این فضا با هدف تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات، فضای سایبری نامیده می‌شود که امکان دارد در رابطه مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی از جمله اینترنت باشد و یا اینکه تنها قابلیت اتصال به محیط اطراف در آن تعبیه شده باشد» [۶، سند راهبردی پدافند سایبری کشور، ۱۳۹۴: ۱]. این بستر مجازی دارای ویژگی‌هایی همچون فشردگی مکان، فردگرایی، تکثر و تنوع عددی، پیوستگی و یکپارچگی، پویایی زمان و گمنامی هویت است [۹] و حضور در آن تقریباً

اجتناب ناپذیر شده است. در همین راستا، بر اساس آمار ارائه شده در سایت Statista «تا آوریل سال ۲۰۲۳، ۵٫۱۸ میلیارد کاربر اینترنت در جهان وجود داشته است که از این تعداد، ۴٫۸ میلیارد نفر کاربر شبکه‌های اجتماعی بوده‌اند؛ افزون بر این، چهار شبکه اجتماعی جهانی محبوب در سال ۲۰۲۳ بر اساس تعداد کاربران به ترتیب عبارت است از: «فیسبوک، یوتیوب، واتساپ و اینستاگرام» [۱۵] که گستردگی ضریب نفوذ این ابزار در جهان و وجود مطالعات متعدد در خصوص آسیب‌های آن از مهم‌ترین دلایل پرداختن به این موضوع (فضای مجازی) در این پژوهش می باشد. لازم به ذکر است که فضای سایبر دارای مزیت‌ها و معایب متعددی است، اما هدف از انجام این پژوهش واکاوی آسیب‌های فضای سایبر و شبکه‌های اجتماعی بر جامعه ایرانی (با تاکید بر بلاگرها) با استفاده از روش توصیفی - تحلیلی می باشد و پرداختن به مزایای این فناوری جزء اهداف این تحقیق نمی‌باشد؛ به عبارت دیگر هدف از انجام این تحقیق آن است که تأثیرات منفی و چالش‌هایی که بعضاً به‌واسطه برخی از چهره‌های فعال فضای سایبر و شبکه‌های اجتماعی تحت عنوان بلاگر در جامعه ایجاد می‌شود مورد بررسی قرار گیرد؛ در نهایت ضمن ارائه‌ی مطالعاتی که در حوزه‌ی آسیب‌های فضای سایبر در ایران انجام شده است، به بررسی تأثیرات چهره‌های مجازی (بلاگر) بر جامعه ایرانی خواهیم پرداخت.

۲ مروری بر کارهای دیگران

در خصوص مشکل‌های ناشی از فضای سایبر پژوهش‌های متعددی انجام شده است که در ادامه به برخی از آن‌ها می‌پردازیم؛ اما مسئله‌ی تاثیر بلاگرها بر جامعه ایرانی جزء چالش‌های نوینی است که نیازمند بحث و بررسی است که در این پژوهش بدان پرداخته خواهد شد. حمایت‌خواه [۲]، در پژوهشی تحت عنوان «تأثیر شبکه‌های اجتماعی مجازی بر انحراف‌های زنان» که با روش توصیفی از نوع پیمایش اجتماعی انجام داده است به این نتیجه دست یافته است که بین تحصیلات، پایگاه اجتماعی - اقتصادی، دینداری، هدف از عضویت، میزان استفاده و نیز سابقه‌ی استفاده از شبکه‌های اجتماعی و اینترنت با متغیر انحراف اجتماعی ارتباط معناداری وجود دارد؛ به‌طور کلی شبکه‌های اجتماعی مجازی، انگیزه و فرصت بیشتری را نسبت به بستر حقیقی جامعه برای تخطی زنان از هنجارهای اجتماعی فراهم کرده است، از این رو، چنین می‌توان استنباط کرد که شبکه‌های اجتماعی مجازی نقشی تأثیرگذار و مستقیم در خصوص بروز انحراف‌های اجتماعی زنان ایفا می‌کند. شیخ انصاری [۸]، در پژوهشی تحت عنوان «جامعه ایرانی و فضای مجازی تحلیل ثانویه تحقیقات علوم اجتماعی در حوزه فضای مجازی» که با روش تحلیل ثانویه انجام داده است و نمونه مورد مطالعه نیز ۷۳۲ مقاله منتشرشده حوزه علوم اجتماعی در بازه زمانی سال ۱۳۸۱ تا ۱۴۰۰ بوده است به این نتیجه دست یافته است که فناوری‌های وب۲، هویت دینی، هویت ملی و ارزش‌های خانوادگی کاربران ایرانی را تضعیف می‌کند؛ روابط اجتماعی، سرمایه اجتماعی و مشارکت سیاسی آنان را افزایش می‌دهد و مسائل اجتماعی نوظهور مانند جرائم اینترنتی، اعتیاد اینترنتی، سوگواری مجازی، زیارت مجازی و ... در فضای سایبر پدید آمده است. احمدی و عسگرزاده [۱]، در پژوهشی تحت عنوان «نشانه‌شناسی سبک زندگی تجمل‌گرایانه در صفحات اینستاگرامی اینفلوئنسرهای ایرانی» که با روش نشانه‌شناسی و با تأکید بر نظریه بازنمایی انجام داده‌اند و در آن ویدیوهای منتشر شده در صفحات اینستاگرامی ۴ نفر از اینفلوئنسرهای ایرانی

که به‌طور متوسط بین ۶۳۰ هزار تا ۴ میلیون دنبال‌کننده دارند را در بازه زمانی ۵ ماهه در سال ۱۳۹۷ مورد بررسی قرار داده‌اند، به این نتیجه دست یافتند که بازنمایی سبک زندگی تجمل‌گرایانه در اینستاگرام عبارت است از: مسکن و محل زندگی، اوقات فراغت و تفریح، وسایل شخصی برند (مانند لباس، گوشی، ساعت و ...)، خودرو، مدیریت بدن و روابط شخصی که جذابیت، خودشیفتگی، قدرت، احساس رضایت، سرسختی و آرامش، احساساتی است که زندگی تجمل‌گرایانه را در نظام معنایی مخاطب خوشایند و مثبت می‌نمایاند. خان محمدی و غازی اصفهانی [۳]، در پژوهشی تحت عنوان «آسیب‌های اجتماعی نوظهور زنان در فضای مجازی با تأکید بر اینستاگرام» از طریق رصد کاربران زن اینستاگرام و کنش‌گری آنها به دنبال بررسی آسیب‌های اجتماعی اینستاگرام بر زنان ایرانی بوده‌اند که نتایج این تحقیق بدین صورت است: مهم‌ترین چالش‌های فضای مجازی (اینستاگرام) برای زنان ایرانی عبارت است از: تعرض جنسی، سایبرسکس، مدگرایی، اعتیاد مجازی، روابط آزاد با نامحرم و خیانت سایبری، مشکلات روحی و روانی، میل به ابراز وجود، بی‌توجهی به انجام دستورات دینی از جمله عفاف و حجاب، افشای حریم خصوصی، عادی‌سازی بی‌اخلاقی، تغییرات فرهنگی، جلوه‌گری خود ایده‌آل، فردگرایی و تضعیف نقش مادری و همسری. عبدالرحمانی و همکاران [۱۲]، در پژوهشی تحت عنوان «بررسی تاثیر محتوای غیراخلاقی شبکه‌های اجتماعی مجازی بر امنیت اجتماعی (مطالعه موردی: شبکه اینستاگرام)» به این نتیجه دست یافتند که میان محتوای غیر اخلاقی و امنیت اجتماعی ارتباط معناداری وجود دارد. قاسم‌زاده برکی و همکاران [۱۳]، در پژوهشی تحت عنوان «بررسی انگیزه‌های سوء استفاده از کودکان، توسط مادران بلاگر و سلامت روانی فرزندان آنان در فضای مجازی» به این نتیجه دست یافتند که «مشکلات خانوادگی فرد، مشکلات فرهنگی- اجتماعی فرد، مشکلات اقتصادی فرد، مشکلات روانی فرد، تلاش برای کسب موفقیت‌های اقتصادی، تلاش برای کسب اعتبار اجتماعی، سرگرم شدن و لذّت بردن فرزند از فضای مجازی و تلاش برای طرح فرزند فضای مجازی»؛ انگیزه‌های مادران بلاگر در سوء استفاده از کودکان خود در فضای مجازی است. خطیب زاده و همکاران [۴]، در پژوهشی تحت عنوان «بررسی وضعیت زنان ایرانی در فضای مجازی: مطالعه صفحات اینستاگرامی (با رویکرد امنیت اجتماعی)» که با روش کیفی و از طریق مطالعه‌ی ۱۵۰ صفحه برتر اینستاگرامی کشور انجام داده‌اند به چندین مضمون اصلی و فرعی دست یافته‌اند که عبارتند از: مخالفت با حجاب (شامل تمسخر حجاب و دختران با حجاب، نمایان ساختن حجاب به عنوان موضوعی مورد منازعه میان مردم، تبلیغات علیه گشت ارشاد پلیس)؛ سیاه‌نمایی وضعیت زنان ایرانی (شامل تبلیغ در خصوص وجود شرایط ناعادلانه و سخت برای زنان ایران، تبلیغ برای حضور زنان ایرانی در ورزشگاه‌ها به عنوان یک خلأ اساسی، انعکاس ویژه برخورد با شبکه‌های مدلینگ در ایران)؛ بازنمایی زنان در رسانه (شامل استفاده ابزاری از زنان برای تبلیغات، حضور زنان در ورزشگاه‌ها، نخبگی بانوان (عدم مغایرت)، استفاده از خانم‌های بازیگر برای تبلیغات لوازم آرایشی و بهداشتی)؛ روابط آزاد (شامل تبلیغ پارتی‌های شبانه‌روزی (مغایرت)، تبلیغ خیانت در زندگی زناشویی (مغایرت)، ترویج چندضلعی‌های جنسی، ارتباط با حیوانات (مغایرت)، ترویج روابط آزاد دختر و پسر (مغایرت))؛ تن‌نمایی (شامل تبلیغ لاغری و مانکن بودن زنان، ترویج بی‌عفتی و بی‌حیایی، توجه حداکثری به زیبایی‌های ظاهری زنان)؛ ضدیت با دین (شامل به سخره گرفتن احکام اسلام، تبلیغ ضد زن بودن دین، تبلیغ سگ بازی). رحیمی و همکاران [۵]، در پژوهشی تحت عنوان «بررسی رابطه شبکه‌های اجتماعی مجازی و گرایش به ناهنجاری‌های اخلاقی» که

با روش پیمایش انجام داده‌اند به این نتیجه دست یافته‌اند که «گرایش به ناهنجاری‌های اخلاقی بر اساس مؤلفه‌هایی مانند جنسیت، وضعیت تأهل، پایگاه اجتماعی و اقتصادی و میزان تحصیلات متفاوت است؛ گرایش به ناهنجاری‌های اخلاقی در میان جوانان شهر تهران متوسط رو به بالا است و جوانانی که عضو شبکه‌های اجتماعی مجازی هستند و استفاده صحیحی از آن ندارند بیشتر در معرض گرایش به ناهنجاری‌های اخلاقی قرار دارند». سهراب زاده و همکاران [۷]، در پژوهشی تحت عنوان «شبکه‌های اجتماعی مجازی و شکل‌گیری تصویر ذهنی زنان از بدنشان» که با روش پیمایش انجام داده‌اند به این نتیجه دست یافته‌اند که ارتباط مستقیم و معناداری میان میزان استفاده از شبکه‌های اجتماعی مجازی با تصویر ذهنی از بدن در زنان مورد مطالعه در سطح اطمینان ۹۵ درصد وجود دارد. طالعی و همکاران [۱۰]، در پژوهشی تحت عنوان «آسیب شناسی ارتباط با جنس متفاوت در شبکه‌های اجتماعی مجازی: یک مطالعه پدیدارشناسی با نوجوانان» که با رویکرد کیفی از نوع پدیدارشناسی توصیفی، ابزار مصاحبه نیمه ساختاریافته و روش کولایزی انجام داده‌اند در نهایت به ۳ مضمون اصلی شامل تجربه ارتباط با جنس مخالف، فساد جنسی، پیامدهای آسیب‌زا و ۱۱ مقوله فرعی شامل انگیزه ارتباط، الگوگیری ارتباط با جنس مخالف، رقابت برای تصاحب کردن، تنوع روابط، ارتباط جنسی، تقویت ارتباط، ترویج فساد جنسی، آسیب‌های جنسی، اجتماعی و فردی و ۷۳ خرده مقوله دست یافته‌اند. طالعی و همکاران [۱۰]، در پژوهشی تحت عنوان «خشونت و پرخاشگری در شبکه‌های اجتماعی مجازی از دیدگاه نوجوانان: یک مطالعه پدیدارشناسی» که با روش کیفی از نوع پدیدارشناسی و ابزار مصاحبه نیمه ساختاریافته و روش کولایزی انجام داده‌اند به دو مضمون اصلی شامل قلدرنمایی و حاضرجوابی و هفت مضمون فرعی شامل الگوسازی، انگیزه، انتقال جدال کلامی، نمایش خود جعلی، دعوای گروهی مجازی، دعوای مجازی و تشدید دعوا و ۱۰۲ مفهوم اولیه دست یافته‌اند. قربانی و همکاران [۱۴]، در پژوهشی تحت عنوان «شناسایی و تبیین آسیب‌های فرهنگی فضای مجازی» که با روش کیفی انجام داده‌اند آسیب‌های فرهنگی را درقالب چهار محور اصلی سبک زندگی، هویت ملی، ارزش‌های فرهنگی و هنجارهای فرهنگی و ۱۵ مضمون فرعی تبیین کرده‌اند که عبارتند از: تأثیر فضای مجازی بر سبک زندگی منطبق بر فرهنگ ایرانی اسلامی (شامل تبدیل ناهنجاری‌ها به هنجار و بالعکس، متأثر شدن هنجارهای سنتی، افزایش توقع‌های بین زوجین و افراد خانواده)؛ تزلزل مرجعیت ارزش‌های فرهنگی (شامل ایجاد جریان‌های فرهنگی علیه نظام، نسبیت گرایی فرهنگی، برجسته سازی انحراف‌های فرهنگ دینی، تضعیف باورهای دینی با انتشار شبهه‌ها، کاهش علاقه به شعائر مذهبی، درآمیختن حق و باطل (مغالطات)، تلاش برای کمرنگ سازی هنجارهای فرهنگی)؛ تزلزل مرجعیت هنجارهای فرهنگی (شامل تلاش برای کمرنگ سازی هنجارهای فرهنگی، تقویت روحیه فمنیستی، تمسخر و هجمه علیه حجاب)؛ تزلزل مرجعیت هویت ملی (شامل تغییر ذائقه به نفع فرهنگ بیگانه، زیر سؤال بردن متولیان فرهنگ، ایجاد هجمه علیه مراکز فرهنگی، سیاه نمایی علیه اوضاع فرهنگی کشور).

۳ تاثیر بلاگرها بر جامعه

در این بخش به مهم‌ترین تأثیرها و آسیب‌هایی که فضای سایبر و شبکه‌های اجتماعی در حوزه‌ی بلاگرها بر جامعه داشته است خواهیم پرداخت، لازم به ذکر است که در فضای مجازی بلاگران و اینفلوئنسرهای بسیاری

در حیطه‌های مختلف (مانند رستوران، مسافرت، محصولات آرایشی، سبک زندگی و ...) فعالیت می‌کنند که اقدامات غیرمتعارف برخی از آنان به یک مسئله‌ی پژوهشی تبدیل شده است که در این تحقیق بدان پرداخته می شود.

۱. **ترویج سبک زندگی متعارض با سبک زندگی ایرانی - اسلامی:** سبک زندگی دارای شاخصه‌ها و ابعاد گوناگونی است که می‌تواند به طرق متفاوت از اینترنت، فضای سایبر و شبکه‌های اجتماعی تأثیر پذیرد مانند: الف) سبک پوشش: سبک پوشش یکی از ابعاد سبک زندگی تلقی می‌شود؛ چهره‌های شناخته شده فضای مجازی، به‌ویژه بلاگرهایی که دنبال‌کنندگان بسیاری دارند و بعضاً در ایران سکونت ندارند می‌توانند با پوشش خاصی که در عکس‌ها و ویدیوهای خود دارند بر سبک پوشش زنان و دختران تأثیراتی داشته باشند و استفاده از برخی پوشاک را که متفاوت با ارزش‌ها و هنجارهای ایرانی و اسلامی است در جامعه گسترش دهند که در نهایت موجب می‌شود زنان و دختران از این مد پیروی کنند. ب) مدیریت بدن: گاهی بلاگرها به‌ویژه آن گروهی که به تبلیغ سبک زندگی خود در فضای مجازی می پردازند، به‌طور مستقیم و غیر مستقیم به تبلیغ جراحی‌های زیبایی می‌پردازند. ج) ترویج سبک زندگی تجمل‌گرایانه: سبک زندگی تجمل‌گرایانه به‌عنوان یکی از انواع سبک‌های زندگی، در اموری همچون پوشاک، خودرو، ساعت، تلفن همراه، نگهداری از حیوانات خانگی، مسکن و ... در زندگی برخی از این افراد نمود پیدا می کند. د) ترویج مبانی ارزشی نامطلوب: در برخی از تعاریف سبک زندگی، مبانی فکری و ارزشی به عنوان یکی از ابعاد سبک زندگی محسوب شده است که می‌تواند به‌نوعی تحت تأثیر فضای سایبر قرار گیرد. فضای سایبر فرصتی را در اختیار افراد قرار داده است که بتوانند توانمندی‌ها، هنرها، مهارت‌ها، دانش و ... خود را به‌نحوی گسترده در معرض دید افراد قرار دهند بدین صورت که می‌توانند محتوای تولید شده خود یا محصولی که به فروش می‌رسانند را به‌طور همزمان از طریق شبکه‌های اجتماعی متعدد مانند اینستاگرام، یوتیوب و تلگرام با تعداد قابل توجهی از افراد به اشتراک گذارند و از این طریق درصورت داشتن شرایطی همچون بازدید بالا درآمد کسب کنند، حال از میان افرادی که در فضای سایبر به کسب درآمد و دیده شدن می‌پردازند گروهی هستند که دارای تحصیلات و دانش مرتبط با موضوعی که تبلیغ می‌کنند نیستند؛ مثلاً شخصی بلاگر است و مهارت سخن‌وری هم دارد و درباره‌ی موضوعات مختلف به‌ویژه موضوعات روان‌شناختی مانند زندگی موفق، زوج درمانگری، مدیریت رابطه و مشاوره خانواده راهکار ارائه می‌کند و از سوی دیگر هم مبلغ استفاده از یک سری لوازم آرایشی است، که این موضوع می‌تواند به نوعی آسیب‌زا تلقی شود زیرا برخی از این افراد در خارج از کشور سکونت دارند و راهکارهای روان‌شناختی که ارائه می‌دهند مناسب برای جامعه‌ای همچون ایران با چنین ویژگی‌های فرهنگی و دینی نیست. برای مثال نامناسب تلقی نکردن ازدواج سفید و فرزند حاصل از آن یکی از این موارد است و بینندگان این ویدیوها در صورت نداشتن سواد رسانه امکان دارد که تحت تأثیر قرار گیرند.

۲. **ترویج تفکر کسب درآمد و شهرت از فضای سایبر و شبکه‌های اجتماعی به هر طریقی:** کاربران فضای سایبر به منظور کسب شهرت و درآمد روش‌های مختلفی را به کار می‌گیرند که بعضی

از این روش‌ها آسیب‌زا است مانند اشاعه‌ی این تفکر آسیب‌زا بین زنان، دختران و نوجوانان که انسان می‌تواند از هر روشی حتی بدون داشتن تحصیلات و مهارت خاصی از فضای مجازی کسب شهرت و یا حتی درآمد کند مانند: به اشتراک گذاشتن موضوعات شخصی با دنبال‌کنندگان خود از قبیل طلاق و فرزندآوری و کسب شهرت؛ تهیه دابسمش با یک آهنگ وایرال‌شده؛ تولید محتوای نامناسب در فضای مجازی تنها برای دیده شدن از طریق بازدید و کامنت بالا (حتی اگر توهین‌آمیز باشد)؛ استفاده از فرزندان توسط برخی بلاگرها: فضای مجازی و شبکه‌های اجتماعی فرصتی را در اختیار افراد قرار داده است که بتوانند توانایی‌ها و مهارت‌های خود را به شیوه‌ای آسان و کم‌هزینه در فضای سایبر عرضه نمایند که در همین راستا برخی از نوجوانان با میل و رغبت خود اقدام به تولید محتوا در فضای سایبر می‌نمایند، اما برخی افراد هستند که از کودکان خود که آگاهی چندانی نسبت به ابعاد گوناگون موضوع‌ها ندارند استفاده می‌کنند و این موضوع به‌منزله نوعی آسیب تلقی می‌شود زیرا تمایل و آگاهی فرد در شهرت او اهمیت خاصی دارد و امکان دارد که کودک بعداً تمایلی به دیده شدن نداشته باشد و خانواده بدون توجه به این مسئله او را وارد دنیای شهرت کرده باشند؛ علاوه بر این، چنین کودکی به‌نوعی کودک کار که وظیفه‌اش حضور در تصاویر و ویدیوهای تبلیغاتی خانواده‌اش است به نحوی که منجر به بازدید، کامنت و یا لایک به تعداد قابل توجه و در نهایت شهرت و درآمد شود، تبدیل می‌شود.

۴ نتیجه‌گیری

چنانچه پیش‌تر بدان اشاره شد هدف این پژوهش واکاوی آسیب‌های فضای سایبر و شبکه‌های اجتماعی بر جامعه ایرانی (با تاکید بر بلاگرها) بوده است و قطعاً فضای سایبر برای بشر مزیت‌هایی به همراه داشته است اما پرداختن به آنها جزء اهداف این پژوهش نبوده است. با بررسی‌های انجام شده دو مقوله‌ی اساسی تحت عنوان ترویج سبک زندگی متعارض با سبک زندگی ایرانی - اسلامی و ترویج تفکر کسب درآمد و شهرت از فضای سایبر و شبکه‌های اجتماعی به هر طریقی، جزء تاثیرات منفی بلاگرها بر جامعه احصا شده است؛ در همین راستا در پژوهش احمدی و عسگرزاده [۱۶]، تحت عنوان «نشانه شناسی سبک زندگی تجمل‌گرایانه در صفحه‌های اینستاگرامی اینفلوئنسرهای ایرانی» سبک زندگی تجمل گرایانه اینفلوئنسرهای ایرانی بازنمایی شده است و در پژوهش قاسم‌زاده برکی و همکاران [۱۳]، نیز تحت عنوان «بررسی انگیزه‌های سوء استفاده از کودکان، توسط مادران بلاگر و سلامت روانی فرزندان آنان در فضای مجازی» انگیزه‌های مادران بلاگر در سوء استفاده از کودکان خود در فضای مجازی مورد توجه بوده است. در مجموع به‌منظور کاهش آسیب‌های فردی و اجتماعی فضای سایبر و شبکه‌های اجتماعی به ویژه در حوزه بلاگرها پیشنهاد می شود که علاوه بر ارتقا دانش رسانه در میان اقشار گوناگون جامعه، انجام پژوهش‌های متعدد با دیدگاه‌های متفاوت، حضور فرهیختگان عرصه‌های مختلف در عرصه تولید محتوای مجازی، سیاست‌گذاری‌ها و اقدام‌های مناسبی جهت مقابله با بعضی آسیب‌های فضای مجازی همچون استفاده ابزاری مادران بلاگر از کودکانشان انجام شود.

مراجع

[۱] احمدی، علی، عسگرزاده، محسن (۱۳۹۹). «نشانه شناسی سبک زندگی تجمل گرایانه در صفحات اینستاگرامی اینفلوئنسرهای ایرانی». فصلنامه انجمن ایرانی مطالعات فرهنگی و ارتباطات. دوره ۱۶، شماره ۶۰، صص. ۲۹۶-۲۷۳.

[۲] حمایت خواه، مجتبی (۱۴۰۰). «تأثیر شبکه‌های اجتماعی مجازی بر انحراف‌های اجتماعی زنان». نشریه علمی انتظام اجتماعی. سال ۱۳، شماره ۱، صص. ۱-۲۶.

[۳] خان محمدی، کریم، غازی اصفهانی، مریم (۱۳۹۹). «آسیب‌های اجتماعی نوظهور زنان در فضای مجازی با تأکید بر اینستاگرام». دوفصلنامه مطالعه‌های اسلامی آسیب‌های اجتماعی، دانشگاه شاهد. دوره ۲، شماره ۱، صص. ۱۲۸-۱۴۴.

[۴] خطیب زاده، سمیرا، بنی هاشمی، سید محسن، سبحانی، عبدالرضا، علیشیری، بهرام (۱۳۹۸). «بررسی وضعیت زنان ایرانی در فضای مجازی: مطالعه صفحه‌های اینستاگرامی(با رویکرد امنیت اجتماعی)». فصلنامه علمی پژوهشی مطالعه‌های امنیت اجتماعی، شماره ۶۰، صص. ۱۳-۵۱.

[۵] رحیمی، محمد، فتحی، لیلا، افراسیابی، فاطمه، اسکندری اندبیلی، رعنا (۱۳۹۸). «بررسی رابطه شبکه‌های اجتماعی مجازی و گرایش به ناهنجاری‌های اخلاقی». نشریه علمی انتظام اجتماعی، سال یازدهم، شماره دوم، صص. ۱۳۵-۱۶۰.

[۶] سند راهبردی پدافند سایبری کشور مصوب سال ۱۳۹۴ برگرفته از سایت وزارت نیرو، شرکت مدیریت منابع آب ایران.

[۷] سهراب زاده، مهران، نیازی، محسن، نژادی، اعظم، افرا، هادی (۱۳۹۸). «شبکه‌های اجتماعی مجازی و شکل گیری تصویر ذهنی زنان از بدنشان». فصلنامه علمی - پژوهشی زن و جامعه، سال دهم، شماره دوم، صص. ۲۱۷-۲۴۰.

[۸] شیخ انصاری، مهین (۱۴۰۰). «جامعه ایرانی و فضای مجازی تحلیل ثانویه تحقیقات علوم اجتماعی در حوزه فضای مجازی». مجله جامعه شناسی ایران، دوره ۲۲، شماره ۴، صص. ۳۲ -۳.

[۹] صادقی، فاطمه، حیدری، مظاهر (۱۳۹۹). «آسیب شناسی نقش شبکه‌های اجتماعی مجازی در تربیت نوجوانان». دوفصلنامه تخصصی مطالعات تربیتی و روانشناختی خانواده، سال ۲، شماره ۲، صص. ۹۵-۱۱۹.

[۱۰] طالعی، علی، اسمعیلی، معصومه، فلسفی نژاد، محمدرضا، کاظمیان، سمیه، برجعلی، احمد (۱۳۹۸). «آسیب شناسی ارتباط با جنس متفاوت در شبکه‌های اجتماعی مجازی: یک مطالعه پدیدارشناسی با نوجوانان». تحقیقات علوم رفتاری، دوره ۱۷، شماره ۱، صص. ۸۷-۹۷.

[۱۱] طالعی، علی، اسمعیلی، معصومه، فلسفی نژاد، محمدرضا، کاظمیان، سمیه، برجعلی، احمد (۱۳۹۸). «خشونت و پرخاشگری در شبکه‌های اجتماعی مجازی از دیدگاه نوجوانان: یک مطالعه پدیدارشناسی». دوفصلنامه مشاوره کاربردی، دانشگاه شهید چمران اهواز، سال ۹، شماره ۱، صص. ۲۹-۴۸.

[۱۲] عبدالرحمانی، رضا، زرگر، علیرضا، سحری، امید (۱۳۹۹). «بررسی تاثیر محتوای غیراخلاقی شبکه‌های اجتماعی مجازی بر امنیت اجتماعی (مطالعه موردی: شبکه اینستاگرام)». فصلنامه علمی پژوهشی مطالعات امنیت اجتماعی، شماره ۶۳، صص. ۷۳-۹۶.

[۱۳] قاسم زاده برکی، سارا، منطقی، مرتضی، محمدی، مریم (۱۳۹۹). «بررسی انگیزه‌های سوء استفاده از کودکان، توسط مادران بلاگر و سلامت روانی فرزندان آنان در فضای مجازی». فصلنامهٔ پژوهش در سلامت روانشناختی، دوره ۱۴، شماره ۲، صص. ۳۴-۴۹.

[۱۴] قربانی، محمد مهدی، علیرمضانی، احمد، دارابی، معصومه (۱۳۹۸). «شناسایی و تبیین آسیب‌های فرهنگی فضای مجازی». دوفصلنامه مطالعات اسلامی آسیب‌های اجتماعی، دانشگاه شاهد، دوره ۱، شماره ۲، صص. ۸۳ - ۱۱۰.

[15] https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[16] https://www.statista.com/statistics/617136/digital-population-worldwide/

از گواهی تا باور مبتنی بر تکنولوژی: بررسی بر اساس تجربه‌گراییِ انتقادیِ زمینه‌ای

محمدعلی عاشوری کیسمی [۱]

[۱] فلسفه، دانشگاه علامه طباطبائی، تهران، ایران
m_ashori@atu.ac.ir

چکیده

هدف این پژوهش بررسی معرفت‌شناختی خروجی‌های هوش مصنوعی در برابر پرسش‌های علمی است. با توجه به اینکه در هوش مصنوعی، از اطلاعات و داده‌های متخصصان و دانشمندان برای یادگیری استفاده می‌شود؛ ممکن است این تصور پدید آید که می‌توان خروجی‌های به‌دست‌آمده در برابر پرسش‌های علمی را نوعی گواهی گروهی در نظر گرفت. این پژوهش با استفاده از روش تحلیلی-انتقادی دیدگاه‌های موجود را مورد ارزیابی قرار می‌دهد که در این راستا از رویکرد تجربه‌گراییِ انتقادیِ زمینه‌ایِ هلن لانجینو استفاده شده است. نتایج پژوهش حاضر نشان می‌دهد رویکردهای سنتی و ابزاری امکان بررسی خروجی هوش مصنوعی تحت عنوان گواهی را ندارند. رویکرد شبه-گواهی بر معرفت‌شناسی اجتماعی جریان اصلی متکی است که بررسی‌ها نشان می‌دهد استدلال‌ها و انتقادات این رویکرد بر پایه شناخت روند تولید دانش علمی استوار نیست. دیگر نتایج پژوهش نشان می‌دهند که کماکان خروجی هوش مصنوعی در برابر پرسش‌های علمی را نمی‌توان گواهی گروهی متخصصان دانست و اصطلاح «باور مبتنی بر تکنولوژی» بهتر آن را تبیین می‌کند.

کلمات کلیدی: گواهی گروهی، هوش مصنوعی، معرفت‌شناسی اجتماعی، هلن لانجینو، تجربه‌گراییِ زمینه‌ای انتقادی.

۱ مقدمه

ما از منابع معرفتی مختلفی همچون ادراک، حافظه، گواهی و غیره برای کسب دانش استفاده می‌کنیم [۱]. در میان این منابع، گواهی نقش بسیار پررنگی دارد. بخش بزرگی از دانش ما در مورد جهان، مانند علم و تاریخ از طریق گواهی دیگران به دست می‌آید. به عبارتی گواهی منبع جدایی‌ناپذیر از دانش ما است [۲]. با توسعه سریع هوش مصنوعی در سالیان اخیر و گسترش تکنیک‌های پردازش زبان طبیعی [۱]، بسیاری از افراد، پرسش‌های خود را از ابزارهای هوش مصنوعی می‌پرسند. بسیاری از این پرسش‌ها، پرسش‌های علمی است.

[1] Natural Language Processing

به‌عبارتی‌دیگر، اکنون از هوش مصنوعی به‌عنوان یک منبع کسب معرفت علمی استفاده می‌کنیم. قابل‌توجه است که فیلسوفان در برابر چیستی پاسخ‌های هوش مصنوعی به این قبیل پرسش‌ها نظرات مختلفی دارند[۲] [۳] [۴] [۵] [۶] . در روش‌های یادگیری ماشین، عموماً از داده‌هایِ آموزشی برای یادگیری استفاده می‌شود [۹]. استفاده از داده‌هایِ علمی، به‌عنوان داده‌های آموزشی برای مواردی که خروجیِ ماشین، پاسخ به یک پرسش علمی است، این تصور را پدید می‌آورد که شاید بتوان این خروجی‌ها را یک گواهی گروهی متخصصین در نظر گرفت. هدف از این پژوهش بررسی این پرسش است که این خروجی‌ها را می‌توان گواهی دانست یا خیر؟ در برابر این پرسش پاسخ‌های مختلفی ارائه‌شده که در ادامه موردبررسی و نقد قرار خواهند گرفت. برای رسیدن به هدف پژوهش، ابتدا با مروری بر ادبیات و پیشینه پژوهش، به بررسی آثار سایر پژوهشگران پرداخته می‌شود. سپس، تعریف هوش مصنوعی به‌اختصار بیان خواهد شد تا مشخص شود چه چیزی را هوش مصنوعی خطاب می‌کنیم. در پایان گواهی و نظریات غالب در خصوص خروجی‌های هوش مصنوعی به نقد و بررسی گذاشته می‌شود.

۱.۱ مروری بر پژوهش‌های دیگران

گواهی را می‌توان یکی از موضوعات مهم پژوهش‌های معرفت‌شناسی تحلیلی دانست که ادبیات فربه‌ای حول آن شکل گرفته است. در این خصوص یکی از پرسش‌های اصلی این است که آنچه از خروجی ماشین به دست می‌آید را چه باید در نظر گرفت؟ آیا می‌توان آن را گواهی دانست یا خیر؟ در برابر این پرسش، سه دیدگاه اصلی وجود دارد. طرفداران دیدگاه اول معتقدند دانش به‌دست‌آمده از تکنولوژی دیجیتال و ابزار را نمی‌توان گواهی دانست. این دیدگاه با تکیه‌بر رویکردهای سنتی در معرفت‌شناسی، معتقد است که منبعِ دانشِ تکنولوژی، یک منبع واحد (فرد انسانی) نیست و از این موضوع نتیجه می‌گیرد که نمی‌توان آن را گواهی خواند [۵] [۴] [۳]. دیدگاه دوم برخلاف دیدگاه اول، دانش به‌دست‌آمده از ابزار را گواهی می‌داند. این دیدگاه با تکیه‌بر این موضوع که زبان یک ابزار ارتباطی است و برای گواهی از آن استفاده می‌شود، معتقد است دانش به‌دست‌آمده از سایر ابزارهای ارتباطی را نیز می‌توان گواهی دانست. قابل‌توجه است که این دیدگاه، بر ابزار ارتباطی بودن هوش مصنوعی تکیه دارد و هوشمندی را در نظر نمی‌گیرد [۶]. دسته سوم، دیدگاهی است که دانش به‌دست‌آمده از تکنولوژی را «شبه-گواهی[۳]» می‌خواند؛ تا هم بر شباهت آن بر گواهی تأکید کند و هم بر اینکه خروجی از سوی یک انسان ارائه نشده و از یک تکنولوژی هوشمند به‌دست‌آمده است[۴] [۳].

[۲] البته برخی پژوهشگران به‌جای پاسخ به این قبیل پرسش‌ها تنها به تغییرات الگوریتمی برای بهبود خروجی‌های توجه دارند [۷] [۸].

[3] Quasi-testimony

[۴] شایان‌ذکر است که پژوهش‌ها در این حوزه گسترده است، برخی از آن‌ها گاهی مباحثی اخلاقی در خصوص گواهی را در ذیل موضوعاتی همچون سوگیری [۱۱] [۱۰]، شفافیت [۱۳] [۱۲]، عاملیت [۱۵] [۱۴] و غیره موردبررسی قرار داده‌اند. دسته‌ای دیگر نیز به محدودیت‌های هوش مصنوعی همچون محدودیت‌های الگوریتمی و عدم امکان تقلیل تجربه انسانی به داده‌هایِ کمی در حوزه دانش علمی پرداخته‌اند [۱۶].

۲ هوش مصنوعی

تعاریف متعددی برای هوش مصنوعی ارائه شده است. دسته‌ای از تعاریف، هوش مصنوعی قوی[۵] را به ذهن متبادر می‌سازند. به‌عنوان‌مثال برخی معتقدند هوش مصنوعی تلاش برای ساخت سیستم‌های کامپیوتری است که مانند یک فرد انسانی عمل یا فکر کنند [۱۷]. یا در تعریفی دیگر آورده شده هوش مصنوعی به ساخت و مطالعه ماشین‌هایی می‌پردازد که توانایی حس کردن، تصمیم‌گیری و عمل مانند یک انسان را داشته باشند [۱۸]. صرف‌نظر از اینکه امکان دستیابی به هوش مصنوعی قوی در آینده وجود دارد یا خیر، اکنون به چنین ظرفیتی دست نیافته‌ایم و لذا این قبیل تعاریف کمی دور از واقعیت هستند. البته این تعاریف با ایراداتی نیز روبرو می‌شوند؛ مثلاً هوش مصنوعی می‌تواند در کلان داده‌ها الگوهایی را بیابد که برای یک فرد انسانی امکان‌پذیر نیست [۱۹] و یا سرعت و دقت محاسبات سیستم‌های کامپیوتری بسیار بیشتر از یک انسان است. لذا برابری با هوشمندی انسان، همیشه مفید و موردنظر نیست. پس به تعریفی نیاز داریم که بتواند هوش مصنوعی را مطابق و یا حداقل نزدیک به آنچه اکنون هست توصیف کند و در ضمن متمرکز بر هم‌سطح بودن با هوشمندی انسان نباشد. بر این اساس، با تکیه‌بر تعریف دائره‌المعارف استنفورد، هوش مصنوعی را سیستم محاسباتی در نظر می‌گیریم که برای دستیابی به هدف، رفتاری هوشمندانه اتخاذ می‌کند و این هوشمندی ممکن است با هوشمندی انسان متفاوت باشد [۲۰]. با تکیه‌بر این تعریف، در پژوهش حاضر زمانی که از اصطلاح هوش مصنوعی استفاده می‌شود، مقصود آن چیزی است که امروز به آن دست‌یافته‌ایم.

۳ گواهی علمی و خروجی ماشین

ممکن است ما از گواهی[۶] در زمینه‌های مختلفی برای کسب دانش استفاده کنیم؛ حال‌آنکه یکی از مهم‌ترین آن‌ها دانش علمی است. مرجعیت معرفت‌شناختی علم به‌صورت کلی از سوی جامعه علمی به دست می‌آید. این مرجعیت مشخص می‌کند چگونه با ادعاهای معرفتی و گواهی برخورد کنیم. نظامِ دانشِ علمی، تابعِ

[5] Strong Artificial Intelligence

[۶] در پژوهش‌های فلسفی بیشتر به توجیه گواهی توجه می شود که در این خصوص می‌توان چهار دیدگاه را از یکدیگر تمیز داد. مطابق دیدگاه اول توجیه باور شنونده به گواهی گوینده بر اساس دلایل شنونده برای درستی گواهی گوینده است [۲۲] [۲۱]. مطابق با دیدگاه دوم پایایی روند/روندهای گواهیِ گوینده مبنای توجیه باور شنونده به‌درستی گواهی او است [۲۵] [۲۴] [۲۳]. بر اساس دیدگاه سوم باور شنونده به گواهی گوینده، بر مبنای توجیه گوینده برای گواهی خود است [۲۸] [۲۷] [۲۶]. دیدگاه چهارم، شنونده، روند/روندهای گواهی و توجیه گوینده را همگی مبنای توجیه باور شنونده به گواهی گوینده می‌داند [۲۹]. سه دیدگاه اول، هرکدام با مشکلاتی روبرو هستند. استفان رایت [۳۰] نشان می‌دهد که دیدگاه اول گاهی خطر زودباوری را به وجود می‌آورد. دیدگاه دوم موجه بودن دانش علمی به‌دست‌آمده از گواهی را تنها بر اساس پایایی روند گواهی فرو می‌کاهد؛ و دیدگاه سوم موجه بودن گواهی برای شنونده را قابل‌انتقال می‌داند. او نشان می‌دهد هر سه گروه از این نظریات در جایگاه خود می‌تواند مبنای موجه بودن گواهی قرار بگیرد؛ اما یک نظریه کامل‌تر نیاز است تا هر سه دیدگاه را پوشش دهد. لذا دیدگاه چهارم که می‌توان آن را نظریه «ترکیبی» دانست برای توجیه باور به‌دست‌آمده از انواع گواهی مناسب‌تر باشد. اگرچه بخش قابل‌توجهی از مطالعات به توجیه در گواهی می‌پردازند اما موضوعاتی همچون عوامل اجتماعی [۳۱]، اعتماد [۳۲] و غیره نیز موردنظر قرارگرفته‌اند. به‌عنوان نمونه شاپین [۳۱] با بررسی تولید علم در قرن انگلستان قرن هفدهم، نشان می‌دهد در این عصر کلمه جنتلمن نقش پررنگی در باور به صداقت گوینده برای گواهی وجود داشته است. در این دوره جنتلمن به فردی خطاب می‌شد که تحت تأثیر عوامل اقتصادی قرار نمی‌گرفت و فشارها نمی‌توانست باعث شود او از گفتن حقیقت باز بماند. یا در خصوص اعتماد، اوری فریمن [۳۲] در پژوهش خود معتقد است که در معرفت‌شناسی اجتماعی جریان اصلی سه فرض وجود دارد، گواهی دهنده ۱- التفات به ارائه گواهی داشته باشد، ۲- مشمول ارزیابی هنجاری باشد و ۳- هدفی برای ایجاد روابط مبتنی بر اعتماد تشکیل شود.

الزاماتِ معرفتی است که امکان دارد در طول تاریخ و در مسیر تحقیق تغییر کنند. طبیعت هنجارهای دانش را برای ما آشکار نمی‌کند؛ بلکه دانش علمی وابسته به مسیر است. فرآیند تاریخی کسب دانش علمی ممکن است بر نتیجه آن تأثیر بگذارد. ارزش‌های معرفت‌شناختی با ایجاد روابط معنادار، پژوهش علمی را در جهت‌های مشخصی هدایت می‌کنند و این موضوع می‌تواند در طول زمان تغییرات شگرفی ایجاد کند [۳۳]. اکنون‌که از هوش مصنوعی برای دانش علمی استفاده می‌کنیم با شرایط جدیدی روبه‌رو هستیم. یک پرسش اساسی این است که آنچه از خروجی هوش مصنوعی در برابر پرسش‌های علمی به دست می آوریم چیست؟ همان‌طور که پیش‌تر اشاره شد، سه دیدگاه اصلی در برابر این پرسش وجود دارد. دیدگاه سنتی که دانش به‌دست‌آمده از ابزار و تکنولوژی را گواهی نمی‌داند. دیدگاه دوم که دانش به‌دست‌آمده از ابزار ارتباطی را گواهی می‌داند. دیدگاه سوم که این دانش را شبه-گواهی یا «باور مبتنی بر تکنولوژی[۷]» می‌داند. پاسخ هایی که از هوش مصنوعی در برابر پرسش‌های علمی به دست می‌آید، عموماً بر اساس داده‌ها و منابع اطلاعاتی است که توسط دانشمندان و متخصصین ثبت شده یا از پژوهش‌های آن‌ها جمع‌آوری می‌شود. آیا در چنین شرایطی، نمی‌توان خروجی را گواهی گروهی دانست؟ در برابر این پرسش، اوری فریمن به‌عنوان نظریه‌پردازِ نظریهِ شبه-گواهی معتقد است نمی‌توان خروجی هوش مصنوعی را یک گواهی گروهی دانست[۸]. او با تکیه‌بر معرفت‌شناسیِ اجتماعی جریان اصلی عقیده دارد تصور خروجی هوش مصنوعی به‌عنوان گواهی گروهی، بر دو مبنا استوار است و او هر دو را رد می‌کند. بر اساس اولین مبنا، برای رسیدن به خروجی هوش مصنوعی از گواهی‌های فردی برای داده‌های آموزشی استفاده می‌شود؛ و بر اساس دومین مبنا، خروجیِ هوشِ مصنوعی، گواهیِ گروهیِ جامعهِ متخصصین آن حوزه دانش است. فریمن معتقد است که اتخاذ چنین دیدگاهی به این معنا خواهد بود که یا هوش مصنوعی را یک دانای جمعی بدانیم که دانش افراد متخصص را در دسترس دارد و بر اساس آن گواهی می‌دهد؛ یا اینکه هوش مصنوعی گواهی افراد را با یکدیگر تطبیق داده و گواهی گروهی به دست می‌دهد. وی معتقد است هر دو این اشکال، به معنی انسان انگاری[۹] هوش مصنوعی است. ازآنجاکه هوش مصنوعی یک انسان هوشمند نیست، او نتیجه می‌گیرد که نمی‌توان هیچ‌کدام از این دو شکل را پذیرفت. همچنین او استدلال می‌کند که اگر خروجی هوش مصنوعی را گواهی گروهی متخصصین بدانیم، آنگاه مسئولیت و فعالیت‌های انسانی در ساخت هوش مصنوعی نادیده گرفته شده و تحلیل الگوریتم‌ها به‌منظور چگونگی توجیه خروجی‌های به‌دست‌آمده بی‌معنا خواهد بود. ایراد دیگر او این است که گواهی جمعی نیازمند التفات افراد گروه برای یک گواهی است؛ حال‌آنکه افرادی که هوش مصنوعی از اطلاعات آن‌ها برای رسیدن به خروجی استفاده کرده است، فاقد التفات برای گواهی گروهی بوده‌اند [۳]. در برابر استدلال‌ها و ایرادات فریمن و دو دیدگاه دیگر، ما تجربه‌گراییِ انتقادیِ زمینه ایِ[۱۰] هلن لانجینو را قرار می‌دهیم تا این دیدگاه‌ها را موردبررسی قرار دهیم[۱۱]. بر اساس این نظریه، دانش علمی نیازمند تعامل انتقادی میان اعضای جامعه علمی

[7] Technology-based belief

[۸] البته پیش‌ازاین موضوع، استدلال‌های فراوانی در رد رویکرد سنتی و ابزاری نیز ارائه می‌کند [۳].

[9] Anthropomorphizes

[10] Critical Contextual Empiricism (CCE)

[۱۱] در برابر این پرسش که چرا نظریه لانجینو برای این مقصود استفاده شده است باید گفت: موضع فریمن بر اساس معرفت‌شناسی اجتماعی جریان اصلی است [۳۲]. در برابر این جریان، لانجینو قصد دارد تا معرفت‌شناسی اجتماعی را واقعاً اجتماعی کند. به

است. لانجینو نشان می‌دهد معرفت‌شناسیِ اجتماعیِ جریانِ اصلی، در تلاش است تا پارادایم‌های گواهی فردی مانند باور و توجیه را به نهادها و گروه‌ها نسبت دهد یا تأثیرات شرایط گروه بر افراد را بررسی کند. او استدلال می‌کند که این‌گونه نظریات، روند تولید دانش علمی را موردتوجه قرار نمی‌دهند. برای تبیین این موضوع وی نشان می‌دهد حداقل پنج مفهوم از اجتماعی بودن وجود دارد: ۱- اجتماعی از افراد در جهان که در کنار دیگران هرکدام کاری را انجام می‌دهند؛ ۲- اجتماعی از حداقل دو فرد یا بیشتر که با یکدیگر کاری انجام می‌دهند؛ ۳- اجتماعی از افراد که چیزی یا اعتقادی مشترک دارند؛ ۴- اجتماعی که در آن ارزش‌های غیرمعرفتی باورهای افراد را تحت تأثیر قرار می‌دهند؛ ۵- اجتماع تعاملی. لانجینو نشان می‌دهد زمانی که اجتماعی بودن را معادل یکی از چهار مفهوم اول بدانیم، پرسش‌های معرفت‌شناسی اجتماعی ذیل پرسش‌های معرفت‌شناسی فردی قرار می‌گیرند. در چنین شرایطی، معرفت‌شناسی اجتماعی جریان اصلی در تقابل دوگانه میان ۱- چالش‌های معرفت‌شناسی سنتی مانند اختلالات ادراک و یا معضلات عوامل معرفتی در موقعیت‌های اجتماعی و ۲- برخورد با گروه به‌عنوان عامل شناختی، قرار دارد. درصورتی‌که اگر به عمل تولید دانش علمی توجه داشته باشیم، می‌دانیم که اجتماعی بودن ویژگی سازنده این دانش است. در تولید و شکل‌گیری دانش علمی، این روندها و به‌ویژه روندهای تعاملی هستند که نقشی تعیین‌کننده دارند[۱۲]. دانش علمی، خروجیِ تعاملِ اجتماعی است و جوامع علمی، عوامل کانونی معرفتی آن هستند؛ و دانش افراد مشتق شده و وابسته به عضویت و مشارکت آن‌ها در این جوامع است[۱۳]. لانجینو در حقیقت دیدگاهی را اتخاذ می‌کند که بین سطح گروهی و فردی قرار دارد. مطابق با این نظریه، افراد بر اساس مشارکت در تعامل‌ها به عامل معرفتی در تولید دانش علمی تبدیل می‌شوند. همچنین شکل‌گیری گروه در این نظریه، بر اساس ارتباط در شبکه‌ای از تعاملات درک می‌شود. قابل‌توجه است که در جامعه علمی این شبکه‌ها دارای ساختار ثابتی نیستند و ممکن است افراد مختلف به آن‌ها وارد شده یا خارج شوند و هرکدام درجه‌ای از ارتباط را در شبکه‌ها داشته باشند. به این شیوه لانجینو جامعه علمی و پدیده‌های اجتماعی را پویا در نظر می‌گیرد و هنجارهای معرفتی به‌جای حالات گروه یا افراد، به تعاملات می‌پردازد [۳۴] تا معرفت‌شناسی اجتماعی واقعاً اجتماعی

همین منظور با مطرح کردن سه موضوع، او معرفت‌شناسی اجتماعی را اصلاح می‌کند. اول آنکه از منظر تاریخی و عملیِ فلسفهِ علم که جامعه علمی را موردنظر قرار می‌دهد، اختلاف‌نظر میان افراد نقشی سازنده در علم دارد. دوم، جامعه تنها مجموعهٔ افرادی که در کنار دیگران زندگی می‌کنند یا اعضای یک گروه که عقاید مشترکی دارند نیست. شباهت و اشتراک نظر افراد مفهومی ضعیف از جامعه را در نظر می‌گیرد. سوم اگر دانش علمی که دانشی تجربی است را معتبرترین شکل دانش بدانیم، تحلیل‌های معرفت‌شناختی هم باید ازآنجا آغاز شود. عوامل شناختی در علوم افراد منزوی نیستند، بلکه در شبکه‌های پیچیده جامعه با یکدیگر در تعامل هستند که شامل مشارکت، انتقاد و اشتراک‌گذاری اطلاعات می‌شود [۳۲].

[۱۲] باید توجه داشت که تعامل نه به معنای عملی مشترک و در کنار هم و نه به معنای تبادل ایده و اشتراک‌گذاری است؛ بلکه مقصود لانجینو از تعامل به معنای تأثیرگذاری و تأثیرپذیری دوسویه میان عوامل انسانی است [۳۴]. در اینجا مشخص می‌شود چرا از اصطلاح انتقادی در نام این نظریه استفاده می‌شود. آنچه این نظریه را انتقادی می‌کند این است که مطابق با تعامل و انتقاد مستمر و دوسویه است که مفروضات علمی مورد تائید و انتقاد قرارگرفته، اصلاح‌شده و به‌صورت عمومی میان جامعه علمی آشکار می‌شود [۳۵].

[۱۳] لانجینو از اختلاف‌نظر (Disagreement) و گواهی برای اثبات گفته خود استفاده می‌کند. در معرفت‌شناسی اجتماعی جریان اصلی، اختلاف‌نظر میان عوامل معرفتی در جامعه علمی یکی از ابزارهای اولیه‌ای است که به‌وسیله آن می‌توان مفروضاتی که در پرتو آن‌ها داده‌ها ارزیابی می‌شوند را مشخص کرده و در معرض بررسی دقیق قرار داد. گواهی در دانش علمی در جریان اعمال شناختی (مشاهده، استدلال) که به باور/دانش در خصوص روابط گواهی منتج می‌شود حضور دارد. مقولات و هنجارهای پیش‌فرض در جریان عمل علمی است که پدید می‌آیند. در حقیقت اختلاف‌نظر و گواهی در جریان عمل تولید دانش علمی به وجود می‌آیند [۳۴].

شود.

۴ بحث و بررسی

سه دیدگاه در برابر خروجی هوش مصنوعی معرفی شد. دیدگاه نخست، به علت اینکه منبعِ دانشِ تکنولوژی، یک منبع واحد (یک فرد) نیست نتیجه می‌گیرد که نمی‌توان آن را گواهی خواند. این دیدگاه از این مشکل رنج می‌برد که نمی‌تواند تولید دانش علمی را موردنظر قرار دهد. اگر بر اساس این دیدگاه پیش برویم، منبع گواهی جوامع علمی نیز یک منبع واحد نیست و افراد مختلفی را شامل می‌شود؛ لذا احتمالاً باید بگوییم که گواهی برای جامعه علمی نیز امکان‌پذیر نیست. دیدگاه دوم، هوش مصنوعی را یک ابزار ارتباطی در نظر می‌گیرد. اشتباه این دیدگاه در این است که روند رسیدن هوش مصنوعی به خروجی را در نظر نمی‌گیرد. اگر صرفاً هوش مصنوعی را ابزار ارتباطی بدانیم، مانند این است که خروجی هوش مصنوعی همان گواهی دانشمندان است و چیزی در جریان یادگیری تغییر نکرده است. در حقیقت این دیدگاه، هوش مصنوعی را به یک پایگاه داده‌ها تقلیل می‌دهد که در برابر یک درخواست، یک خروجی را منتشر می‌کند. لذا این دیدگاه از عدم شناخت هوش مصنوعی رنج می‌برد. بر اساس دیدگاه سوم یا نظریه فریمن، اگر خروجی هوش مصنوعی را گواهی گروهی در نظر بگیریم باید یکی از این دو حالت را بپذیریم: ۱- هوش مصنوعی به‌عنوان یک دانای جمعی که دسترسی به دانش افراد متخصص دارد؛ ۲- هوش مصنوعی گواهی افراد را با یکدیگر تطبیق می‌دهد. در اینجا سه ایراد به سخنان فریمن وارد می‌شود. اول آنکه دسترسی به داده‌ها و تطبیق آن‌ها در هوش مصنوعی امری دور از انتظار نیست؛ در حقیقت این هردو حالت در جریان یادگیری ماشین رخ می‌دهند. هدف فریمن از تصور این دو حالت رد انسان‌انگاری هوش مصنوعی[۱۴] و توجه به نقش و مسئولیت سازندگان هوش مصنوعی و اهمیت بررسی الگوریتم‌ها است. در اینجا ایراد دوم و سوم نمایان می‌شوند. بر اساس ایراد دوم، انسان انگاری هوش مصنوعی از نظر فریمن متکی بر معرفت‌شناسیِ اجتماعیِ جریانِ اصلی است. با توجه به آنچه لانجینو به ما نشان داد، هر دو حالتی که فریمن متصور می‌شود، بر اساس نسبت دادن ویژگی‌های گواهی فرد به گواهی گروه است. فریمن گواهی گروهی را ذیلِ مجموعِ گواهیِ افراد در نظر می‌گیرد. حال اگر این دیدگاه را کنار بگذاریم و به شکلی اجتماعی به گواهی گروهی در دانش علمی نگاه کنیم، ۱- گواهی گروهی به یک دانای جمعی منتسب نمی‌شود و ۲- گواهی گروهی در روندی تعاملی و در شبکه‌ای پیچیده شامل مشارکت، انتقاد و اشتراک‌گذاری اطلاعات و در جریان تولید دانش علمی به دست می‌آید و نه بر اساس تطبیق نظرات افراد. مطابق با سومین ایراد، فریمن برای توجه به اخلاق و حقوق هوش مصنوعی و طراحان آن، بر حقوق و اخلاق جامعه علمی چشم می‌پوشد. البته که مشارکت و مسئولیت سازندگان و طراحان هوش مصنوعی در رسیدن به خروجی مهم است؛ اما این موضوع به معنای بی‌اهمیت بودن داده‌ها و اطلاعات جامعه علمی که در هوش مصنوعی برای رسیدن به آن خروجی استفاده شده نیست. همچنین توجه به این داده‌ها و اطلاعات، به معنای نادیده انگاشتن نقش و اهمیت بررسی الگوریتم‌ها در رسیدن به خروجی نیست. در ایراد دیگر فریمن به عدم

[۱۴] قابل‌توجه است که فریمن در پژوهش دیگری نیز این موضوع را به‌وضوح بیان می‌کند که عقیده دارد گواهی تنها برای فرد امکان‌پذیر است، زیرا بر اساس معرفت‌شناسی جریان اصلی، گواهی تنها برای فرد امکان‌پذیر است [۳۲].

التفات افرادی که هوش مصنوعی از داده‌ها و اطلاعات آن‌ها برای ارائه خروجی استفاده کرده است برای رد گواهی گروهی استفاده می‌کند. او التفات فرد را برای گواهی گروهی امری ضروری می‌داند. اگر به سخنان لانجینو باز گردیم، متوجه خواهیم شد که تولید دانش علمی بر اساس روندهای تعاملی صورت می‌گیرد و نه التفات افراد. افراد ممکن است در زمان‌های مختلف در فرآیند تولید علم، عامل معرفتی باشند و زمانی از آن جامعه خارج شده و افراد دیگر جایگزین شوند. در مسیر تولید دانش علمی، افراد مشارکت‌کننده در جامعه علمی به نقد و مخالفت با یکدیگر می‌پردازند. به‌عبارتی‌دیگر تصور اینکه در تولید دانش علمی، التفات مشترک برای رسیدن به یک گواهی گروهی مشخص میان افراد جامعه علمی وجود دارد، امری است که با واقعیت جامعه علمی و روند تولید دانش علمی همخوانی ندارد. لذا می‌توان این‌طور نتیجه گرفت که التفات فرد در تعامل برای گواهی گروهی امری ضروری نیست و می‌توان این ایراد فریمن را رد کرد. تا به اینجا دلایل فریمن در خصوص رد گواهی گروهی خواندن دانش علمی موردنقد قرار گرفت. حال توجه به دو نکته ضروری است. اول اینکه ایرادات به نظرات فریمن، برای گواهی در خصوص دانش علمی وارد است. به‌عبارتی‌دیگر، این ایرادات مربوط به زمینه دانش علمی هستند و به معنای رد کامل نظریه او در خصوص گواهی در سایر حوزه‌ها نیست که این موضوع را می‌توان در پژوهش‌های دیگری پیگیری کرد. دوم آنکه ایرادات وارد شده به نظرات فریمن، به معنای آن نیست که خروجی به‌دست‌آمده از هوش مصنوعی را گواهی گروهی در حوزه دانش علمی بدانیم. مطابق با تجربه‌گراییِ انتقادیِ زمینه‌ایِ می‌توان با فریمن در خصوص آنکه نمی‌توان خروجی هوش مصنوعی در حوزه دانش علمی را گواهی گروهی دانست، همدل بود؛ چراکه این خروجی‌ها شرایط لازم برای گواهی گروهی را از این دیدگاه نیز ندارند. از منظر تجربه‌گرایی انتقادی زمینه‌ای که می‌توان آن را معرفت‌شناسی اجتماعی به معنای قوی درک کرد[۱۵]، برای تولید دانش علمی و گواهی علمی نیازمند تعاملات اجتماعی هستیم. آنچه در هوش مصنوعی برای رسیدن به خروجی صورت می‌گیرد تعاملات اجتماعی پویا در جامعه علمی نیست. لذا شاید تا زمان رسیدن به چنین مرحله‌ای بهتر باشد به‌مانند فریمن، این خروجی را دانش مبتنی بر تکنولوژی بخوانیم. چراکه اولاً دانش است، دوما این دانش شرایط گواهی یعنی تعاملات اجتماعی را ندارد و نمی‌توان آن را گواهی خواند و به‌نوعی تفاوت این دانش با گواهی گروهی متخصصان علمی مشخص می‌شود و سوما با استفاده از تکنولوژی به این دانش دست‌یافته‌ایم؛ که به این شیوه مشارکت و مسئولیت طراحان در نظر گرفته شده و بررسی الگوریتم‌ها نیز دور از نظر نمی‌ماند.

۵ نتیجه‌گیری

در برابر پاسخ‌های ماشین به پرسش‌های علمی سه دیدگاه اصلی وجود دارد که از منظر تجربه‌گرایی انتقادی زمینه‌ای، هر سه قابل نقد هستند. دیدگاه سنتی گواهی را محدود به یک منبع واحد (یک فرد) می‌کند. این دیدگاه به علت اینکه روند تولید دانش علمی را به فرد محدود کرده و نمی‌تواند تولید علم و جامعه علمی را موردبررسی قرار دهد قابل نقد است. دیدگاهی که هوش مصنوعی را ابزار ارتباط در نظر می‌گیرد، بر شناختی نادرست از هوش مصنوعی استوار است و رد می‌شود. دیدگاه سوم که خروجی‌های هوش مصنوعی را شبه-

[۱۵] به سخنی دیگر معرفت‌شناسی اجتماعی که واقعاً اجتماعی است.

گواهی می‌داند بر معرفت‌شناسی اجتماعی جریان اصلی تکیه کرده و اشتباهات این جریان را با خود به همراه دارد. بررسی‌های انتقادات و استدلال‌های فریمن نشان می‌دهد که این رویکرد در بررسی گواهی گروهی، بر نگاهی فردی استوار است و تعاملات اجتماعی تولید دانش علمی و گواهی علمی را در نظر نمی‌گیرد. در ادامه مشخص شد که اگرچه دیدگاه شبه-گواهی دچار اشتباه است، اما خروجی هوش مصنوعی در برابر پرسش‌های علمی، شرایط لازم گواهی گروهی را ندارد.

مراجع

[1] M. Steup, R. Neta. (2020). Epistemology [Online]. Available: https://plato.stanford.edu/entries/epistemology/

[2] L. Nick. (2023). Epistemological Problems of Testimony [Online]. Available: https://plato.stanford.edu/entries/testimony-episprob/

[3] O. Freiman. “Analysis of Beliefs Acquired from a Conversational AI: Instruments-based Beliefs, Testimony-based Beliefs, and Technology-based Beliefs”. Episteme. 2023, pp. 1-17.

[4] S.C. Goldberg. (2012). “Epistemic extendedness, testimony, and the epistemology of instrument-based belief”. Philosophical Explorations, Vol. 15, Issue 2. 2012, pp. 181-197.

[5] S.C. Goldberg. “Epistemically engineered environments”. Synthese, Issue 197. 2017, pp. 2783–2802.

[6] S. Kletzl. “Scrutinizing thing knowledge”. Studies in History and Philosophy of Science Part A, Issue 47, 2014, pp. 118-123.

[7] E. Bozdag, J. Van Den Hoven. “Breaking the filter bubble: democracy and design”. Ethics and information technology, Vol. 17, Issue 4. 2015, pp. 249-265.

[8] F. Masrour, T. Wilson, H. Yan, P. Tan, A. Esfahanian. “Bursting the filter bubble: Fairnessaware network link prediction”. Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 34, Issue 01. 2020. pp. 841-848.

[9] A. Jung. Machine Learning, Singapore: Springer, 2022, pp. 19-39.

[10] O. Keyes, Z. Hitzig, M. Blell. “Truth from the machine: artificial intelligence and the materialization of identity”. Interdisciplinary Science Reviews, Vol. 46, Issue 1-2. 2021, pp.158-175.

[11] T. Panch, H. Mattie, R. Atun. “Artificial intelligence and algorithmic bias: implications for health systems”. Journal for health systems. Vol. 9, Issue 2. 2019.

[12] P.D. Winter, A. Carusi. “(De)troubling transparency: artificial intelligence (AI) for clinical applications”. Medical Humanities. Vol. 49, Issue 1. 2023, pp.17-26.

[13] C. Zednik, H. Boelsen. “Scientific exploration and explainable artificial intelligence”. Minds and Machines. Vol. 32, Issue 1. 2022, pp. 219-239.

[14] B.D. Lund, T. Wang, N.R. Mannuru, B. Nie, S. Shimray, Z. Wang. “ChatGPT and a new academic reality: Artificial Intelligence-written research papers and the ethics of the larg

language models in scholary publishing". Journal of the Association for Information Science and Technology. Vol 74, Issue 5. 2023, pp. 570-581.

[15] K. Huang, T. Fu, W. Gao, Y. Zhao, Y. Roohani, J. Leskovec. W.C. Conner, X, Cao, J. Sun, M. Zitnik. "Artificial intelligence foundation for therapeutic science". Nature chemical biology, Vol. 18, Issue 10. 2022, pp. 1033-1036.

[16] B. Chin-Yee, R. Upshur. "Three problems with big data and artificial intelligence in medicine". Perspectives in Biology and Medicine. Vol. 62, Issue 2. 2019, pp. 237-256.

[17] S. Russel, P. Norvig. Artificial intelligence: A modern approach. Forth edition. London: Pearson. 2020, pp. 1-2.

[18] B. Mondal. "Artificial intelligence: state of the art". Recent trends and advances in artificial intelligence and internet of things. 2020, pp. 389-425.

[19] V. Muller. "Deep opacity undermines data protection and explainable artificial intelligence". In symposium Overcoming opacity in machine learning, Ed. C. Zednik, H. Boelsen. 2021, pp. 18-21.

[20] V. Muller. (2021). Ethics of Artificial intelligence and robotics [Online].

[21] E. Fricker. Against gullibility. In Knowing from words. Dprdrecht: Springer, pp. 125-161, 1994

[22] R. Fumerton. "The epistemic role of testimony: Internalist and externalist perspectives" in The Epistemology of Testimony. E. Sosa, J. Lackey, Ed. United Kingdom: Clarendon Press, 2006, pp. 77-92.

[23] S. Goldberge. Relying on others: An essay in epistemology. Oxford: Oxford University Press, 2010.

[24] J. Lackey. "Learning from words". Analysis. Vol. 60. Issue 3. 2009.

[25] E. Sosa. Epistemology: Oxford Bibliographies Online Research Guide. Oxford: Oxford University Press, 2010.

[26] T. Burge. "Content preservation". The Philosophical Review. Vol. 102. Issue 4, pp. 457-488, 1993.

[27] P. Faulkner. Epistemology of testimony. In Philosophical Perspectives for Pragmatics, Ed. M. Sbisa, J. Ostman, J. Verschueren. Amesterdam: John Benjamins Publishing Company, 2011, pp. 82-84.

[28] S. Wright. "Sosa on knowledge from testimony". Analysis, Vol. 74, Issue 2, 2014, pp. 249-254.

[29] M. Gerken. "Internalism and externalism in the epistemology of testimony". Philosophy and phenomenological research, Vol. 87, Issue 3. 2013, pp. 532-557.

[30] S. Wright, "The nature of testimonial justification," Ph.D. dissertation, Dept. Philosophy. Eng., Sheffield Univ., Sheffield, South Yorkshire, 2014.

[31] S. Shapin, A social History of Truth. Chicago: University of Chicago Press, 1994.

[32] O. Freiman, “The role of knowledge in the formation of Trust in Technologies,” Ph.D. dissertaion, Dep, Philosophy, Bar-Ilan University, Ramat Gan, 2021.

[33] M. Carrier. “Historical epistemology: O the diversity and change of epistemic values in science”. Berichte zur Wissenschaftsgeschichte. Vol. 35, Issue 3. 2012, pp. 239-251.

[34] H. Longino. “What’s Social About Social Epistemology?”, The Journal of Philosophy. Vol. 119, Issue 4. 2022, pp. 169-195.

[35] A. K. Yee. “Machine Learning, Misinformation, and Citizen Science”. European Journal for Philosophy of Science. 2023, Preprint.

دلیل عقلی جرم‌انگاری سایبری مبتنی بر قاعده اعانت بر اثم

محسن نادری[۱]، علی‌اکبر ایزدی فرد[۲]، محمدمهدی زارعی[۳]

[۱] دانشجوی کارشناسی ارشد فقه و مبانی حقوق اسلامی، دانشگاه مازندران
mnnnnarsenal9085@gmail.com
[۲] عضو هیئت علمی دانشگاه و استاد فقه و مبانی حقوق اسلامی، دانشگاه مازندران
izadifard@umz.ac.ir
[۳] استادیار و عضو هیئت علمی گروه فقه و مبانی حقوق اسلامی دانشگاه مازندران
m.zarei@umz.ac.ir

چکیده

امروزه عقل ابر لزوم بهره‌گیری از فضای مجازی جهت تسهیل در امور مختلف اتفاق نظر دارند. برای کارآیی و بهره‌گیری مطلوب از این فضا مدیریت و سازماندهی قانونی فضای مجازی امری عقلانی و شایان توجه است. پژوهش حاضر با روش توصیفی-تحلیلی و مراجعه به کتب فقهی و آراء فقها، همراه با توجیه، تبیین، استدلال و استنتاج است. فرصت‌ها و چالش‌های فضای مجازی با عنایت به لزوم حفظ امنیت عمومی جامعه ضمن احترام به حرمت و حریم خصوصی اشخاص حقیقی و حقوقی موجب نگرانی و دغدغه در شیوه حکمرانی منطقی و اصولی بر این فضاشده است. ارائه چارچوب و ضابطه عقلایی مبتنی بر فرهنگ و عقاید جامعه جهت ورود و استفاده از فضای مجازی امری لازم و ضروری است و لزوم و اقتضای این مهم را عقل مستقلاً درک می کند. از یافته‌های پژوهش حاضر می‌توان به ضرورت عقلانی بهره‌گیری از عامل تنظیم‌کننده و سازمان‌دهنده استفاده از فضای مجازی اشاره کرد که همان «قانون» نام دارد و عدم وجود آن موجب هرج و مرج، نابسامانی و اختلال در امنیت روانی جامعه می‌شود و در نهایت استفاده از قواعد کاربردی فقهی نظیر قاعده اعانت بر اثم با رویکرد تبیینی-تنبیهی می‌توانند در ساماندهی بیش از پیش فضای سایبری مؤثر باشند.

کلمات کلیدی: فضای مجازی، اعانت بر اثم، مجازات، علم فقه، پیشگیری.

۱ مقدمه

تعاریف متفاوت و گوناگونی از فضای مجازی ارائه شده است. از جمله این تعاریف آن است که «فضای مجازی یا فضای سایبر، مفهومی برای توصیف فناوری دیجیتال به هم پیوسته گسترده‌است». نمی‌توان فضای مجازی را مترادف با اینترنت دانست، اما اینترنت ابزار ورود به فضای مجازی است (سیاح طاهری دیگران، ۱۳۹۶، ج۱: ۳۰). اشخاص می‌توانند با استفاده از این فضا تعامل و تبادل‌ایده، اشتراک‌گذاری اطلاعات، انجام کار،

بازی کردن، فعالیت‌های اجتماعی، هنری، سیاسی و غیره را انجام دهند.

فضای مجازی نقطه مقابل فضای حقیقی است. این فضا از چهارلایه تشکیل شده است.اولین لایه تجهیزات و ابزار فیزیکی می‌باشد، در دومین لایه سامانه‌ها و سکوهای فناورانه که تشکیل، ذخیره و تبادل، تغییر داده‌ها و اطلاعات را ممکن می‌سازند، وجود دارند. لایه سوم مربوط به اطلاعات و محتوا است و درنهایت لایه چهارم عامل انسانی، به عنوان کاربران و بهره وران از این فضا حضور دارند.این لایه هابایکدیگر دارای تأثیر و تاثر متقابل هستند (اسلامی تنها، پارسانیا، نجف پورآقابیگلو، ۱۴۰۰: ۳۱۱). فضای مجازی، قلمرویی وسیع و بدون مرز است که باتوجه به ویژگی‌های منحصر به فرد برای کاربران خود امکانات، آزادی‌ها، فرصت‌ها، دلهره‌ها و آسیب‌هایی را به همراه دارد. همین امر از جمله دلایلی است که هر کشوری نسبت به کاهش آسیب‌ها و مشکلاتی که ممکن است فضای مجازی با خود به دنبال داشته باشد در عین توجه به مزایای آن اقدام به وضع قوانین و مقرراتی کند تا امنیت کاربران و حکومت خود را حفظ کند.

فقه دنیای بایدها و نبایدها است. در جهان مجازی با توجه به بهره‌گیری از ابزار متنوع و پیشرفته فناورانه به مراتب وقوع جرم و ارتکاب عمل خلاف شرع بیشتر و آسان‌تر از دنیای حقیقی و عالم خارج است بایدعلم فقه و فقها در ارائه احکام شرعی دقیق‌تر و حساس‌تر باشند تا مکلفین وظیفه خود را دانسته دچارحیرت و سرگردانی در این فضا نشوند. متأسفانه فقه فضای مجازی مورد تغافل و غفلت علما و پژوهشگران قرار گرفته است. تشریع احکام از سوی شارع مقدس برای تمحیض و خالص شدن مخلوقات و رسیدن به اوج و قله‌های رفیع انسانیت و آزادگی بوده است. در این مسیر علم فقه که اصطلاحاً علم به احکام شرعی فرعی از روی ادله تفصیلی (کتاب، سنت عقل، اجماع) است (علامه حلی ۱۳۷۲، ج۱: ۱). با استفاده از قواعد سازنده و بازدارنده خود (احکام وجودی یا عدمی) درابعاد مختلف زندگی فردی و اجتماعی انسان‌ها اعم از زمینه‌های دنیوی، اخروی، سیاسی، اقتصادی، فرهنگی، دینی و کنش گری‌های مدنی و اجتماعی هدف و غایتی جز تزکیه، اصلاح، تربیت فرد و جامعه دربر ندارد (فیض، ۱۳۹۱، ج۱: ۱۲۳). از جمله قواعد کاربردی فقهی قاعده حرمت اعانت بر اثم است که با استفاده از این قاعده می‌توان نسبت به مدیریت مطلوب‌تر فضای مجازی اقدام نمود. چه آن که نیازهای اساسی اشخاص به ویژه نسل جوان که عبارت است از سلامت، نیازهای عاطفی، امنیت و... (آیت اللهی، بانکی پورفرد، بداغی، ۱۳۹۶، ج۱: ۱۹) در فضای مجازی به مخاطره می‌افتد و بایستی مدیریت شود. نخستین کسی که اعانت بر اثم را در اثر خود هرچند به طور ضمنی بیان نموده است شیخ الطائفه شیخ طوسی صاحب کتاب خلاف و مبسوط بوده است. ایشان با استناد به اعانت براثم پرداخت زکات به فرد نیازمندی که آلوده به گناه و عصیان است را حرام می‌داند (شیخ طوسی، ۱۳۸۷ق، ج۱: ۲۵۱). نسبت به اعانت بر اثم تعاریف گوناگونی توسط فقها ارائه شده است. شیخ مرتضی انصاری در باب اعانت براثم آن را این گونه ترسیم کرده است: «شخصی مقدمات فعل غیر را ایجاد کند و در انجام این مقدمات دارای قصد باشد.» از این رو تهیه مقدمات عمل حرام دیگری بدون قصد را اعانت بر اثم نمی‌داند (شیخ انصاری، ۱۴۱۱ ق، ج۱: ۶۸). برخی نیز اعانت بر اثم را به این صورت تعریف نموده‌اند که «اعانت بر اثم یعنی کمک کردن به دیگری برای انجام محرمات. مانند اینکه فروشنده‌ای انگور را به قصد تهیه شراب به دیگری بفروشد» (مکارم شیرازی، ۱۴۲۷ق، ج۱: ۴۸۱). هرجایی که محل زیست جمع و اجتماعی باشد نیازمندو مستلزم وجود قانون و اجرای آن جهت عدم تضییع حقوق دیگران و برقراری نظم و جلوگیری از

هرج و مرج در آن محیط است. فضای مجازی به عنوان محل زیست بشر از این قاعده مستثنی نیست و این مسأله امری عقلانی و منطقی است. این مهم که فضای مجازی دارای فواید و نقشی غیر قابل انکار در زندگی انسان امروزی است پذیرفته شده و عقلانی می‌باشد. اما با وجود فواید و بهره‌مندی مطلوب از امکانات این فضا ممکن است سوء استفاده‌های متفاوتی در زمینه‌های مختلف توسط شیادان، ظالمین، مستکبران، سارقان و به طور کلی مجرمان و تبه کاران صورت گیرد که امنیت روانی جامعه را به مخاطره میاندازند. جامعه برای قوام وبقای خود نیازمند وجود عناصری است که استمرار آن را تضمین نمایند. یکی از بنیادی‌ترین نیازهای جامعه انسانی آرامش روانی به انضمام مقوله امنیت روانی اجتماع است. امروزه با ایجاد و پیشرفت روز افزون وسایل و فناوری‌های الکترونیکی و ظهور پدیده‌ای به نام «فضای مجازی» و استفاده نامطلوب از آن فراد و جامعه متحمل آسیب‌های روانی فراوانی شده‌اند. از این روباید این فضا تحت مدیریت و تدبیر اهل فن قرار گرفته تا آسیب‌ها و اثرات سوء آن به حد اقل ممکن برسد هرچند که با توجه به ویژگی‌هایی که فضای مجازی از آن برخوردار است ایجاد نظم و نظارت بر آن امری سخت و پیچیده است. در انجام این وظیفه، علم فقه و قواعد کاربردی آن می‌تواند یاری‌گر مسئولین ذی ربط باشد. از جمله این قواعد، قاعده حرمت اعانت بر اثم است که می‌تواند هم نقش تبیین‌کننده (پیشگیری) و هم نقش بازدارندگی قهری و سلبی (درمان) را ایفاء کند.

از نوآوری‌های پژوهش حاضر می‌توان به نقش پیشگیرانه و درمانگرایانه استعمال قاعده اعانت بر اثم بارویکرد تبیینی-تنبیهی اشاره نمود که مطابق این قاعده فقهی محاکم قضایی می‌توانند برای آن دسته از مواردی که تحت قاعده اعانت بر اثم قرار می‌گیرند به اقتضاء تأثیر آن‌ها بر امنیت روانی شهروندان یا جامعه و اثرگذاری اجتماعی برخی از گناهان در فضای مجازی جرم انگاری و مجازات متناسب را در نظر گیرند. به طور مثال یکی از مواردی که در فضای مجازی مشکلات روز افزونی را برای کاربران ایجاد کرده است، سرقت علمی و یا سرقت اطلاعات خصوصی اشخاص است و این امور موجب تشویش اذهان و نگرانی جامعه مؤلفان آثار علمی و آحاد جامعه از هر قشری شده است و سوء مدیریت‌ها و سخت بودن نظارت و مدیریت داده‌ها و قدرت یافتن انواع سخت‌افزارها و نرم‌افزارهای الکترونیکی، هک وسایل دیجیتالی وقفل شکن‌ها عاملی جهت تقویت سرقت‌های اطلاعاتی در همه زمینه‌ها می‌باشد.

(طارمی، ۱۳۸۷: ۳۵) نسبت به این مسأله احتمال وقوع اعانت بر اثم وجود دارد. از این جهت که مثلاً ممکن است «الف» در مسائل مربوط به فناوری‌های ارتباطی و دیجیتالی زبده و مجرب باشد و از این قابلیت خود سوء استفاده کرده و جهت کلاهبرداری شخص «ب» پیوند آلوده‌ای را در اختیار او قراردهد که با استفاده از آن اقدام به کلاهبرداری و یا سرقت اطلاعات خصوصی افراد کند و از این طریق به ارعاب، تهدید و اخاذی از آن‌ها بپردازد. در این جا شخص «الف» که ابزار کلاهبرداری را در اختیار شخص «ب» قرار داده است معین بر اثم خواهد بود.

پژوهشگران و نویسندگان به بررسی فقهی و حقوقی قاعده اعانت بر اثم در فضای مجازی پرداخته‌اند. در ادمه به برخی از آن‌ها اشاره می‌شود:

زراعت، نجفی، یزدیان، گلی (۱۳۹۹) درپژوهش خود باعنوان «مشروعیّت جرم انگاری عمل تولید، توزیع و انتشار بدافزارهادرفضای سایبر» ازجمله دلایل و مستندات شرعی مشروعیّت جرم تولید، توزیع و انتشار

بدافزارها را وجود قاعده اعانت براثم می‌دانند.

زند اقطاعی (۱۳۹۸) درمقاله‌ای باعنوان «بررسی فقهی و حقوقی اعانه براثم در فضای سایبر باراهبرد پیشگیری» وجوه تمایز و تفاوت معاونت درجرم در فضای سایبر را بستر وقوع جرم، سهولت وقوع جرایم در این فضا، شدت ضرر و کثرت و فراوانی بزه دیده می‌داند. اومعتقد است اعانت از امور تبعی است و قصد از آن به ذهن متبادر می‌شود و مفهوم قصد در معنای اعانت ظاهر است. او حرمت اضرار به غیر و مقدمه حرام را علاوه برکتاب از دلایل حرمت اعانت براثم می‌داند.

پیرمرادیان (۱۳۹۴) در پژوهشی تحت عنوان «حرمت اعانه بر اثم و اعانه به ظالم در رسانه‌های خبری ومطبوعات از دیدگاه فقه اسلامی و با تأکید براندیشه‌ی فقهی امام خمینی (ره)» عنوان می‌دارد اگر مخاطبان رسانه‌های جمعی و مطبوعات، رفتاری را در رادیو و تلویزیون بشنوند و یامشاهده کنند و مطلبی را در روزنامه‌ها بخوانند، که احتمال تقلید از رفتارهای نابهنجار و مجرمانه و گناه را در آن‌ها تقویت کند، در این صورت رسانه خبری معین بر اثم بوده ومرتکب حرام شده است.

از جمله تفاوت‌های پژوهش حاضر نسبت به مقالات مذکور توجه به دوجنبه پیشگیری و درمان مبتنی بر قاعده اعانت بر اثم در کنار یکدیگر است که متناسب با موارد مختلف می‌توان یکی از این دو روش را برگزید. همچنین می‌توان گفت محکمه این اختیار را دارد تا در حوزه مجازات معین بر اثم مستقل از مجازات یا عدم مجازات فاعل فعل حرام عمل کند.

۲ دلیل عقل مهم‌ترین مستند حرمت اعانت بر اثم

با توجه به تقسیم‌بندی‌ای که از ادراکات عقلی (به عقل عملی و و نظری) توسط فقها و فلاسفه انجام شده است و بین عقل نظری و عقل عملی تفاوت قایل شده‌اند، به نظر می‌رسد، عقل یکی از راه‌های استنباط احکام شرعی فرعی برای مجتهدین باشد به گونه‌ای که شیخ مفید (ره) عقل را طریق و راه معرفت حجیت آیات و روایات و اخبار دانسته است (شیخ مفید، ۱۴۱۳ ق، ج۱: ۲۸) و روایات هم موید حجیت عقل هستند و جایگاه وشانیت عقل را می‌توان از حدیث مشهوری که از امام کاظم وارد شده است دریافت. ایشان فرمودند خداوند دو حجت را در اختیار مردم قرار داد، حجتی ظاهری که پیامبران و معصومین علیهم السلام هستند و دیگری حجت باطنی که همانا عقل است (کلینی رازی، ۱۴۰۷ ق، ج۱: ۱۶) انجام منکر قبیح است. این قبح را عقل مستقلا درک می‌کند و به ترک آن عمل حکم می‌کند. بناء بر این امر به حرام و تحریک دیگری و فراهم ساختن مقدمات برای انجام فعل ناشایست توسط دیگری نیز توسط عقل مذمت شده و قبیح خواهد بود و این حکم عقل به قبح انجام عمل حرام و کمک و امدادرسانی برای وقوع آن در شرع مورد تأیید است اگر چه که به لحاظ شدت قبح و اعمال مجازات بین معان و معین تفاوت باشد. مستند این حکم روایتی است که در کتب معتبر فقهی ازجمله کافی مرحوم کلینی آمده است. از امام صادق علیه السلام روایت شده است که از سه نفر نزدامیر المؤمنین علی علیه السلام شکایت شد. یکی از آن‌ها مردی را نگه داشته بود و دیگری او را کشت و شخص ثالثی هم نظاره‌گر (دیدبان) بود. حضرت (علیه السلام) قضاوت نمود به این که بیننده (دیدبان) چشمانش کور گردد و کسی که ممسک و نگهدارنده بود در حبس بماند تازمانی که بمیرد و قاتل

به قتل برسد و قصاص شود (کلینی رازی، ۱۴۰۷ ق، ج ۷: ۲۸۸). به نظرامام خمینی اگر شخصی به سرقت سارقی کمکی کند صرف نظر از این که قصد وقوع فعل مجرمانه و ارتکاب عمل حرام را داشته یا نداشته باشد عقلا این کار مجرمانه دانسته شده و از منظر عقل قبیح است و قبح عقلی دارد. اگرچه باوجود قصد قطعاً و عقلا قبح بیشتری خواهد داشت (خمینی، ۱۳۶۸، ج۱: ۱۳۰) در واقع بنای عقلا بر مجازات معین، بر اساس درک حسن و قبح عقلی یک عمل است؛ به این معنا که هرگاه عقلا چیزی را مجرمانه بدانند به دلیل قبیح بودن آن است و به تعبیر علامه طباطبایی بنای عقلا مبتنی بر فطرت انسانی و ضرورت نظام اجتماعی بوده و مستند آن عقل است (طباطبایی، بی‌تا، ج۲: ۱۸۸-۲۰۵) نسبت به مسائلی که جنبه اجتماعی دارند عقل حکم می‌کند به این که برای حفظ نظام و عدم هرج و مرج باید از کارهایی که موجب هرج و مرج می‌شود پرهیز کرد. از این رو عقل مستقلاً حکم می‌کند به حرمت آن چه که موجب اختلال نظام عالم شود (موسوی قزوینی، ۱۴۲۳ ق، ج۵: ۳۰۱) اعانت بر اثم از قبیل کارهایی است که در صورت وقوع و فراگیرشدن و عدم برخورد با شایع شدن آن باعث هرج و مرج و نابسامانی و اختلال نظام می‌گردد. بر اساس این مقدمات عقل حکم می‌کند به حرمت اعانت بر اثم و حکم می‌کند به برخورد و مقابله با آن. البته عکس این قضیه را هم عقل حکم می‌کند؛ یعنی این که افراط در بحث اعانت بر اثم موجب هرج و مرج می‌شود بلکه ملاک صدق عرفی عمل است که مشمول اعانت بر اثم خواهد شد یا که خیر. چرا که در اعانت به اثم رابطه مستقیم شرط است. رابطه غیر مستقیم اعانت به اثم نیست (مطهری، ۱۳۸۸، ج۲۰: ۳۴۴) چون در غیر این صورت به طور مثال نباید با کسانی که عصیان می‌کنند و گناهی مرتکب می‌شوند تجارت و داد و ستد کرد تا از این طریق متنبه شوند و در غیر این صورت اعانت براثم محقق می‌شود و این افراط خیلی از کارها را تعطیل کرده و موجب عسر و حرج می‌گردد (مکارم شیرازی، ۱۴۲۴ ق، ج۱: ۵۸).

دلیل عقل مهم‌ترین مستند قاعده اعانت بر اثم است. از این رو عقل حکم می‌کند به قبیح بودن کمك به انجام فعلی که مبغوض خداوند خواهد بود (حسینی مراغی، ۱۴۱۷ ق، ج ۱: ۵۶۵).

۳ رویکرد پیشگیرانه و تربیتی مبتنی بر قاعده اعانت بر اثم

زمانی که بشر ابزاری را تولید می‌کند؛ چگونگی کار کردن با آن ابزار را به دیگران آموزش می‌دهد تا بتوانند از آن وسیله سالیان متمادی بهره ببرند. حال اگرفردی به توصیه‌ها درباب بهره‌مندی ازاین ابزارها توجهی نکند متضرر شده و روز به روز کارآیی و کارکرد آن وسایل و ابزارتنزل می‌یابد و نهایتاً از بین می‌روند. انسان که آفریده آفریدگاری حکیم است می‌بایست به دستورات صانع خویش عمل کند؛ در غیر این صورت روز به روز به تباهی و سقوط نزدیک می‌شود. این فرامین و احکام در قالب فقه برای مردم بازگو می‌شود. مفهوم فقه یک مفهوم بسیط (فراگیر و گسترده) است که همه ابعاد زندگانی فردی و اجتماعی انسان‌ها را فرا گرفته است. در بهره‌گیری و مدیریت ازفضای مجازی علم فقه و قواعد کاربردی آن می‌تواند یاری‌گر مسئولین ذی ربط باشد. از جمله این قواعد، قاعده حرمت اعانت بر اثم است که می‌تواند هم نقش تبیین‌کننده و پیشگیری‌کننده و هم نقش بازدارندگی قهری و سلبی و درمان را ایفاء کند. فضای تعاملی شبکه‌های مجازی شمشیری دولبه است که یک لبه آن فرصت و لبه دیگر آن تهدید است. این مسأله که یک نوجوان و یا جوان بتواند باگذر از مرزهای

جغرافیایی با افراد هم سن خود در نقاط مختلف از جهان واقعی تعامل پیداکند از این منظر که می‌تواند به معرفی باورها، اعتقادات، اندیشه‌های صحیح، فرهنگ و آداب و رسوم خود بپردازد و آن‌ها را بادیگران به اشتراک بگذارد، کارکرد مثبت فرهنگی و ارتباطی فضای مجازی خواهد بود. اما این تعامل با افراد دیگر بر اساس نوع نیازها دینی، اعتقادی و دنیوی اشخاص توسط آن‌ها ساماندهی می‌شود (خاکسار، عدلی پور، معمار، ۱۳۹۱: ۱۷۱). از این رو ممکن است با کاهش تعلقات مذهبی و اخلاقی در طیف جوانان و نوجوانان که از آسیب‌های فضای مجازی است (همان). این قشر حساس مرعوب زندگی مادی هم سنین خود در نقاط دیگر جهان واقعی شده و تأثیر منفی بر رفتار و کردار آن‌ها داشته باشد و دست به اعمال و کرداری بزنند که خلاف عقل و شرع باشد. چراکه در هرجایی که فردیت نباشد و جمعی در کنار هم قرار بگیرند احتمال وقوع اثم و یاری رساندن بر آن وجود دارد. بناء بر این حکمرانی و نظام اجتماعی باید هنجارها و ارزش‌های اعتقادی و اجتماعی خود را برای آحاد جامعه تبیین کرده و در اثر بخشی هویت ثابت افراد در فضای مجازی نهایت تلاش خود را کند در غیر این صورت اشخاص برای جبران ضعف‌هایشان و با عنایت به از دست دادن هویت اجتماعی خود دست به اقدامات نامعقول‌زده و به افرادی پناه می‌برند که منتظر فرصت برای سوء استفاده از چنین افراد آسیب دیده و آسیب‌پذیری هستند (خاکسار، عدلی پور، معمار، ۱۳۹۱: ۱۷۰) و این مهم در وهله اول برعهده خانواده است و پس از آن همت نهادهای اجتماعی را می‌طلبد.

دشمن به محض آن که اتفاقی در کشور ما واقع می‌شود سعی در سیاه نمایی و بزرگ نمایی می‌کند و اگر مشابه همان اتفاق نسبت به خود آن کشور یا کشورهای مشترک المنافعشان رخ دهد سکوت کرده و یا سعی در توجیه آن اتفاق می‌کنند و با نهایت توان خود در جهت ارعاب مسلمانان و تهاجمات فرهنگی و اقصادی و سیاسی و از همه مهم‌تر اعتقادی گام بر می‌دارند. از طرفی خداوند متعال در قرآن کریم حکم به عدم مرعوب شدن و عدم تسلط کافران بر مؤمنان داده است و تسلط کافران بر مؤمنان را نفی کرده است و می‌فرماید «وَلَنْ يَجْعَلَ اللَّهُ لِلْكَافِرِينَ عَلَى الْمُؤْمِنِينَ سَبِيلًا» (نساء/۱۴۱) «و خداوند هرگز کافران را بر مؤمنان تسلّطی نداده است».

البته مقصود از نفی جعل، نفی تشریعی است نه تکوینی، زیرا اگر نفی جعل تکوینی بود، می‌بایست در خارج هیچ گونه تسلّطی برای کافران تحقّق نمی‌یافت، حال آن که در برخی موارد سلطه کافران بر مؤمنان در عالم خارج وجود دارد (هاشمی رفسنجانی و دیگران، ۱۳۸۹، جلد ۲۲: ۳۶۹). دولت‌های اسلامی به خصوص جمهوری اسلامی ایران به عنوان تنها دولت مقتدر شیعی در جهان کنونی که مورد هجمه‌های شدید فرهنگی، اقتصادی و سیاسی از سوی مستکبران و دولت‌های مستبد قرار دارد بایستی نرم‌افزارها، سخت‌افزارها و تمامی امکانات مورد نیاز را جهت حمایت از تولید و تقویت سکوهای پیام رسان‌های داخلی به کار گیرد و در ضمن قراردادهای رسمی و الزامی نسبت به پیام رسان‌های جهانی که دفاتر آن‌ها در کشورهای خصمانه‌ای چون ایالات متحده آمریکا است تنظیم کرده و تعهدات لازم را در جهت حفظ منافع و امنیت ملی اخذ کند و هرجا حاکمیت، استقلال، باورها و ارزش‌های الهی جامعه در معرض تهاجم و خطر قرار گرفت با اقدامات به هنگام و دقیق به مقابله به مثل با آن بپردازند. در صورت اهمال و سستی مقامات مربوطه می‌توان بر اساس قواعد فقهی‌ای نظیر نفی سبیل و حرمت اعانت بر اثم مورد مؤاخذه واقع شوند.

علم فقه و به‌خصوص شاخه تربیتی آن رویکرد پیشگیرانه به مسائل داشته و آداب و شیوه تربیتی را در

اختیار جامعه قرار می‌دهند. مربی باید به متربی بیاموزد که در اجتماع با چه اشخاصی مجالست نماید تا به رشد برسد و از همنشینی باچه کسانی بپرهیزد و برحذر باشد تا به سعادت برسد. «الهی همنشین از همنشین رنگ می گیرد خوشا آنکه با تو همنشین است» (علامه حسن‌زاده آملی، ۱۳۷۲، ج۱: ۸۲) اجتماع امروزی فقط در عالم حقیقی نیست و در فضای مجازی گروه‌های مختلف و متعددی با اهداف گوناگونی گرد هم می‌آیند. آداب معاشرت، تشخیص حق و باطل، رعایت حقوق دیگران، کنترل غریزه جنسی و دقت نظر در صحبت با جنس مخالف و ... همه به تربیت فقهی و تأثیرپذیری شخص از احکام تکلیفی و پیروی از آن برمی گردد. انسان به ناچارجهت رفع حوائج و تحصیل امور باید با اصناف مردم معاشرت داشته باشد که این معاشرت موجبات تأثیر و تاثر متقابل می‌گردد. از این رو باید آداب معاشرت و حقوق دیگران را بداند و رعایت کند. علما علم اخلاق گفته‌اند که بایدباشش طیف مجالست نمود که عبارت‌اند از: علما، صلحا، کریمان، عقلا، فقرا و معمرین و از مجالست با چهارده دسته و گروه پرهیز کرد، نظیر ظالمان، بخیلان، فاسقان، حمقا و ... (علامه فشارکی، ۱۳۹۲، ج۱: ۱۰۱). متأسفانه پدیده‌ای که امروزه در بین نوجوانان و جوانان در فضای مجازی به وفور به چشم می‌خورد و منجربه بحران‌های هویتی و اجتماعی می‌شود، دوستی باجنس مخالف است. دوستی با جنس مخالف اکثرا هوس آلود بوده ودر قرآن کریم مورد مذمت و نهی قرار گرفته است و به کنترل قوای جنسی قبل از ازدواج تأکید شده است و از دوستی‌های پنهانی منع نموده است (متخذی اخدان) (مائده/۵) (آیت اللهی، بانکی پورفرد، بداغی و دیگران، ۱۳۹۴، ج۱: ۲۱). دوستی باجنس مخالف پیامدهای ناگواری از قبیل ضعف اراده، ایجاد اضطراب، افت تحصیلی، ناراحتی‌های روحی و روانی، کاهش اعتماد، افزایش ازدواج‌های ناپایدار (آیت اللهی، بانکی پور فرد، بداغی، ۱۳۹۴، ج۱: ۲۳) و وابستگی‌های شدید که در برخی از موارد در صورت ترک طرف مقابل منجر به اعمال قبیح و خطرناکی چون خودکشی می‌شود. برای جلوگیری از وقوع این پیامدهای ناگوار که آسیب جدی به یکی از مهم‌ترین ارکان اجتماع یعنی خانواده می‌زنند و درنهایت اثرات منفی آن به کل جامعه سرایت می‌کند تربیت فقهی باید نقش سازنده‌ای را ایفاء کند.

۴ رویکرد تنبیهی-درمانی مبتنی بر جرم‌انگاری اعانت بر اثم

هر جایی که محل زیست جمع و اجتماعی باشد نیازمند و مستلزم وجود قانون و اجرای آن جهت عدم تضییع حقوق دیگران و برقراری نظم و جلوگیری از هرج و مرج در آن محیط است و این مسأله امری عقلانی و منطقی است. فضای مجازی به عنوان محل زیست بشر از این قاعده مستثنی نیست. ایجاد هرگونه محدودیتی ناخودآگاه ذهن انسان را به سمت وجود عامل پیشگیرانه و بازدارنده جهت شکل‌گیری آن محدودیت و ضمانت اجرای آن می‌برد. به نظر می‌رسدعامل پیشگیرانه جهت لزوم ایجاد محدودیت در فضای مجازی دین و اخلاق برگرفته از احکام شرع مقدس اسلام است که با ارائه بایدها و نبایدها وظایف مکلفین را روشن می‌کند و محدودیت‌های برگرفته از مستندات نقلی و عقلی را تبیین می‌کند و نهایتاً عامل قانون و مواد قانونی ابزار ضمانتی اجرای محدودیت‌ها را تضمین خواهد نمود. بسیاری از هنجارها در کشور ما منطبق با حکم شارع مقدس و آموزه‌های اسلامی است و در دین مبین اسلام امر و نهی (ایجاد محدودیت) برای سعادت دنیوی و اخروی انسان‌ها وارد شده است.

در اجتماع، از مهم‌ترین اجزاء در اجتماعی شدن افراد جامعه، رعایت و پیروی از هنجارها، ارزش‌ها و قوانین می‌باشد. رعایت تقوا الهی و عدم ارتکاب آن چه که توسط شارع مقدس و قانون‌گذار نهی شده است به طور مکرر در آیات و روایات وارد شده است. از جمله اموری که شارع از آن‌ها نهی کرده اعانت بر اثم می‌باشد که در سوره مبارکه مائده آیه دو به آن اشاره شده است. راحتی در دسترسی به امکانات فضای مجازی و تنوع در ارائه سرویس‌ها و خدمات در بستر آن موجب ورود بسیاری از افراد به فضای مجازی بلکه اعتیاد بیش از حد آن‌ها خصوصاً نسل جوان به استفاده از فضای مجازی می‌شود (سیاح طاهری و دیگران، ۱۳۹۶، ج۱: ۸۲) و این تسهیل و تنوع مشکلاتی را ایجاد می‌کند که نیازمند تدبیر مسئولین و نهادهای مربوطه برای کاهش آسیب‌های فضای مجازی است. یکی از شایع‌ترین آسیب‌ها و مخاطرات این فضا انتشار اخبار کذب به صورت آگاهانه توسط معاندین و ظالمان در عصر حاضر جهت بهره وری سیاسی، اقتصادی و فرهنگی خویش است. حال اگر رسانه‌های خبری و افراد مشهور که موضع‌گیری آن‌ها در معرض دید عموم قراردارد و به طورکلی کنش تمامی کاربران فضای مجازی متأثر از رفتار تقلیدی و کورکورانه باشد و بدون فحص و بررسی صحت و کذب اخبار، به باز نشر مطالب کذب رسانه‌های معاند اقدام کنند، کنش آن‌ها مشمول اعانت بر اثم خواهد بود (پیرمرادیان، ۱۳۹۴: ۶۸).

قتل نفس و کشتن انسان بی‌گناه از جمله گناهان کبیره و معظمی است که خداوند نسبت به ارتکاب آن چنین می‌فرماید: «مَنْ قَتَلَ نَفْسًا بِغَيرِ نَفْسٍ أوفَسادٍ فِي الأَرضِ فَكانَّما قَتَلَ النَّاسَ جميعاً» (مائده/۳۲).

وقتی انسانی به ناحق کشته شود گویی همه انسان‌ها کشته شده‌اند. از این رو قتل نفس به غیر حق در شرع مقدس حرام شده است و غایت دلالت مفهومی قید مذکور در آیه آن است که شخصی که مفسد فی الارض بوده است خونش محترم نبوده و مشمول حکم آیه نمی‌شود (هاشمی شاهرودی، ۱۳۷۸، ج۱: ۲۴۹). امروزه بارشد فزاینده استفاده از فضای مجازی و پیشرفت علوم و فنون و مهارت انسان امروزی در به کارگیری صنایع و ابزارهای مرتبط با فناوری‌های ارتباطات و سخت‌افزارها و نرم‌افزارهای مجازی امکان وقوع قتل در فضای مجازی میسر شده است به این شکل که شخصی با انجام عملیات و اقداماتی زمینه موت دیگری را فراهم کند یا خود عامل فوت دیگری شود (ایزدی فرد، حسین نژاد، ۱۳۹۵: ۱۰).

بناء بر این هم امکان وقوع اثمی از نوع قتل نفس در فضای مجازی ممکن است و هم احتمال ایجاد مقدمات آن و وقوع اعانت بر اثم در آن می‌رود.

به طور مثال شرکت دانش‌بنیانی اقدام به تولید کوادکوپتر (یکی از انواع پهبادها و ریزپرنده‌ها) در زمینه اطفاء حریق شرکت‌ها و منازل مسکونی نماید و یا جهت شناسایی خطرات در محیط‌های حساس ساخته شود و کسانی که به لحاظ تجاری و یا نظامی از تولید این ابزار ناراحت و عصبانی هستند و مقاصد شوم خود را در خطر می‌بینند با استفاده از افراد متبحر و ماهر و بانفوذ در نیروهای خلق‌کننده آن ریزپرنده اقدام به خرابکاری و در دست گرفتن مدیریت آن کرده و باتعبیه بمب‌های کوچک و وسایل احتراق‌زا موجب آتش‌سوزی در محل شده و از این طریق جان آدم‌های بی‌گناه را می‌گیرند. این افراد قطعاً آثم هستند. نمونه دیگر از قتل نفس در فضای مجازی که مرتبط با اعانت بر اثم در فضای مجازی می‌باشد آن است که مثلاً شرکت تولیدکننده بازی‌های رایانه‌ای اقدام به تولید بازی‌ای کند که در یکی از مراحل آن تشویق به خودکشی افراد و کاربران شود و یا از آنها خواسته شود که برای گذر از مرحله‌ای از بازی به مرحله دیگر خودشان یا شخص دیگری را به

قتل برسانند. اقدام این شرکت در تحریک و تشویق کاربران بر قتل نفس علاوه بر اثم قطعاً از مصادیق اعانت بر اثم خواهد بود.

این موارد فقط گوشه کوچکی از مشکلاتی است که فضای مجازی باوجود مزایایی که در عصر حاضر برخوردار است به‌وجود آورده است. جامعه انسانی (اسلامی) از بازوی قهری خود به‌نام قوانین (جزایی) صرفاً برای اینکه مردم از ترس عقاب به دستورات و فرمان‌ها جامه عمل بپوشانند اکتفاء نمی‌کند بلکه غایت و هدف نهایی آن است که انسان به عنوان اشرف مخلوقات به درجه‌ای از خودمراقبتی رسیده تا دارای فضائل و عادات نفسانی نیکو که مدنظر شارع بوده است برسد (علامه طباطبایی، ۱۳۷۴، ج۶: ۵۲۳). قواعد فقهی که در چارچوب بایدها و نبایدها هستند و علاوه بر نقش بازدارندگی بعضاً نقش سازندگی نیز دارند می‌توانند در موارد ضروری با رویکرد قهری نسبت به تنبیه که یکی از روش‌های تربیتی و خاص است در مراحل بالاتر از نافرمانی‌های مدنی و تربیتی استعمال شوند و بر کاهش آسیب‌ها و مخاطرات در فضای حقیقی و مجازی مؤثر باشند. در هر ثانیه میلیاردها محتوا و بیشتردر فضای مجازی تولید، منتشر و باز نشر داده می‌شود. در کشور ما تولید برخی محتواها جرم‌انگاری شده است و البته در برخی مواردخلأ قانونی وجود دارد. به‌عنوان نمونه قمار بازی با هر وسیله‌ای ممنوع است و طرح دعوا در این زمینه مسموع نیست (قانون مدنی ماده ۶۵۴) و مطابق با قانون جرایم رایانه‌ای (ماده۱۴) انتشار، توزیع و معامله محتوا مستهجن علیه عفت و اخلاق عمومی جرم‌انگاری شده است. همچنین جرایم علیه امنیت و آسایش عمومی جامعه در بستر فضای مجازی به‌عنوان جرمی مستقل دارای مجازات‌های معین است. اما علاوه بر این نمونه‌ها و مواردی که مستقلاً و مستقیماً دارای عنوان مجرمانه هستند و منجر به تخلفات شرعی و قانونی می‌شوند ممکن است در مواردی به‌صورت غیرمستقیم باشد. مانند منطوق ماده ۱۵ قانون جرایم رایانه‌ای که اشعار می‌دارد تحریک، ترغیب، تطمیع و دعوت افراد به فحشاء و ارتکاب جرایم منافی عفت یا انحرافات جنسی واعتیاد به مواد مخدر و خودکشی و اعمال خشونت‌آمیز جرم است و حسب مورد مجازات‌هایی را تعیین کرده است. از این رو ممکن است از طریق تولید بازی‌ها، سایت‌ها، تبلیغات ویدیویی و غیره به‌صورت غیرمستقیم و یا حتی بدون این که هدف اصلی از آنها تولید محتوای مخرب باشد مقدمه‌ای برای انجام فعل حرام، تسهیل و ارتکاب عمل نامشروع گردد.

باتوجه به این که فضای مجازی قایل به زمان و مکان نمی‌باشد جرایم سازمان یافته فراوانی در این فضا در حال گسترش است و درعین حال تولید محتوا و برنامه‌ها در این فضا بی‌شمار است و دقت نظر، تخصص و تعهد نهادهای تجویزکننده ونظارتی را در پیش‌بینی، پیشگیری، برخورد با نابهنجاری‌ها و ساماندهی فضای مجازی می‌طلبد.

۵ نتیجه‌گیری

بر اساس آن چه که عنوان شد، می‌توان نتیجه گرفت:

مشکلات حقوقی نظیر عدم رعایت حق صاحب اثر، حق تألیف، کلاهبرداری، سرقت، ارعاب و تهدید انتشار مسائل خصوصی و ... باعث می‌شود تا کاربران با احتیاط بیشتری پا در عرصه فضای مجازی گذاشته و سعی در رعایت حدود الهی و چارچوب‌های عقلایی و منطقی کنند تا کمتر دچار تنش و آسیب‌های بعضا غیر قابل

جبران گردند.

از طرفی دولت‌ها باید مطابق عقل و شرع قوانین محکم و قابل اجرایی را به اقتضای مقتضیات زمان حاضر نسبت به فضای مجازی وضع نموده و بر حسن اجرای آن قوانین نظارت مستمری داشته باشند. بناء بر این برای جلوگیری از سوء استفاده نسبت به قابلیت‌های موجود در فضای مجازی، عدم تضییع حقوق دیگران، برقراری نظم و امنیت اجتماعی وجغرافیایی، حفظ استقلال و قدرت حکومت اسلامی در برابر دشمنان و بدخواهان واز همه مهم‌تر عدم فراموشی نسبت به قادر متعال؛ بایستی محدودیت‌های دقیق و قابل اجرایی ایجاد نمود که منطبق بر عقل و شرع باشند و در این زمینه علم فقه و قواعد استخراج شده از آن نظیر قاعده لاضرر، قاعده اعانت بر اثم و قاعده نفی سبیل که مبتنی بر آیات، روایات و دستورات شارع مقدس هستند کمک حال قانون‌گذار است. البته باید به‌درستی شناخته و تبیین گردند تا به‌نحو شایسته‌ای از هرکدام از این قواعد و سایر قواعد کاربردی در علم فقه بهره‌مندی جامع و کاملی برده شود.

برای ساماندهی فضای مجازی و کاهش جرایم سایبری:

۱- ابتداء و در بادی امر بارویکرد تربیتی نهادهای مختلف از جمله خانواده و نهادهای متولی فرهنگی با شناخت نیازهای جامعه امروزی و شناخت واقعیت‌های فضای مجازی به کاهش آسیب‌ها و تنش‌های نشأت گرفته از فضای مجازی کمک کنند.

۲- تنبیه یکی از ابزارهای تربیتی است. این شیوه بایستی با دقت و با هدف پیشگیری از اشاعه اعمال مجرمانه و اثربخشی و تنبه افراد صورت بگیرد تا امنیت روانی جامعه در معرض خطر قرار نگیرد.

بناء بر این پیشنهاد می‌شود که قوه مقننه با ارائه قوانینی متناسب با ویژگی‌های دنیا مجازی وظایف نهادهای ذی‌ربط مرتبط با این حوزه و کاربران را در جهت بهره‌برداری مطلوب از این فضا تعیین وتسهیل کرده و جرایم سایبری را به حداقل برساند و محاکم قضایی نیز با توجه به حرمت اعانت بر اثم در شرع می‌توانند نسبت به آن دسته از گناهانی که جنبه اجتماعی داشته و با امنیت روانی جامعه در ارتباط هستند از جنبه تعزیری رویکرد جرم‌انگاری و مجازات را در نظر بگیرند.

مراجع

[۱] قرآن کریم

[۲] قانون جرایم رایانه‌ای

[۳] قانون مدنی

[۴] اسلامی تنها، علی اصغر، آقابیگلو، عزیز، پارسانیا، حمید (۱۴۰۰). مدینه فاضله مجازی چارچوب نظری حکمرانی فضای مجازی جمهوری اسلامی، دو فصلنامه علمی دین و ارتباطات، سال بیست و هشتم، ش اول، بهار و تابستان، صص ۳۰۵-۳۳۰.

[۵] انصاری، شیخ مرتضی، (۱۴۱۱ق). المکاسب، چاپ اول، قم: انتشارات دارالذخائر.

[۶] آیت‌اللهی، زهرا، بانکی‌پورفرد، امیرحسین، بداغی، فاطمه، و دیگران، (۱۳۹۴). دانش خانواده و جمعیت، قم، نهاد نمایندگی مقام معظم رهبری در دانشگاه‌ها.

[۷] ایزدی‌فرد، علی‌اکبر، حسین‌نژاد، سید مجتبی، (۱۳۹۵). بررسی فقهی قتل در فضای مجازی، مطالعات فقه و حقوق اسلامی، سال هشتم، ش۱۴، بهار و تابستان، صص ۷-۳۴.

[۸] پیرمرادیان، سیدمحمدرضا، (۱۳۹۴). «حرمت اعانه بر اثم و اعانه به ظالم در رسانه‌های خبری ومطبوعات از دیدگاه فقه اسلامی و با تأکید براندیشه‌ی فقهی امام خمینی (ره)»، سپهرسیاست، ش ۵، پاییز، صص ۶۱-۷۵.

[۹] حسن‌زاده آملی، حسن، (۱۳۷۲). الهی نامه، تهران، مرکز نشر فرهنگی رجاء، چاپ چهارم.

[۱۰] حسینی مراغه‌ای، سید میرعبدالفتاح، (۱۴۱۷ ق). العناوین الفقهیة، چاپ دوم، قم، مؤسسة النشر الإسلامی التابعة لجماعة المدرسین.

[۱۱] حلی، حسن بن یوسف بن المطهر، (۱۳۷۲). تذکرة الفقها، چاپ اول، قم، مؤسسة آل البیت علیهم السلام لاحیاء التراث.

[۱۲] خاکسار، فائزه، عدلی‌پور، صمد، معمار، ثریا (۱۳۹۱). شبکه‌های اجتماعی مجازی و بحران هویت (باتأکید بربحران هویتی ایران)، فصلنامه علمی پژوهشی مطالعات و تحقیقات اجتماعی در ایران، دوره اول، ش ۴، زمستان، صص ۱۷۶-۱۵۵.

[۱۳] خمینی، سیدروح الله الموسوی، (۱۳۶۸). المکاسب المحرمة، چاپ سوم، قم، مؤسسه اسماعیلیان.

[۱۴] زراعت، عباس، گلی، سلمان، نجفی حسین، یزدیان جعفر، (۱۳۹۹). «مشروعیّت جرم‌انگاری عمل تولید، توزیع و انتشار بدافزارها در فضای سایبر»، مطالعات فقه و حقوق اسلامی، ش۲۳، پاییز و زمستان، صص ۴۱۵-۴۳۸.

[۱۵] زنداقطاعی، فاطمه، (۱۳۹۸). «بررسی فقهی و حقوقی اعانه بر اثم در فضای سایبر با راهبرد پیشگیری»، دوفصلنامه تخصصی مطالعات فقهی، سال دوم، ش دوم، بهار و تابستان، صص ۳۹-۶۱.

[۱۶] سیاح طاهری، محمد حسین و دیگران، (۱۳۹۶). حقیقت مجازی (درباره فضای مجازی چه بدانیم و چه بگوییم؟)، تهران، مرکز ملی فضای مجازی.

[۱۷] شیخ مفید، محمدبن محمد بن نعمان بن حارثی مذحجی عکبری، (۱۴۱۳ق). التذکرة باصول الفقه، چاپ اول، قم، المؤتمر الاعالمی لالفیة الشیخ المفید.

[۱۸] طارمی، محمد حسین، (۱۳۸۷). فضای سایبر، آسیب‌ها و مخاطرات، ره‌آورد نور، ش۲۲ بهار، صص ۳۲-۳۹.

[۱۹] طباطبایی، محمد حسین، (۱۳۷۴). ترجمه تفسیر المیزان، چاپ پنجم، قم، دفتر انتشارات اسلامی.

[۲۰] طباطبایی، محمدحسین، (بی تا)، حاشیة الکفایة، قم، بنیاد علمی و فکری علامه طباطبایی.

[۲۱] طوسی، محمد بن حسن، (۱۳۸۷ق). المبسوط فی فقه الامامیة، تهران، المکتبة المرتضویة.

[۲۲] فشارکی، محمد حسین، (۱۳۹۲). آداب الشریعة (دستورات زندگی)، قم، انتشارات ارم، چاپ هفتم.

[۲۳] فیض، علی‌رضا، (۱۳۹۱). مبادی فقه و اصول، تهران، مؤسسه انتشارات دانشگاه تهران، چاپ بیست و دوم.

[۲۴] کلینی رازی، ابی جعفر محمد بن یعقوب، (۱۴۰۷ق). (اصول) الکافی ط اسلامیه، چاپ چهارم، تهران، دار الکتب الاسلامیه.

[۲۵] مطهری، مرتضی، (۱۳۸۸). مجموعه آثار ط صدرا، تهران، صدرا.

[۲۶] مکارم شیرازی، ناصر، (۱۴۲۴ق). کتاب النکاح، چاپ اول، قم، مدرسة الامام علی بن ابی طالب(ع).

[۲۷] مکارم شیرازی، ناصر، (۱۴۲۷ق). دائرة المعارف فقه مقارن، چاپ اول، قم، مدرسة الامام علی بن ابی طالب(ع).

[۲۸] موسوی قزوینی، سیدعلی، (۱۴۲۳ق). تعلیقة علی المعالم الاصول، چاپ اول، تهران، مؤسسه نشر اسلامی.

[۲۹] هاشمی رفسنجانی، اکبر و دیگران، (۱۳۸۹). فرهنگ قرآن، مرکز فرهنگ و معارف قرآن، مؤسسه بوستان کتاب.

[۳۰] هاشمی شاهرودی، سید محمود، (۱۳۷۸). بایسته‌های فقه جزا، تهران، نشر میزان.

بررسی امکان جرم‌انگاری جرایم مرتبط با اعانت بر اثم در فضای مجازی

محسن نادری[۱]، علی‌اکبر ایزدی فرد[۲]، محمدمهدی زارعی[۳]

[۱] دانشجوی کارشناسی ارشد فقه و مبانی حقوق اسلامی، دانشگاه مازندران
mnnnnarsenal9085@gmail.com
[۲] عضو هیئت علمی دانشگاه و استاد فقه و مبانی حقوق اسلامی، دانشگاه مازندران
izadifard@umz.ac.ir
[۳] استادیار و عضو هیئت علمی گروه فقه و مبانی حقوق اسلامی دانشگاه مازندران
m.zarei@umz.ac.ir

چکیده

قوانین جزایی جامعه ایران به‌لحاظ محتوایی برگرفته از فقه و حقوق اسلامی است. برای برخی از جرایم و گناهان در فقه و حقوق اسلامی توسط شارع مجازات معینی تعیین شده است که باید عیناً همان حکم توسط محکمه اجرا شود. در مقابل نسبت به برخی از موارد شارع مجازات معینی را تعیین نکرده است. یکی از این موارد اعانت بر اثم است. اعانت بر اثم حرام است و هر آنچه که حرام بوده و قابلیت مجازات دنیوی را داشته باشد محکمه می‌تواند مجازات تعزیری را برای آن در نظر بگیرد. پژوهش حاضر با روش توصیفی-تحلیلی و مراجعه به کتب فقهی و آراءفقها، همراه با توجیه، تبیین و استدلال و استنتاج است. مستنداتی برای حرمت اعانت بر اثم توسط فقها مطرح شده است. بررسی این مستندات و تعمیم آن نسبت به فضای مجازی این امکان که بتوان جرایم مرتبط با اعانت بر اثم را در فضای سایبری جرم‌انگاری کرد را فراهم می کند. خلاصه این که با استدلال و تبیین این مستندات حرمت اعانت بر اثم اعم از فضای حقیقی و فضای مجازی اثبات می شود و با توجه به حکم حرمت محاکم قضایی می‌توانند از جنبه تعزیری مجازات متناسبی را برای موارد مختلف اعمال کنند.

کلمات کلیدی: اعانت بر اثم، مستندات، فضای مجازی، فضای حقیقی، امکان مجازات.

۱ مقدمه

معنایی که برای اعانت در لغت وضع کرده‌اند عبارت از یاری کردن غیر است (ابن منظور، ۱۴۱۴ق، ج۱۳: ۲۹۸) به یاری‌دهنده «مُعین»، به یاری‌شونده «مُعان» و امری که بر آن یاری می‌شود، «مُعان علیه» می‌گویند (هاشمی شاهرودی و دیگران، ۱۳۷۴، ج ۱ :۵۹۰). در فقه اسلامي درتعریف معاونت و اعانت تعاریف گوناگون و متفاوتي وجود دارد. ازجمله شیخ انصاری اعتبار قصد را در تحقق عنوان اعانت شرط می‌داند و معتقد است

که اعانت در صورت وجود قصد مترتب بر انجام دادن و اعمال برخی از مقدمات کار شخص دیگر است (شیخ انصاری، ۱۴۱۱ق، ج۱: ۶۸).

سید محمد بجنوردی درکتاب قواعد فقهیه به‌نقل از پدر خود میرزا حسن بجنوردی بیان نموده که اعانت در لغت به معنای مساعدت است و معین کسی است که فردی را در انجام کاری یاری می‌دهد. بنابراین مقصود از اعانت بر اثم یاری کردن بر گناه است (موسوی بجنوردی، ۱۳۷۹، ج۲: ۲۲۷) از این رو اعانت عبارت است از انجام برخی از مقدمات کار معان (یاری‌شونده) توسط معین (یاری‌کننده) به‌صورت مطلق خواه با قصد تحقق اثم در عالم واقع باشد و نتیجه محقق شود و خواه قصد و نتیجه حاصل نشود که شیخ انصاری در مکاسب این قول را قول اکثر فقها دانسته و به آنها نسبت داده است (همان).

فضای مجازی (cyberspace) نخستین بار توسط ویلیام گیبسون نویسنده‌ی اهل کانادا-ایالات متحده آمریکا و در یکی از داستان‌های کوتاهی که نگاشته به‌کار برده شد (دهه ۱۹۸۰ میلادی). از نظر گیبسون فضای مجازی فضایی تخیلی است که از اتصال رایانه‌ها پدید آمده است، که تمامی انسان‌ها و منابع اطلاعاتی را به‌هم متصل کرده است (امام جمعه، ۱۳۸۲: ۲۵). درتعریف فضای مجازی، تعریف رسمی کاملاً دقیق و موافقی وجود ندارد. اما در تعریف آن گفته شده است: «فضای مجازی یا فضای سایبر، مفهومی برای توصیف فناوری دیجیتال به‌هم پیوسته گسترده‌است». نمی‌توان فضای مجازی را مترادف با اینترنت دانست، اما اینترنت ابزار ورود به فضای مجازی است (سیاح طاهری و دیگران، ۱۳۹۶، ج۱: ۳۰). اشخاص می‌توانند با استفاده از این فضا تعامل و تبادل ایده، اشتراک‌گذاری اطلاعات، انجام کار، بازی کردن، فعالیت‌های اجتماعی، هنری، سیاسی و غیره را انجام دهند. این فضا از چهارلایه تشکیل شده است: اولین لایه تجهیزات و ابزار فیزیکی می‌باشد، در دومین لایه سامانه‌ها و سکوهای (پلتفرم‌ها) فناورانه به‌عنوان زیرساخت‌ها و سخت‌افزارهایی که تشکیل، ذخیره و تبادل، تغییر داده‌ها و اطلاعات را ممکن می‌سازد، وجود دارد. لایه سوم مربوط به اطلاعات و محتوا است و در نهایت لایه چهارم عامل انسانی، به‌عنوان کاربران و بهره‌وران از این فضا حضور دارند و این لایه‌ها با یکدیگر دارای تأثیر و تأثر متقابل هستند (اسلامی تنها، پارسانیا، نجف پورآقابیگلو، ۱۴۰۰: ۳۱۱). به هر حال فضای مجازی با هر تعبیر و هر تعریفی، قلمرویی وسیع و بدون مرز است که با توجه به ویژگی‌های خود برای کاربران خود امکانات، آزادی‌ها، فرصت‌ها، دلهره‌ها و آسیب‌هایی را به‌همراه دارد. همین امر از جمله دلایلی است که هر کشوری نسبت به کاهش آسیب‌ها و مشکلاتی که ممکن است فضای مجازی با خود به دنبال داشته باشد در عین توجه به مزایای آن اقدام به وضع قوانین و مقرراتی کند تا امنیت کاربران و حکومت خود را حفظ کند.

امروزه با ورود و گسترش فضای مجازی، فعالیت و زیست بشری محدود در فضای حقیقی نیست و اشخاص حقیقی و حقوقی ساعات زیادی از شبانه‌روز را در فضای سایبری و مجازی سپری می‌کنند. تسهیل فعالیت‌های مختلف در فضای مجازی امکان وقوع جرایم مختلف و متفاوتی را فراهم می‌کند. درکشور ما تولید برخی محتواها جرم‌انگاری شده است و البته در برخی موارد دارای خلأ قانونی است. به عنوان نمونه قماربازی باهر وسیله‌ای ممنوع است و طرح دعوا در این زمینه مسموع نخواهد بود (قانون مدنی ماده ۶۵۴) و مطابق با قانون جرایم رایانه‌ای (ماده۱۴) انتشار، توزیع و معامله محتوا مستهجن علیه عفت و اخلاق عمومی جرم‌انگاری شده است. همچنین جرایم علیه امنیت و آسایش عمومی جامعه در بستر فضای مجازی به عنوان

جرمی مستقل دارای مجازات‌های معین می‌باشد. اما علاوه بر این نمونه‌ها و مواردی که مستقلاً و مستقیماً دارای عنوان مجرمانه هستند و منجر به تخلفات شرعی و قانونی می‌شوند ممکن است در مواردی به‌صورت غیرمستقیم باشد. مانند منطوق ماده ۱۵ قانون جرایم رایانه‌ای که اشعار می‌دارد تحریک، ترغیب، تطمیع و دعوت افراد به فحشا و ارتکاب جرایم منافی عفت یا انحرافات جنسی و اعتیاد به مواد مخدر و خودکشی و اعمال خشونت‌آمیز جرم است و حسب مورد مجازات‌هایی را تعیین کرده است. از این رو ممکن است از طریق تولید بازی‌ها، سایت‌ها، تبلیغات ویدیویی و غیره به‌صورت غیرمستقیم و یا حتی بدون اینکه هدف اصلی از آنها تولید محتوای مخرب باشد مقدمه‌ای برای انجام فعل حرام، تسهیل و ارتکاب عمل نامشروع گردد. یکی از مواردی که احتمال وقوع آن در فضای مجازی وجود دارد اعانت بر اثم است مانند این که شخص یا شرکت تولیدکننده برنامه و بازی‌ای در فضای مجازی بازی یا برنامه‌ای را تولید می‌کند، حال می‌تواند قابلیت چت و صحبت کردن افراد را تعبیه کند و در صورت تعبیه می‌تواند تنظیمات نظرات (کامنت ها) و گفت‌وگوها (چت‌ها) را به‌گونه‌ای تنظیم کند که متن، تصاویر و فیلم های خلاف شرع و اخلاق را که قبیح و مستهجن است حذف کند، در غیر این صورت با توجه به وظیفه خاصی که جهت مدیریت آن بستر داشته است ترک فعل او در صورت علم و التفات می‌تواند از مصادیق اعانت بر اثم باشد و قابلیت پیگیری جزایی و حقوقی را حسب موارد مختلف داشته باشد.

برای اثبات حرمت اعانت بر اثم در فضای مجازی باید مستندات متقنی برای آن ارائه شود که اعم از فضای حقیقی و مجازی باشد تا بتوان از این مستندات به‌عنوان مدارک و دلایل احتمال وقوع اعانت بر اثم در فضای مجازی استفاده نمود. از جمله مستنداتی که فقها و پژوهشگران برای قاعده اعانت بر اثم به آنها متمسک شده اند عبارتند از: کتاب (قرآن کریم)، روایات، دلیل عقل، قاعده لاضرر، که در ادامه بررسی اجمالی نسبت به هر کدام صورت گرفته و ثابت می‌شود که امکان اعانت بر اثم در فضای مجازی وجود دارد و بر اساس حرمت اعانت بر اثم مطابق این قاعده فقهی محاکم قضایی می‌توانند مجازات متناسبی را در نظر بگیرند.

زراعت، نجفی، یزدیان، گلی (۱۳۹۹) در پژوهش خود باعنوان «مشروعیّت جرم‌انگاری عمل تولید، توزیع و انتشار بدافزارها در فضای سایبر» ازجمله دلایل و مستندات شرعی مشروعیّت جرم تولید، توزیع و انتشار بدافزارها را وجود قاعده اعانت بر اثم می‌دانند.

زند اقطاعی (۱۳۹۸) درمقاله‌ای باعنوان «بررسی فقهی و حقوقی اعانه بر اثم در فضای سایبر با راهبرد پیشگیری» وجوه تمایز و تفاوت معاونت درجرم در فضای سایبر را بستر وقوع جرم، سهولت وقوع جرایم در این فضا، شدت ضرر و کثرت و فراوانی بزه‌دیده می‌داند.او معتقد است اعانت از امور تبعی است و قصد از آن به ذهن متبادر می‌شود و مفهوم قصد در معنای اعانت ظاهر است. او حرمت اضرار به غیر و مقدمه حرام را علاوه بر کتاب از دلایل حرمت اعانت بر اثم می‌داند.

پیرمرادیان (۱۳۹۴) در پژوهشی تحت عنوان «حرمت اعانه بر اثم و اعانه به ظالم در رسانه‌های خبری ومطبوعات از دیدگاه فقه اسلامی و با تأکید بر اندیشه‌ی فقهی امام خمینی (ره)» عنوان می‌دارد اگر مخاطبان رسانه‌های جمعی و مطبوعات، رفتاری را در رادیو و تلویزیون بشنوند و یا مشاهده کنند و مطلبی را در روزنامه‌ها بخوانند، که احتمال تقلید از رفتارهای نابهنجار و مجرمانه و گناه را در آنها تقویت کند، در این صورت رسانه خبری معین بر اثم بوده و مرتکب حرام شده است. ممکن است این شبهه و سؤال مطرح شود که مستندات

قاعده اعانت بر اثم مربوط به فضای حقیقی بوده و قابل استناد در فضای مجازی نباشد. پژوهش حاضر با بررسی اجمالی این مستندات این شبهه را رد کرده و مستندات مذکور را اعم از فضای حقیقی و فضای سایبر می‌داند.

۲ بررسی مستندات قاعده اعانت بر اثم در فضای مجازی

۱.۲ کتاب

فقها حرمت اعانت بر اثم را مستند بر دلایلی می‌دانند. از جمله آنها تمسک به آیات نورانی کلام الله مجید است. مشهورترین آیه‌ای که برای حرمت اعانت بر اثم به آن استناد شده است، آیه ۲ سوره مبارکه مائده است که به آیه تعاون معروف است: «وَتَعَاوَنُوا عَلَى الْبِرِّ وَالتَّقْوَى وَلَا تَعَاوَنُوا عَلَى الْإِثْمِ وَالْعُدْوَانِ» «و در نیکوکاری و پرهیزگاری با یکدیگر همکاری کنید، و در گناه و تعدّی دستیار هم نشوید».

از منظر علامه طباطبایی، قسمت اخیر از آیه ۲ سوره مبارکه مائده بیانگر پایه و اساس سنت اسلامی؛ برگرفته از دستور خداوند تبارک و تعالی است (طباطبایی، ۱۳۷۴، ج۵: ۲۶۶). همان‌طور که از معنای آیه بر می‌آید؛ آیه مذکور یاری دادن یکدیگر بر گناه ، ظلم و تجاوز را نهی نموده است. در روایتی علی علیه السلام می‌فرماید: «لا تعن قویا علی الضعیف» هیچ قدرتمندی را بر علیه ضعیفی یاری مکن (تمیمی امدی، ۱۳۶۶، ج۱: ۲۵۰). آیه مذکور عصیان و معصیت نسبت به امر پروردگار و ایجاد انشقاق و تفرقه در جامعه اسلامی را نهی کرده است و به سبیل مؤمنین که عبارت از تعاون بر سبیل نیکوکاری و تقوا است؛ حکم می کند (طباطبایی، ۱۳۷۴، ج۵: ۱۳۲). درباره آیه تعاون گروهی از فقها حرمت اعانت بر اثم را استنباط کرده‌اند و گروهی دیگر این آیه «لا تعانوا علی الاثم و العدوان» را برای این مقصود کافی ندانسته‌اند. آن دسته از فقهایی که آیه مذکور را برای حرمت اعانت بر اثم ناکافی می‌دانند؛ از جمله محقق ایروانی در حاشیه بر مکاسب معتقد هستند که نهی به کار رفته در آیه مؤید نهی تنزیهی است که در مقابل نهی تحریمی قرار دارد؛ بنابراین اعانت بر اثم مکروه است (ایروانی نجفی، ۱۳۸۴، ج۱: ۱۵). اما در پاسخ به این ایرادات مطروحه می‌توان گفت که آیه از دو عبارت مستقل و جدای از هم تشکیل شده است که یکی امر به تعاون در تقوا است که حکم آن استحباب است زیرا امر به تقوا مستحب است و بخش دیگر جمله امر به عدم تعاون در اثم و عدوان است که حکم حرمت را دارد، به این خاطر که اثم و عدوان حرام هستند. بنابراین این دو عبارت منفک از یکدیگر می‌باشند و این که امر بر تقوا و معاونت در آن مستحب است (واجب نیست) دلیلی بر اینکه این حکم به عدم اعانت بر اثم تسری کرده و حکم حرمت را جاری نکرد نخواهد بود؛ و این مسئله توسط ادراک عقلی متناسب با با تناسب حکم و موضوع به‌دست می‌آید چراکه ظلم و عدوان عقلاً قبیح و مذموم است و عقل مستقلاً بر حرمت آن دلالت دارد نه کراهت آن. بنابراین امام خمینی (ره) در پاسخ به شبهه محقق ایروانی نسبت به مدلول آیه برآمده و اذعان می‌کند که در عبارت و آیه مذکور قراینی وجود دارد که مؤید تحریمی بودن نهی هستند. اول آنکه به تناسب حکم و موضوع، از نهی بر اعانت بر اثم و عدوان، حرمت اعانت به ذهن متبادر می‌شود. دومین شاهد براین مدعا نیز عطف کلمه عدوان است که عقلًا و شرعاً اعانت دیگران بر ظلم، حرام است (خمینی، ۱۳۸۱، ج۱: ۱۳۱) و با توجه به اینکه در اینجا با دو جمله با دو حکم متفاوت (امر و نهی) روبرو هستیم بحث وحدت

سیاق منتفی خواهد بود؛ چراکه وحدت سیاق زمانی موجود است که دو عبارت دارای حکم واحدی باشند که مشتمل بر امر یا نهی باشد (موسوی بجنوردی، ۱۳۷۹، ج۲: ۲۳۲). پس از رد ایرادات فقهایی نظیر محقق ایروانی نسبت به عدم دلالت آیه تعاون بر اعانت بر اثم و مطابق آیاتی که اعانت ظلمه را نهی می‌کند و به قرینه درکنار هم قرار گرفتن اثم و عدوان در آیه ۲ سوره شریفه مائده می‌توان گفت: اعانت بر اثم (مطلق گناه) و عدوان (ظلم) حرام است و با توجه به اینکه مخاطبان ظواهر قرآن و احکام استخراج شده از آن عموم مردم می‌باشند (معرفت، ۱۴۲۹ق، ج۱: ۵۷)، مراد شارع مقدس بر امر به تعاون و اعانت در تقوا و نیکی‌ها و امر بر عدم اعانت بر اثم و ظلم و عدوان امری کلی است که از عمومیت برخوردار است و مخاطب آن عموم مسلمانان در همه ادوار تاریخ می‌باشند که باید نسبت به همدیگر در تقوا و امور خیر معین و یاری‌رسان باشند و نسبت به عصیان الهی و ارتکاب اثم و عدوان نباید تشویق‌کننده و یاری‌دهنده یکدیگر باشند. بنابراین کوچکترین فعل و ترک فعلی که یاری‌کننده ظلمه و آثم باشد اعم از این که در عوالم حقیقی یا مجازی رخ بدهد، حرام خواهد بود.

۲.۲ روایات

در کتب روایی و معتبر شیعی از جمله اصول کافی مرحوم کلینی، وسائل الشیعه شیخ حر عاملی، ثواب الاعمال و عقاب الاعمال شیخ صدوق و سایر کتب روایی احادیث فراوانی نسبت به موضوع یاری و اعانت ظلمه یافت می‌شود که حاکی از آن است که اعانت و یاری کردن ظلمه از قبیح‌ترین گناهان است که مؤاخذه و عقاب شدید الهی بر آن مترتب می‌شود (مکارم شیرازی، ۱۳۷۴، ج۱۶: ۵۷). به‌عنوان نمونه: در وسائل الشیعه در حدیثی که از محمد بن یعقوب نقل شده و سلسله راویان آن به امام سجاد علیه السلام می‌رسد ایشان از همنشینی با گناهکاران و اعانت ظالمان بر حذر داشته‌اند و می‌فرمایند «إیاکم وصحبة العاصین ومعونة الظالمین» (حرعاملی، ۱۴۰۳، ج۱۲: ۱۲۸). درروایت دیگری که سلسله روایات آن نهایتاً به ابی عبدالله امام جعفر صادق علیه السلام می‌رسد را صاحب ثواب الاعمال در کتاب خود آورده است که آن حضرت نسبت به شخصی که معین قاتلی باشد فرمودند مورد غضب و خشم خداوند در روز قیامت واقع خواهد شد و هرگز مشمول عفو و رحمت باری تعالی قرار نخواهد گرفت: «مَنْ أَعَانَ عَلَى قَتْلِ مُؤْمِنٍ بِشَطْرِ كَلِمَةٍ جَاءَ يَوْمَ الْقِيَامَةِ بَيْنَ عَيْنَيْهِ مَكْتُوبٌ آيِسٌ مِنْ رَحْمَةِ اللَّهِ تَعَالَى» (ابن بابویه (صدوق)، ۱۴۰۶ق، ج۱: ۲۷۶). بر اساس روایات مذکور خصوصا روایت مندرج در کافی به‌نقل از رئیس مذهب شیعه امام جعفر صادق علیه السلام که کوچکترین خدمت و یاری به ظلمه و دستگاه ظلم را حتی در هنگام تنگدستی جایز نمی‌دانند و اطلاق سایر روایات و عرضه آنها به آیات مرتبط با بحث اعانت بر اثم و عدوان، هرگونه عملیات اعم از فعل و ترک فعل که در جهت کمک گناه و ظلم صورت بگیرد، خواه در فضای حقیقی و خواه در دنیای مجازی حرام بوده و حسب مورد و شرایط عقوبت و مؤاخذه دنیوی و اخروی شامل حال فرد معین خواهد شد.

۳.۲ دلیل عقل

هرجایی که محل زیست جمع و اجتماعی باشد نیازمند و مستلزم وجود قانون و اجرای آن جهت عدم تضییع حقوق دیگران و برقراری نظم و جلوگیری از هرج و مرج در آن محیط است و این امر امری عقلانی و منطقی است. فضای مجازی هم به‌عنوان محل زیست بشر از این قاعده مستثنی نیست. روایات هم مؤید حجیت عقل هستند و جایگاه و شأنیت عقل را می‌توان از حدیث مشهوری که از امام کاظم وارد شده است دریافت که ایشان فرمودند: خداوند دو حجت را در اختیار مردم قرار داد، حجتی ظاهری که پیامبران و معصومین علیهم السلام هستند و دیگری حجت باطنی که همانا عقل است (کلینی، ۱۴۰۷ق، ج۱: ۱۶). انجام منکر و اعمالی که حرام و ناپسند است قبیح است. این قبح را عقل مستقلاً درک می‌کند و به ترک آن عمل حکم می‌کند. بنابراین امر به حرام و تحریک دیگری و فراهم ساختن مقدمات برای انجام فعل ناشایست توسط دیگری نیز توسط عقل مذمت شده و قبیح خواهد بود. به نظر امام خمینی اگر شخصی به سرقت سارقی کمکی کند صرف نظر از این که قصد وقوع فعل مجرمانه و ارتکاب عمل حرام را داشته یا نداشته باشد عقلاً این کار مجرمانه دانسته شده و از منظر عقل قبیح است و قبح عقلی دارد، اگرچه با وجود قصد قطعاً و عقلاً قبح بیشتری خواهد داشت (خمینی، ۱۳۶۸، ج۱: ۱۳۰). در واقع بنای عقلا بر مجازات معین، بر اساس درک حسن و قبح عقلی یک عمل است؛ به این معنا که هرگاه عقلاً چیزی را مجرمانه بدانند به‌دلیل قبیح بودن آن است و به‌تعبیر علامه طباطبایی بنای عقلا مبتنی بر فطرت انسانی و ضرورت نظام اجتماعی بوده و مستند آن عقل است (طباطبایی، بی تا، ج۲: ۱۸۸-۲۰۵) نسبت به مسائلی که جنبه اجتماعی دارد عقل حکم می‌کند به این که برای حفظ نظام و عدم هرج و مرج باید از کارهایی که موجب هرج و مرج می‌شود پرهیز کرد. از این رو عقل مستقلاً حکم می‌کند به حرمت آنچه که موجب اختلال نظام عالم شود (موسوی قزوینی، ۱۴۲۳ق، ج۵: ۳۰۱) که اعانت بر اثم از قبیل کارهایی است که در صورت وقوع و فراگیر شدن و عدم برخورد با شایع شدن آن باعث هرج و مرج و نابسامانی و اختلال نظام می‌گردد. بر اساس این مقدمات عقل حکم می‌کند به حرمت اعانت بر اثم و حکم می‌کند به برخورد و مقابله با آن.

۴.۲ قاعده لاضرر

قاعده لاضرر(لاضرر و لاضرار) از جمله قواعدی است که بر سایر قواعد و احکام اولیه حکومت دارد (موسوی بجنوردی، ۱۳۷۷، ج۱: ۲۴۳). وقتی لا در لاضرر «لا نفی» در نظر گرفته شود و واژه «حکم» در تقدیر باشد مراد از آن این است که حکمی که ضرر دارد در دایره تشریع احکام وضع نشده است (محقق داماد، ۱۳۹۸، ج۱: ۱۸۴). پس ضرر به خویش و اضرار به غیر بنابراین وضع و نظریه و مطابق قاعده لاضرر حرام است (سبحانی، ۱۴۱۵ ق، ج۲: ۱۸۲). پس از اثبات حرمت ضرر و ضرار مطابق آیات و روایات می‌توان گفت که باتوجه به فتوا فقها استفاده و بهره‌مندی از فضای مجازی مباح بوده و حکم اولیه در باب این مسئله اباحه شرعی است لکن زمانی که استفاده سوء از این فضا شود و به حیثیت، مال، جان و آبرو و شخصیت افراد خدشه و ضرری وارد شود، مطابق لاضرر حرام است و بنابراین که ضرر و ضرار حرام بوده و بر حکم اولیه که اباحه است حکومت دارد، اعانت بر اثم که موجبات ضرر به شخص معان و یا اشخاص ثالث می‌گردد در فضای مجازی همچون

فضای حقیقی حرام خواهد بود.

۳ بررسی امکان پیش‌بینی مجازات متناسب برای اعانت بر اثم در فضای مجازی

۱- ابتدا باید این مسئله تبیین شود که اساساً اعانت بر اثم حرام است یا حرام نیست تا بتوان برای آن به لحاظ شرعی و قانونی مجازات متناسب را در نظر گرفت. زیرا اگر فرضاً مجازات اعانت بر اثم صراحتاً در شرع مقدس و توسط شارع حکیم ذکر نشده باشد در مورد اعمال حرام و یا واجبی که برای انجام یا عدم انجام آنها در نظام تشریعی اسلام، مجازات مشخصی تعیین نشده، تعیین مجازات تعزیری به رأی محکمه و شخص قاضی واگذار شده است و بنابر رویکرد غالب و دیدگاه فقهی مشهور فقها، حاکم شرع می‌تواند به صلاحدید خود، فردی را کـه عمل حرامی مرتکب شده است تعزیر کند ولی بایـد ما دون الحد و کمتر از مقدار حد باشد (مسجدسرایی، ۱۳۹۲: ۸۷). با توجه به مستندات مذکور اعانت بر اثم اعم از فضای حقیقی و فضای مجازی حرام بوده و محاکم قضایی می‌توانند حسب موارد مختلف مجازات‌های متناسبی را در نظر بگیرند.

۲- نکته دیگر که حائز اهمیت است تفاوت اعانت بر اثم نسبت به‌مورد مشابه آن در قانون مجازات اسلامی یعنی معاونت در جرم است که این امر در چگونگی و کیفیت مجازات معین بر اثم اثرگذار است. در تفاوت بین اعانت بر اثم با اصطلاح معاونت در جرم که در قانون مجازات اسلامی و در مواد ۲۲۶ تا ۲۲۹ به آن اشاره شده و مورد تعریف واقع گردیده است و مجازات آن حسب مورد تعیین گشته است؛ می‌توان گفت: اعانت براثم زمانی محقق می‌شود که گناهی توسط فردی صورت گرفته باشد و دیگری او را در رسیدن به مقصودش که نامشروع بوده یاری کرده باشد که در این صورت فرد یاری‌دهنده معین بر اثم خواهدبود (محقق داماد، ۱۳۹۸، ج۴: ۲۰۶)؛ مانند اینکه مثلاً زن مشاطه و آرایشگری که می‌داند مشتری وی جهت نشان دادن آرایش خود به نامحرم به او مراجعه کرده است چنانچه وحدت قصد با وی داشته باشد اعانت بر اثم خواهد بود (اراکی، ۱۳۷۱، ج۱: ۵۹۹)؛ و در حالی که برخی گناهان جرم هستند و بالعکس اما در عین حال در برخی از موارد عمل انجام شده توسط شخص از گناهان و از رذیلت‌های اخلاقی و شرعی است اما در قانون جرم‌انگاری نشده است نظیر غیبت یا دروغ‌گویی. از این رو رذیلت‌های اخلاقی مانند دروغ‌گویی و یا غیبت ناپسند است اما در حقوق نسبت به برخی از موضوعات و با تحقق پاره ای از شرایط جرم‌انگاری شده و دارای مجازات خواهد بود. به این خاطر اثم و جرم در باب ضمانت اجرا نیز با یکدیگر متفاوت خواهند بود (کاتوزیان، ۱۳۹۳: ۶۱). از این رو با وجود اینکه برخی از اثم‌ها جرم نیستند و برخی جرم‌ها نیز ممکن است اثم نباشند اما بسیاری از جرم‌ها در زمره گناهان جا می‌گیرد و مجازات آن از طریق حکم حرمت بر اساس یکی از این دو امر صورت می‌گیرد. نظیر مثال ساختن کلید برای اجرای عمل مجرمانه و گناه سرقت.

همچنین باتوجه به این مسئله که گناهانی که نسبت به دیگران صورت می‌گیرد بر ذهن و روان اشخاص اثرات منفی و نامطلوبی می‌گذارد می‌توان با توجه و عنایت به آزار روحی اشخاص درصورت شکایت افراد مجازات متناسب با آن عمل خلاف را مد نظر قرار داد. مشکلات حقوقی نظیر عدم رعایت حق صاحب اثر، حق تألیف، کلاهبرداری، سرقت، ارعاب و تهدید انتشار مسائل خصوصی و ... در فضای مجازی قابلیت پیگیری و

تعقیب حقوقی و جزایی را با توجه به قواعدی نظیر قاعده لاضرر و قاعده اعانت بر اثم دارا است.

۴ نتیجه‌گیری

مستندات قاعده اعانت بر اثم اعم از فضای حقیقی و فضای مجازی است و با توجه به اثبات حرمت اعانت بر اثم محاکم قضایی می‌توانند باتوجه به موضوعات مختلف و با هدف جلوگیری از اشاعه جرم و گناهانی که با امنیت و آسایش شهروندان و جامعه مرتبط هستند به مقابله و برخورد بپردازند.

فضای مجازی باتوجه به ویژگی‌های منحصر به فرد خود از جمله سرعت انتشار پیام، تسریع در روند فعالیت‌های تجاری و اقتصادی و برطرف کردن نیازها و کارهای اداری و ... فرصت‌های زیادی را برای افراد ایجاد کرده است اما در عین حال با توجه به گستردگی و بی‌انتها بودن آن و ویژگی‌هایی مانند گمنامی و ناشناخته بودن هویت اشخاص می‌تواند موجبات مشکلات عاطفی و جرایم اخلاقی و اجتماعی شود. از این رو مدیریت این فضا توسط افراد متخصص و مجرب کاملاً ضروری است.

در نهایت پیشنهاد می‌شود علاوه بر مدیریت فضای مجازی و فرهنگ‌سازی در استفاده مطلوب از این فضا برای حفظ امنیت و آرامش روانی جامعه با برهم‌زنندگان امنیت روانی جامعه در فضای مجازی و کمک‌کنندگان و تسهیل‌کنندگان این امر که معین و معاون در آن اثم و جرم هستند برخورد قضایی و تنبیهی متناسبی جهت تنبیه و اصلاح صورت گیرد.

مراجع

[۱] قرآن کریم

[۲] قانون جرایم رایانه‌ای

[۳] قانون مدنی

[۴] ابن بابویه (شیخ صدوق)، محمد بن علی، (۱۴۰۶ق). ثواب الاعمال و عقاب الاعمال، چاپ دوم، قم، دار الشریف الرضی للنشر.

[۵] ابن منظور، محمد بن مکرم بن علی، أبوالفضل، جمال الدین، (۱۴۱۴ق). لسان العرب، چاپ سوم، بیروت، دار صادر.

[۶] اراکی، محمدعلی، (۱۳۷۱). توضیح المسائل، قم، مرکز انتشارات دفتر تبلیغات إسلامي حوزه علمیه قم.

[۷] اسلامی تنها، علی اصغر، اقابیگلو، عزیز، پارسانیا، حمید، (۱۴۰۰). مدینه فاضله مجازی چارچوب نظری حکمرانی فضای مجازی جمهوری اسلامی، دوفصلنامه علمی دین و ارتباطات، سال بیست و هشتم، ش اول، بهار و تابستان، صص ۳۰۵-۳۳۰.

[۸] امام جمعه، طیبه، (۱۳۸۲). آموزش و پرورش در عصر اطلاعات، ماهنامه تکنولوژي آموزشي رشد، دوره ۱۹.

[۹] انصاری، شیخ مرتضی، (۱۴۱۱ق). المکاسب، چاپ اول، قم: انتشارات دارالذخائر.

[۱۰] ایروانی نجفی، میرزا علی، (۱۳۸۴). حاشیه المکاسب ،تهران، انشارات کیا.

[۱۱] پیرمرادیان، سیدمحمدرضا، (۱۳۹۴). «حرمت اعانه بر اثم و اعانه به ظالم در رسانه‌های خبری ومطبوعات از دیدگاه فقه اسلامی و با تأکید بر اندیشه‌ی فقهی امام خمینی (ره)»، سپهر سیاست، ش ۵، پاییز، صص ۶۱-۷۵.

[۱۲] تمیمی آمدی ،عبدالواحدبن محمد، (۱۴۱۰ق). غرر الحکم و درر الکلم، چاپ دوم، قم، دار الکتاب الاسلامیه.

[۱۳] حر عاملی، محمد بن الحسن، (۱۴۰۳ق). وسائل الشیعة، چاپ پنجم، بیروت: دار احیاء التراث.

[۱۴] خمینی، سیدروح الله الموسوی، (۱۳۶۸). المکاسب المحرمة، چاپ سوم، قم، موسسه اسماعیلیان.

[۱۵] خمینی، سیدروح‌الله موسوی، (۱۳۸۱). المکاسب المحرمة، تعلیق مجتبی تهرانی؛ قم، نشر مهر.

[۱۶] زراعت، عباس، گلی، سلمان، نجفی، حسین، یزدیان، جعفر، (۱۳۹۹). «مشروعیّت جرم‌انگاری عمل تولید، توزیع و انتشار بدافزارها در فضای سایبر»، مطالعات فقه و حقوق اسلامی، ش۲۳، پاییز و زمستان، صص ۴۱۵-۴۳۸.

[۱۷] زنداقطاعی، فاطمه، (۱۳۹۸). «بررسی فقهی و حقوقی اعانه براثم در فضای سایبر باراهبرد پیشگیری» ،دوفصلنامه تخصصی مطالعات فقهی،.سال دوم، ش دوم، بهار و تابستان، صص۳۹-۶۱ .

[۱۸] سبحانی، جعفر، (۱۴۱۵ق). الرسائل الاربع، چاپ اول، قم، مؤسّسه امام صادق علیه السلام.

[۱۹] سیاح طاهری، محمد حسین و دیگران، (۱۳۹۶). حقیقت مجازی (درباره فضای مجازی چه بدانیم و چه بگوییم؟)، تهران، مرکز ملی فضای مجازی.

[۲۰] طباطبایی، محمد حسین، (۱۳۷۴). ترجمه تفسیر المیزان، چاپ پنجم، قم، دفتر انتشارات اسلامی.

[۲۱] طباطبایی، محمدحسین، (بی تا). حاشیه الکفایة، قم، بنیاد علمی و فکری علامه طباطبایی.

[۲۲] کاتوزیان، ناصر، (۱۳۹۳)، مقدمه علم حقوق و مطالعه در نظام حقوقی ایران، چاپ نود و ششم، تهران، شرکت سهامی انتشار.

[۲۳] کلینی رازی، ابی جعفر محمد بن یعقوب، (۱۴۰۷ق). (اصول) الکافی ط اسلامیه، چاپ چهارم ،تهران، دار الکتب الاسلامیه.

[۲۴] محقق داماد، سیدمصطفی، (۱۳۹۸). قواعد فقه بخش جزایی (۴)، چاپ سی و هفتم، تهران، مرکز نشر علوم اسلامی.

[۲۵] مسجدسرایی، حمید، (۱۳۹۲). واکاوی در ادله شمول تعزیر، مطالعات اسلامی: فقه و اصول، سال چهل و پنجم، شمارپیاپی ۹۵، زمستان، صص ۸۷-۱۰۳.

[۲۶] معرفت، محمد هادی، (۱۴۲۷ق). التمهید فی علوم القرآن، چاپ دوم، قم، مؤسسه فرهنگی انتشاراتی التمهید.

[۲۷] مکارم شیرازی، ناصر، (۱۳۷۴). تفسیر نمونه ط دار الکتب الاسلامیه، چاپ سی و دوم، تهران، دار الکتب الاسلامیه.

[۲۸] موسوی بجنوردی، سید حسن، (۱۳۷۷). القواعد الفقهیة، چاپ اول، قم، نشر الهادی.

[۲۹] موسوی بجنوردی، سید محمد، (۱۳۷۹). قواعد فقهیة، چاپ سوم، تهران، مؤسسه عروج.

[۳۰] موسوی قزوینی، سیدعلی، (۱۴۲۳ق). تعلیقه علی المعالم الاصول، چاپ اول، تهران، مؤسسه نشر اسلامی.

[۳۱] هاشمی شاهرودی، سیدمحمود و دیگران، (۱۳۷۴). فقه اهل بیت علیهم السلام – فارسی، قم، مؤسسه دائرة المعارف فقه اسلامی.

اثر آموزش سواد رسانه‌ای بر هویت ملی

علیرضا بخشایش[۱]، مریم بابایی[۲]

[۱]عضو هیئت علمی بخش‌های روان‌شناسی و علوم تربیتی دانشکده روان‌شناسی و علوم تربیتی دانشگاه یزد
abakhshayesh20@yahoo.com
[۲]دانشجوی کارشناسی ارشد روان‌شناسی عمومی دانشگاه یزد
mary.babaei@yahoo.com

چکیده

هویت از مهم‌ترین موضوعات و مفاهیم علوم انسانی است که در عصر اطلاعات دستخوش تغییر و دگرگونی شده است. هویت ملی از جمله مفاهیمی است که به‌علت اهمیت ویژه‌ی آن برای دولت و ملت‌ها، حفظ آن ضروری است. رسانه‌ها نیز از جمله عواملی هستند که می‌توانند، این نوع هویت را به نفع خود تقویت یا تضعیف کنند. اما در صورتی که مخاطب مجهز به سواد رسانه‌ای باشد، تحت تأثیر ظاهر پیام‌ها قرار نمی‌گیرد و از هویت ملی خود محافظت می‌کند. هدف و روش: هدف از نگارش این مقاله بررسی یافته‌هایی بود که هویت ملی، تأثیرپذیری آن از رسانه و فایده‌ی سواد رسانه‌ای در حفظ هویت ملی را مورد بررسی قرار داده بودند، به‌همین دلیل به روش کتابخانه‌ای (تحلیلی-اسنادی) و با استفاده از کتاب ها، منابع الکترونیکی و بانک‌های اطلاعاتی این کار انجام شد. نتیجه‌گیری: با بررسی‌های به‌عمل آمده نتیجه می‌گیریم که هویت ملی متأثر از رسانه‌های جمعی و فناوری اطلاعات و ارتباطات است و راه محافظت از این تأثیرات، مجهز بودن به سواد رسانه‌ای است.

کلمات کلیدی: هویت ملی، رسانه، بحران هویت، عصر ارتباطات، سواد رسانه‌ای.

۱ مقدمه و بیان مسئله

موضوع هویت از ابتدایی‌ترین و مهم‌ترین موضوعات بشر است. این موضوع زمانی پیچیده‌تر می‌شود که دریابیم انسان‌ها همیشه تابع یک هویت واحد نیستند، به این معنی که آنها در مقابل وضعیت‌های متفاوت، هویت‌های متعددی را بدون هیچ تعارضی تجربه می‌کنند (معینی علمداری، ۱۳۸۳).

هویت در فرهنگ معین، ذات بارتعالی، هستی و وجود و آنچه موجب شناسایی شخص می‌شود، معنی شده است (معین، ۱۳۷۱). هویت فرآیندی سیال و نوشونده است که در طی زمان توسط خانواده، طایفه و جامعه به افراد داده می‌شود (شیخاوندی، ۱۳۷۹) که دارای انواع مختلفی است اما می‌توان دو نوع کلی هویت را از یکدیگر متمایز کرد: «هویت فردی» یعنی چیزی که فرد به واسطه ویژگی‌ها و خصوصیات منحصربه‌فرد خود مورد شناسایی قرار می‌گیرد و از دیگران متمایز می‌شود. نوع دوم «هویت جمعی» است که عبارت است

از تعلق خاطر تعدادی از افراد به امور مشترک با عنوانی خاص. چنین تعلقی، موجب احساس همبستگی و شکل‌گیری یک واحد جمعی می‌شود که با عنوان ما از ماهای دیگر جدا می‌شود (توسلی و قاسمی، ۱۳۸۳).

دیدگاه‌های نظری درباره‌ی هویت در سه دسته قرار می‌گیرند: گروه اول، یک نگرش فرهنگی و جمعی از هویت دارند و نمایانگر باورهای یک جمع هستند. گروه دوم نگاه ساختاری به هویت دارند و به بررسی ارتباطات نقش افراد و تفاوت‌های آنها با هویت می‌پردازد. این دیدگاه که پیروانی چون بورک[۱]، استریکر[۲]، مک‌کال[۳] و سیمونز[۴] دارد، به نظریه‌ی هویت، معروف است. سومین دیدگاه در مورد هویت، نظریه‌ی هویت اجتماعی است که در این نظریه، رفتار درون‌گروهی مانند ارتباط بین اعضای گروه، در نظر گرفته نمی‌شود. این نظریه در آثار تاجفل[۵]، ترنر[۶]، هوگ[۷] و ریچر[۸] دیده می‌شود (آقا محمدی و اسدی، ۱۳۹۸).

یکی از بخش‌های جامع هویت جمعی، هویت ملی[۹] است که از اساسی‌ترین عناصر کسب وحدت و همبستگی ملی است (حاجیانی، ۱۳۷۹). هویت ملی آخرین هویت اکتسابی است که توسط فرد، طی فرآیند جامعه‌پذیری از طریق خانواده، مدرسه و رسانه کسب می‌شود (شیخاوندی، ۱۳۷۹). اهمیت این هویت بدان جهت است که اگر افراد جامعه، از هویت ملی خود آگاهی نداشته باشند و یا این آگاهی سطحی باشد، تعهدی نسبت به جایگاه خود، برای حفظ جامعه نخواهند داشت (جعفرزاده پور،۱۳۸۹).

هویت ملی وقتی شکل می‌گیرد که اعضای جامعه، عناصر هویت[۱۰] خویش را بشناسند و برداشت درست از اجزای سازنده آن داشته باشند؛ زیرا هویت افراد در متن اجتماع و فرهنگ شکل می‌گیرد (زهیری، ۱۳۸۱). منابع و ابزارهای اصلی ساخت و حفظ هویت‌ها، مکان و فضا، زمان، دین ، زبان و فرهنگ هستند، که مهم‌ترین منبع هویتی به‌شمار می‌آیند. امروزه، وسایل نوین ارتباطی و فرآیند جهانی شدن، با متحول ساختن فضا و زمان و جدا کردن آنها از مکان، فضای انحصاری هویت‌سازی که در اختیار جوامع و فرهنگ‌ها بود را از بین برده و توانایی آنها در هویت‌سازی و هویت‌یابی افراد را کاهش داده است (کاروانی، ۱۳۹۷).

از آنجایی که پدیده‌ی فیلترسازی در کشور ما به کرات انجام می‌شود، ضرورت بررسی این موضوع که آیا پدیده‌ای جایگزین برای فیلترسازی وجود دارد یا خیر احساس شد. نوآوری این پژوهش روش تحلیل آن است که به‌صورت اسنادی-کتابخانه‌ای، پژوهش‌های بسیاری درباره ی این پدیده‌ی جایگزین یعنی سواد رسانه‌ای بررسی شد و نتایج آن در قالب یک کار جمع‌بندی شد.

باتوجه به آنچه در باب اهمیت حراست از هویت ملی گفته شد، هدف این پژوهش بررسی تحقیقاتی است که در زمینه‌ی اثرگذاری رسانه‌ها بر هویت ملی و چگونگی محافظت از آن، در برابر اثرات سوء رسانه‌ها، انجام

[1] Burke
[2] Striker
[3] M. Call
[4] Simons
[5] Tajfel
[6] Turner
[7] Hogg
[8] Richer
[9] National Identitiy
[10] Identity Elements

شده‌اند.

پژوهش‌های پیشین درباره‌ی تأثیر استفاده از رسانه‌ها و هویت همسو نیستند. برخی از این پژوهش‌ها حاکی از اثرات مثبت و برخی دیگر نیز نشان‌دهنده‌ی اثرات منفی رسانه بر هویت هستند که در ادامه به چند مورد اشاره می‌گردد.

تحقیقات دانایی و بابایی (۱۳۹۶)، ملکی و عباسپور (۱۳۸۸)، ربانی و همکاران (۱۳۸۸)، ربیعی (۱۳۸۸)، رانی (۲۰۲۲) و گوندوز (۲۰۱۷) نشان‌دهنده‌ی این امر است که افرادی که بسیار در معرض انواع رسانه‌های جمعی قرار می‌گیرند، تفکر و انواع ابعاد هویت آنان دستخوش تغییرات منفی خواهد شد.

از طرف دیگر برخی پژوهش‌ها مانند تاجیک (۱۳۸۷)، حسینی انجدانی و همکاران (۱۳۸۸)، قربان‌زاده سوار و همکاران (۱۳۹۵)، بهشتی و حقمرادی (۱۳۹۶)، بیات و آزادواری (۱۳۸۹) و کیبارگارد و همکاران (۲۰۱۱) نتایج خوش‌بینانه و امیدوارکننده‌ای درباره‌ی اثر رسانه بر هویت نشان می‌دهند و معتقدند که ابعاد هویتی در اثر تماس با رسانه تقویت می‌شوند.

به‌طور کلی این تحقیقات به دو دسته‌ی کلی تقسیم می‌شوند: دسته‌ی اول مانند دیدگاه آندرسون، نگاه خوش‌بینانه‌ای به رابطه‌ی رسانه و هویت ملی دارند. این گروه هویت ملی را به‌طور عمده تحت تأثیر ظهور تجدد و تکوین رسانه‌های جمعی، در چارچوب یک ملت واحد قرار می‌دهند. دسته‌ی دوم بر عکس گروه اول به این رابطه نگاه منفی دارند و مانند گیدنز معتقدند که هویت ملی در نتیجه‌ی گسترش ارتباطات جهانی و تحولات نظام‌های نمادین، تضعیف و به واسطه‌ی درهم فشرده شدن زمان و مکان به چالش کشیده می‌شود (ربانی و دیگران، ۱۳۸۸).

با توجه به اینکه به هر صورت، مثبت یا منفی، رسانه بر هویت اثرگذاری خواهد داشت، لازمه‌ی تجهیز به سواد رسانه‌ای احساس می‌شود، تحقیقات زیادی درباره‌ی اثر سواد رسانه‌ای در حفظ هویت در مواجهه با رسانه انجام شده‌اند. به‌طور مثال هابز و فراست (۲۰۰۳) و مک آرتور (۲۰۱۹)، لیویکستون (۲۰۱۴) و حسینی (۱۳۹۲) در مطالعات خود سواد رسانه‌ای را، ابزاری برای ایجاد تفکر خلاق و نقادانه یافتند.

در پژوهش نیومن (۲۰۱۵)، چو و دیگران (۲۰۲۲)، اژدری (۱۳۹۷)، بهشتی و مؤمنی (۱۳۹۸) نیز مشخص شد که سواد رسانه‌ای، مانند یک محافظ، از هویت در برابر عوامل خطر، محافظت می‌کند.

۲ جمع‌بندی ادبیات تحقیق

جمع‌بندی ادبیات تحقیق در جدول ۱ انجام شده است.

با توجه به ادبیات تحقیق، این نوشتار می‌کوشد یافته‌های کنونی، در زمینه‌های زیر را مورد بررسی قرار دهد:

- اثری که عصر ارتباطات بر هویت گذاشته است؟
- استفاده از رسانه‌ها چه اثری بر هویت ملی داشته است؟
- فایده‌ی آموزش سواد رسانه‌ای در حفظ هویت ملی چیست؟

جدول ۱: جمع‌بندی ادبیات تحقیق

نگاه خوش‌بینانه به تأثیر رسانه بر هویت	نگاه بدبینانه به تأثیر رسانه بر هویت
تاجیک (۱۳۸۷)، حسینی انجدانی و همکاران (۱۳۸۸)، قربان‌زاده سوار و همکاران (۱۳۹۵)، بهشتی و حقمرادی (۱۳۹۶)، بیات و آزادواری (۱۳۸۹) و کیبارگارد و همکاران (۲۰۱۱).	دانایی و بابایی (۱۳۹۶)، ملکی و عباسپور (۱۳۸۸)، ربانی و همکاران (۱۳۸۸)، ربیعی (۱۳۸۸)، رانی (۲۰۲۲)، گوندوز (۲۰۱۷).
سواد رسانه‌ای به‌عنوان محافظ در برابر عوامل خطر	**سواد رسانه‌ای به‌عنوان ایجاد کننده‌ی تفکر نقادانه**
نیومن (۲۰۱۵)، چو و دیگران (۲۰۲۲)، اژدری (۱۳۹۷)، بهشتی و مؤمنی (۱۳۹۸)، لیویکستون (۲۰۱۴).	هابز و فراست (۲۰۰۳) و مک آرتور (۲۰۱۹) و حسینی (۱۳۹۲).

۳ روش

داده‌های این پژوهش با جست‌وجو در پایگاه‌های اطلاعاتی مختلف جمع‌آوری شد. در فرآیند جست و جوی انگلیسی از کلمات کلیدی، identity and media، effect of media on identity، globalization and identity، effect of media on identity crisis و media literacy استفاده شد و در فرآیند جست‌وجوی فارسی، از کلمات کلیدی هویت ملی و رسانه، اثر رسانه بر هویت، سواد رسانه‌ای، رسانه و بحران هویت استفاده شد.

با بررسی چکیده‌ی مقالات به‌دست آمده، مقالات نزدیک‌تر به موضوع انتخاب و مقالاتی که ضعف و کاستی‌هایی داشتند کنار گذاشته شدند. همچنین در طی بررسی مقالات، مقالاتی که در متن مقالات جمع‌آوری شده به آنها ارجاع داده شده بود نیز انتخاب و بررسی شدند. تعدادی کتاب هم که قرابت موضوعی داشتند، انتخاب و بررسی شدند.

۴ یافته‌ها

۱.۴ عصر ارتباطات چه اثری بر هویت می‌گذارد؟

جهانی‌شدن روندی پرشتاب است، به حدی که جامعه‌ی نوینی در حال شکل‌گیری است. این روند پرشتاب مفاهیم بنیادی مانند هویت را نیز دچار تحولات اساسی کرده است، چرا که هویت در طول زمان حالتی پویا دارد و در دیالکتیک با خود و دیگری شکل می‌گیرند (کوپایی و بشارتی فرد، ۱۳۹۸). کاستلز معتقد است که فناوری‌های نوین اطلاعات، باعث پیوند نقاط دور عالم در شبکه‌های جهانی شده و جوامع مجازی را ایجاد کرده است که در نتیجه همه‌ی ساختارها و فرآیندهای مادی و معنوی بشر دگرگون می‌شوند (خدایاری و دیگران، ۱۳۹۳).

رسانه‌های گروهی بر تکوین یا تغییر هویت فردی و جمعی تأثیر شگرفی داشته‌اند، زیرا رسانه‌ها بافت نمادین زندگی اجتماعی معاصر را تشکیل می‌دهند. کارکرد رسانه، برقراری ارتباطات، برخورد ایده‌ها و

برداشت‌های ذهنی انسان، ایجاد فضای گفت‌وگو و ساخت افکار عمومی است (قربان‌زاده سوار و دیگران، ۱۳۹۵). آنها هم می‌توانند هویت را تقویت کنند و هم موجب گسست فرهنگی گردند (بهرامیان و یاقوتی، ۱۳۹۵). به‌عبارت دیگر همان‌گونه که می‌توانند هم هویت‌ساز و تدبیرکننده‌ی بحران باشند، می‌توانند هویت‌سوز و ایجادکننده‌ی بحران نیز باشند (بوربور و اسماعیلی، ۱۴۰۰).

رسانه ها این قدرت را دارند که با آشکار ساختن انواع خاصی از باورها و شکل دادن به رفتارها، اشکال خاص صدق و کذب را دسته‌بندی کنند و ایدئولوژی‌سازی کنند. از جمله خصوصیت‌های ایدئولوژی غیرآشکار بودن آن است، به این معنی که افراد ناخودآگاه آن را می‌گیرند و درونی‌سازی می‌کنند (مهدی‌زاده، ۱۳۸۹).

۲.۴ استفاده از رسانه بر هویت ملی چه اثری دارد؟

اگر در اثر کارکرد منفی رسانه، عناصر هویت ملی درونی نشود، هویت ملی دچار چالش خواهد شد. رسانه‌ها از طریق درونی‌سازی ارزش‌های جامعه، آنها را به نسل‌های آینده منتقل می‌سازد و باعث تداوم آنها می‌شود؛ اگر این درونی‌سازی به‌خوبی صورت نگیرد، مشکل شکاف نسلی[11] ایجاد شده و بحران هویت[12] در پی آن رخ می‌دهد. این بحران در زمینه‌های مختلفی مانند زمینه‌ی فردی، سیاسی، اجتماعی، اخلاقی، فرهنگی و اقتصادی رخ داده و فرد و جامعه را تحت تأثیر قرار می‌دهد. در این میان رسانه‌های رقیب با ایجاد تردید در مبانی هویت ملی سایر ملت‌ها، هویت ملی آنها را درگیر بحران کرده و دچار استحاله‌ی هویتی[13] می‌شوند (قربان‌زاده سوار و دیگران، ۱۳۹۵).

رسانه‌های تعاملی با جذابیت‌های خود نوع خاصی از مناسبات ارتباطی را در فضای رایانه‌ای شکل می‌دهد. مارک پاستر[14] معتقد است که رسانه‌های الکترونیکی، هویت افراد را بدون آگاهی آنان شکل می‌دهد (حاجیانی و محمدزاده، ۱۳۹۴).

دانایی و بابایی (۱۳۹۶) در بررسی نقش رسانه‌های مجازی در گرایش به هویت ملی دریافتند که مؤلفه‌های هویت ملی با افزایش حضور در اینترنت کاهش می‌یابند.

یافته‌های ملکی و عباس‌پور (۱۳۸۸) نشان می‌دهد افرادی که دارای مصرف رسانه‌های الکترونیکی هستند، میانگین هویت ملی آنها به‌طور معنی‌داری پایین تر از جوانانی است که اصلاً از این رسانه‌ها استفاده نمی‌کنند.

از تحقیق ربیعی (۱۳۸۷) درمی‌یابیم که رسانه‌های نوین، عامل تغییرات در نهادهای هویت‌ساز شده‌اند و فضای مجازی عوامل معناساز هویتی را دستخوش تغییر نموده است.

از تحقیق تاجیک (۱۳۸۷) پیداست که رسانه‌ها می‌توانند با بهره جستن از نمادها و واژه‌ها، به پدیده‌ها و حوادث و رفتارها و کردارها، محتوا و معنای خاص خود را اعطا کنند و از رهگذر انتقال این معنی و محتوا، بر فرد مصرف‌کننده تأثیری ژرف بگذارند و او را از گزند بحران‌های هویتی، فرهنگی، معرفتی، ارزشی، سیاسی و

[11] Generation Gap
[12] Identity Crisis
[13] Identity Transformation
[14] Mark Poster

اجتماعی برهانند یا در معرض و مسیر چنین بحرانی‌هایی قرار دهند.

نتایج پژوهش حسینی انجدانی و همکاران (۱۳۸۸) نشان داد میزان استفاده از رادیو-تلویزیون و رایانه، رشد هویت ملی و شناخت علائم و نمادهای ملی را پیش‌بینی می‌کند. استفاده از کتاب‌ها و مجلات غیردرسی و پایگاه اجتماعی-اقتصادی، نیز پیش‌بینی کننده میزان شناخت علائم و نمادهای ملی هستند.

آزمون فرضیه‌های تحقیق ربانی و همکاران (۱۳۸۸) نشان می‌دهد بین استفاده از رسانه‌های جمعی و هویت ملی، رابطه وجود دارد. به این ترتیب که افراد استفاده‌کننده از رسانه‌های داخلی در سازه هویت ملی نمره بالایی دریافت کرده‌اند و بر عکس، نمره افراد استفاده‌کننده از رسانه‌های خارجی در این سازه، نمره پایینی بوده است. این یافته، نشان‌دهنده تغییر نگرش‌ها به سمت الگوها و گرایش‌های جدید است. یافته‌های تجربی این تحقیق نشان می‌دهد که از میان متغیرهای اثرگذار بر هویت ملی به‌ترتیب، جنس، میزان استفاده از رسانه‌های خارجی، میزان استفاده از رسانه‌های داخلی، سن و وضعیت تأهل در تعیین گرایش هویت ملی، از سهم بیشتری برخوردار بوده‌اند.

یافتههای پژوهش قربان‌زاده سوار و همکاران (۱۳۹۵) با بهرهگیری از روشهای تحلیلی ـ تبیینی حاکی از آن است که رسانه‌ها با تأثیر در سه شاخص هویتی، یعنی عناصر، مبانی، و جایگاه آن در هویت ملی تأثیر شگرف مثبت یا منفی می‌گذارد.

بهشتی و حق‌مرادی (۱۳۹۶) با فرا تحلیل ۵۰ مقاله دریافتند که ۴۰ درصد مقالات قائل به هم‌سازی بین هویت ملی و هویت قومی بوده‌اند و ۴۸ درصد آنها رسانه‌ها و فضای جهانی‌شدن را باعث تقویت هویت قومی دانسته‌اند.

یافته های تحقیق بیات و آزادواری (۱۳۸۹) نشان می‌دهد که در معرض فرآیند جهانی (رسانه‌های ارتباطی نوین) قرار گرفتن رابطه‌ای با هویت ملی ندارد ولی با احساس تعلق جهانی رابطه معنادار دارد.

رانی (۲۰۲۲) نیز در تحقیق خود نشان می‌دهد که افراد به این دلیل که می‌خواهند خود را در اندازه‌ی افراد به تصویر کشیده شده در رسانه‌ها نشان دهند، با بحران هویت مواجه می‌شوند.

گوندوز (۲۰۱۷) نیز اینگونه بیان می‌کند که با توجه به اینکه افراد در رسانه‌های اجتماعی، می‌توانند نقش یا نقش‌های متعددی را تجربه کنند می‌تواند بر هویت‌های آنها اثرگذار باشد.

کییارگارد و همکارانش (۲۰۱۱) در پژوهش خود نشان می‌دهند که پوشش رسانه‌ای مثبت از یک نهاد، سازمان، سرزمین، تا زمانی که تناقضی با تصویر مثبت ارائه شده نداشته باشد می‌تواند اثر مثبتی بر هویت افراد تحت آن نهاد یا سازمان و یا سرزمین بگذارد.

۳.۴ فایده‌ی آموزش سواد رسانه‌ای در حفظ هویت ملی چیست؟

از مجموع این مطالعات ناهمسو و با بررسی عوامل مؤثر بر تقویت و تضعیف هویت ملی چنین استناد می‌شود که بهره‌مندی از رسانه‌های اطلاعاتی و ارتباطی همراه با مجموعه‌ای از صلاحیت‌ها، مهارت، دانش، نگرش و آگاهی، می‌تواند این استفاده را مؤثرتر نماید (مقدس‌زاده و صفاهیه، ۱۳۹۶). این برخورد هدفمند سواد

رسانه‌ای[15] است که موجب بالا رفتن سطح آگاهی افراد جامعه به عنوان مخاطبین رسانه‌ها می شود و منجر به ارتباطی دوسویه با رسانه‌ها و تقویت ساختار دموکراتیک جامعه در راستای مباحث مشارکت فعال در حوزه رسانه می‌گردد (زارع کهن، ۱۳۹۳).

توانایی دسترسی و استفاده از رسانه‌ها، تولید پیام و ارتباط با رسانه‌ها، تحلیل و ارزیابی انتقادی رسانه‌ها سواد رسانه‌ای نام دارد (آکسترند،۲۰۰۹). از منظر انجمن ملی آموزش سواد رسانه‌ای، سواد رسانه‌ای یعنی توانایی دسترسی، تحلیل، ارزیابی و تولید اطلاعات در قالب‌های متنوع رسانه‌ای که شامل پیام‌های چاپی و غیرچاپی است (مازندرانی، ۱۳۹۶).

سواد رسانه‌ای، بیش از چهار دهه است که به‌عنوان یکی از کارآمدترین راهبردهای نظارتی و هویتی، به‌ویژه در سیاست‌گذاری کشورهای توسعه‌یافته و مالکان رسانه‌های بزرگ نقش ایفا کرده است (هزارجریبی و صفری شالی، ۱۳۹۱).

یونسکو[16]، هدف آموزش سواد رسانه‌ای را دسترسی به رسانه‌ها به‌عنوان ابزارهای درک جامعه، ارتقای مهارت‌های تحلیل انتقادی پیام‌های رسانه‌ای، خلاقیت و تعامل در حوزه‌های مختلف ارتباطات رسانه‌ای و گسترش ارزیابی انتقادی پیام‌ها به‌منظور تقویت فعالانه‌ی توانایی‌های افراد می‌داند (تقی‌زاده و کیا، ۱۳۹۳).

تامن سواد رسانه‌ای را «فیلتری داوری کننده و حافظ هویت» می‌داند و می‌گوید برخورداری از سواد رسانه‌ای باعث می‌شود مخاطب در برابر القای پیام‌های رسانه‌ای، هویت خود را حفظ کند و جهان واقعی را همسان با تفسیر رسانه‌ای در نظر نمی‌گیرد (بولز، ۲۰۰۲). اندیشمندان حوزه ارتباطات و رسانه‌ها برای کاهش اثرات مخرب رسانه‌ها ایده‌ها و پیشنهادهایی را ارائه کرده‌اند که یکی از این پیشنهادها، تقویت «سواد رسانه‌ای» شهروندان در جامعه است (فرهنگی، ۱۳۸۷).

سواد رسانه‌ای به دنبال شناخت جنبه‌های ظاهراً حذف‌شده‌ی پیام است که در لایه‌های بعدی پیام جاسازی شده است، به‌همین دلیل به آن «فهم سطح بالاتر» گفته می‌شود. با دارا بودن این سواد، مخاطب، انتشار یک پیام را دلیل بر تطابق آن با واقعیت نمی‌داند (قاسمی، ۱۳۸۵).

آموزش سواد رسانه‌ای زمینه ارتقای انتظام و امنیت اجتماعی و فردی، سواد سیاسی، جامعه‌پذیری، نظارت بر رفتار دولت‌مردان و سایر نهادهای متولی امر تربیت را فراهم می‌سازد. آموزش سواد رسانه‌ای، قصد هوشیارسازی و اختیاربخشی به مخاطب را دارد، چرا که این مهارت، پایه و اساس آینده‌ی جامعه‌ی آگاه را تشکیل داده و باعث تقویت ساختارهای دموکراتیک می‌شود (ترک‌زاده و دیگران، ۱۳۹۸).

سواد رسانه ای مبتنی بر هفت اصل است که ازین قرارند: ۱. ساختگی و سازه‌ای بودن رسانه‌ها، ۲. بازسازی واقعیت توسط رسانه‌ها، ۳. کسب مفهوم مورد نظر مخاطبان از رسانه‌ها، ۴. تجاری بودن محصولات رسانه‌ای، ۵. حضور پیام‌های ایدئولوژیکی و ارزشی در رسانه‌ها، ۶. جهت‌گیری سیاسی و اجتماعی در رسانه‌ها، ۷. توجه به اصل زیبایی‌شناختی در رسانه‌ها (قاسمی، ۱۳۸۵).

لیویکستون (۲۰۱۴) در پژوهشی نشان داد که مهارت سواد رسانه‌ای بر کاهش آسیب‌های شبکه‌های اجتماعی و احساس تعلق به ابعاد هویت اثرگذار است.

[15] Media Literacy
[16] UNESCO

هابز و فراست (۲۰۰۳) طی تحقیقی دریافتند که افراد دارای سواد رسانه‌ای می‌توانند به شکل تأثیرگذاری، تکنیک‌های اقناع کلامی به‌کار رفته در تبلیغ، مخاطب هدف، نقطه‌نظر و تکنیک‌های ساختار خلاق به کار رفته در تبلیغات را تشخیص دهند.

مک آرتور (۲۰۱۹) در مقاله‌ی خود این‌گونه عنوان می‌کند که چون اغلب جوانان از تأثیر رسانه‌ها بر روان خود آگاه نیستند، درصورت تجهیز به سواد رسانه‌ای، با تفکر انتقادی با رسانه‌ها روبرو می‌شوند.

نیومن (۲۰۱۵) نیز این‌گونه توضیح می‌دهد که دارا بودن سواد رسانه‌ای برای جوانانی که در ارتباط با رسانه‌ی اینستاگرام هستند، از هویت آنان محافظت می‌کند.

چو و دیگران (۲۰۲۲) نیز دارا بودن سواد رسانه‌ای را به‌عنوان یک درمان بالقوه در برابر مضرات احتمالی رسانه‌های جمعی می‌دانند.

بهشتی و مؤمنی (۱۳۹۸) در اثر خود سعی کرده‌اند تا رابطه ضروری بین سواد رسانه‌ای و سواد اطلاعاتی را با نمادسازی در تلویزیون برای بازتعریف هویت ملی در جامعه ایرانی با روش تحلیلی- توصیفی بررسی کنند.

حسینی (۱۳۹۲) نیز در اثر خود این‌گونه ذکر می‌کند که دارا بودن سواد رسانه‌ای این امکان را برای مخاطب فعال فراهم می‌کند که در برابر القای سوگیرانه بازنمایی رسانه‌های رقیب، هویت ملی را همسان با تفسیرهای مذکور در نظر نگرفته و کنترل خود را در پنج حوزه بینش، دانش، گرایش، روش و کنش، به شکلی ناخودآگاه به نظام بازنمایی رسانه‌ای نسپارد.

اژدری(۱۳۹۷) نیز در نتایج اثر خود نشان می‌دهد که سواد رسانه‌ای به‌مثابه درسی آموزشی در رشته علوم سیاسی می‌تواند ابزاری قوی و مؤثر به‌منظور آگاهی دانشجویان از تأثیرات رسانه‌ها جهت ساخت و بازسازی هویتی آنان باشد.

۵ بحث و نتیجه‌گیری

آنچه که موجب شناسایی ما می‌شود هویت نام دارد. هویت فرآیندی است که فرد، بخشی از آن را از خانواده و بخشی دیگر آن را از جامعه کسب می‌کند. این پدیده دارای انواعی است که دو نوع کلی آن فردی و جمعی است . یکی از بخش‌های جامع هویت جمعی، هویت ملی است. وقتی که اعضای جامعه، عناصر هویت خویش را بشناسند و برداشت صحیحی از اجزای سازنده آن داشته باشند هویت ملی شکل می‌گیرد اگر افراد از عناصر هویت ملی خود آگاهی نداشته باشند، نسبت به جامعه‌ی خود و جایگاه خودشان در جامعه بی‌تعهد شده و این بی‌تعهدی یک عامل خطر محسوب می‌شود.

پس حفظ هویت ملی، به‌دلیل کمک به انسجام یک ملت اهمیت به‌سزایی دارد. رسانه‌ها این قدرت را دارند که عقاید مردم را بسته به هدف خود، تغییر دهند. پس منابع ساخت هویت، تحت تأثیر رسانه‌ها و روند جهانی شدن، مدام تغییر می‌یابند. بسته به اینکه فرد تا چه میزان و با چه مهارت و دانشی از رسانه استفاده می‌کند، ممکن است که هویت ملی وی دچار تغییرات مثبت یا منفی شود. یکی از این عوامل که می‌توانند تقویت‌کننده و محافظ هویت ملی باشد، دارا بودن سواد رسانه‌ای است. سواد رسانه‌ای، مانند یک ملاک و

مرجعی درآگاهی فرد قرار گرفته که به کمک آن، فرد می‌آموزد که آنچه در قالب پیام از هرکدام از انواع رسانه‌ها، دریافت می‌کند واقعیت پیام نیست و تفسیر ارائه شده را سریعاً نمی‌پذیرد. به‌تعبیر دیگر، آگاهی از سواد رسانه‌ای مانند یک سپر، هویت افراد را در برابر تهاجمات پیام‌هایی که تغییر ظاهر می‌دهند حفظ می‌کند، پس در عصر اطلاعات و جهانی شدن، به‌وسیله‌ی سواد رسانه‌ای می‌توان از هویت ملی محافظت کرد و همچنین آن را تقویت نیز نمود، چرا که زمانی که افراد یک جامعه مجهز به سواد رسانه‌ای باشند با آگاهی پیام‌های دریافتی را تعبیر و تفسیر و قبول یا رد می‌کنند.

مراجع

[۱] آقا محمدی، جواد؛ اسدی، سودابه (۱۳۹۸). واکاوی ابعاد و مؤلفه های شاخصه هویت ملی در اسناد تحولی آموزش و پرورش ایران، فصلنامه سیاست‌های راهبردی و کلان، دوره‌ی ۷، شماره‌ی ۳، صص. ۱-۷.

[۲] آل قیس، علیرضا؛ دادگران، سید محمد؛ رسولی، محمدرضا (۱۳۹۸). تبیین ارتباط میان اقناع رسانه‌ای شبکه‌های اجتماعی و سبک زندگی- موردکاوی تلگرام، مطالعات رسانه‌ای، سال ۱۴، شماره‌ی ۵، صص. ۱۱۴-۱۲۰.

[۳] اژدری، بهناز (۱۳۹۷). نقش سواد رسانه‌ای در هویت‌یابی و ضرورت آموزش آن در رشتهٔ علوم سیاسی. جستارهای سیاسی معاصر ۹(۲)، صص. ۸۱-۱۰۴.

[۴] اصغری، صالح (۱۳۹۲). آموزش واحد درسی «سواد رسانه‌ای» در آموزش و پرورش، بایسته‌ها و راهکارها. همایش ملی انجمن مطالعات درسی ایران (تغییر در برنامه درسی دوره‌های تحصیلی آموزش و پرورش)، شماره ۱، صص. ۱-۵.

[۵] بهرامیان، امید؛ یاقوتی، هدی (۱۳۹۵). رابطه‌ی استفاده از شبکه‌های ماهواره‌ای فارسی‌زبان و پایبندی به هویت فرهنگی در زنان شهر تهران، مطالعات اجتماعی روان‌شناختی زنان، سال ۱۴، شماره‌ی ۱، صص. ۲۱۶-۱۸۷.

[۶] بهشتی، صمد؛ حقمرادی، محمد (۱۳۹۶). فراتحلیل مطالعات مرتبط با رابطه بین هویت قومی و هویت ملی در ایران با تأکید بر نقش رسانه. مسائل اجتماعی ایران، ۸(۲) صص. ۵-۲۷.

[۷] بیات، بهرام؛ آزادواری، علی اکبر (۱۳۸۹). تأثیر جهانی‌سازی بر هویت ملی و هویت جهانی (با تأکید بر رسانه‌های ارتباطی نوین). مطالعات امنیت اجتماعی، دوره جدید(۲۲)، صص. ۸۳-۱۰۴.

[۸] تاجیک، محمدرضا (۱۳۸۷). رسانه و بحران در عصر فراواقعیت (با تأکید بر بحران هویت). پژوهش‌های ارتباطی (پژوهش و سنجش)، ۱۵(۵۶)، صص. ۶۹-۹۳.

[۹] ترک‌زاده، جعفر؛ مرزوقی، رحمت‌اله؛ محمدی، مهدی؛ احمدی، حبیب؛ جوکار، ناصر (۱۳۹۸). تدوین برنامه درسی آموزش سواد رسانه‌ای در راستای بسط امنیت اجتماعی: یک مطالعه کیفی. رهیافتی نو در مدیریت آموزشی، ۱۰(۲)، پیاپی ۳۸، صص. ۱۱۳-۱۳۲.

[۱۰] تقی زاده، عباس؛ کیا، علی‌اصغر (۱۳۹۳). نیازسنجی برنامه‌ی آموزش سواد رسانه‌ای در مدارس، سال پانزدهم، شماره‌ی ۲۶، صص. ۱-۵.

[۱۱] توسلی، غلام؛ قاسمی، یوسف (۱۳۸۳). هویت‌های جمعی و جهانی‌شدن، نامه‌ی علوم اجتماعی، شماره‌ی ۲۴، صص. ۱-۴.

[۱۲] جعفرزاده‌پور، فروزنده (۱۳۸۹). کتاب‌های درسی و هویت ملی (فراتحلیل مطالعه‌های انجام شده درباره کتاب‌های درسی)، مطالعات ملی، ۱۱ (۲ (۴۲))، صص. ۳۱-۵۴.

[۱۳] حاجیانی، ابراهیم (۱۳۷۹). تحلیل جامعه‌شناختی هویت ملی در ایران و طرح چند فرضیه، فصلنامه مطالعات ملی، س۲، ش۵، صص. ۱-۳.

[۱۴] حاجیانی، ابراهیم؛ محمدزاده، حمیدرضا (۱۳۹۴). بررسی تأثیر فضای مجازی (اینترنت) بر هویت ملی دانشجویان. مطالعات ملی، ۱۶(۱ (۶۱))، صص. ۶۷-۸۴.

[۱۵] حسینی انجدانی، مریم؛ درویزه، زهرا؛ خسروی، زهره؛ پورشهریاری، مه سیما (۱۳۸۸). نقش رسانه‌ها در رشد هویت ملی نوجوانان شهر تهران. پژوهش‌های ارتباطی (پژوهش و سنجش)، ۱۶(۲ (پیاپی ۵۸))، صص. ۳۹-۶۴.

[۱۶] حسینی، سیدبشیر (۱۳۹۲). سواد رسانه‌ای راهبرد استحکام هویت فردی و ملی. مطالعات ملی، ۱۴(۲ (۵۴))، صص. ۹۹-۱۲۰.

[۱۷] خدایاری، کلثوم؛ دانشور حسینی، فاطمه؛ سعیدی، حمیده (۱۳۹۳). میزان و نوع استفاده از شبکه‌های اجتماعی مجازی (مطالعه موردی: دانشجویان دانشگاه آزاد مشهد). فصلنامه پژوهش‌های ارتباطی، ۲۱(۱)، صص. ۱۹۲-۱۶۷.

[۱۸] دی اسمیت، آنتونی (۲۰۰۱). ناسیونالیسم: نظریه، ایدئولوژی، تاریخ، مترجم: منصور انصاری (۱۳۸۳)، تهران: مؤسسه مطالعات ملی، تمدن ایرانی، چاپ اول، صص. ۱۰-۱۵.

[۱۹] ربیعی، علی (۱۳۸۷). رسانه‌های نوین و بحران هویت. مطالعات ملی، ۹(۴ (۳۶))، صص. ۱۴۹-۱۷۶.

[۲۰] ربانی، علی؛ ربانی، رسول؛ حسنی؛ محمدرضا (۱۳۸۸). رسانه‌های جمعی و هویت ملی (مطالعه ی موردی دانشجویان دانشگاه اصفهان)، فصلنامه‌ی پژوهش‌های ارتباطی، سال ۱۶، شماره ۲ (پیاپی ۵۸)، صص. ۶۵-۹۳.

[۲۱] زارع کهن، نفیسه (۱۳۹۳). ارتقای سواد رسانه‌ای لازمه تحقق جامعه مدنی. فصلنامه علمی رسانه، ۲۵(۴)، صص. ۱۰۹-۱۱۹.

[۲۲] زاویه، سعید؛ عزیزی، سیده مهدیه (۱۳۹۲). تصاویر کتاب‌های درسی و رابطه آنها با هویت ملی و دینی مطالعه کتاب‌های اول و دوم دبستان. مطالعات ملی، ۱۴(۴ (۵۶))، صص. ۱۲۱-۱۴۰.

[۲۳] شیخاوندی، داور (۱۳۷۹). تکوین و تنفیذ هویت ایرانی، تهران، مرکز بازشناسی اسلام و ایران، شماره ۲، صص. ۲-۳.

[۲۴] فرهنگی، علی اکبر و نصیری، بهار (۱۳۸۷). «ارتباطات اجتماعی سالم با رسانه‌ها از طریق سواد رسانه‌ای»، پژوهشنامه سواد رسانه‌ای، انتشارات مرکز تحقیقات استراتژیک، مجمع تشخیص مصلحت نظام، شماره ۵، صص. ۳-۴.

[۲۵] قاسمی، طهمورث (۱۳۸۵). سواد رسانه‌ای، رویکرد جدید به نظارت. رسانه، ۷(۴)، صص. ۴۵-۵۸.

[۲۶] قربان‌زاده سوار، قربانعلی؛ رحمتی، مهدی؛ ناطقی، هاشم (۱۳۹۵). رسانه و هویت ملی (تأثیر رسانه بر شاخص‌های هویت ملی) رسانه و فرهنگ پژوهشگاه علوم انسانی و مطالعات فرهنگی، سال ششم، شماره ۱، صص. ۱۳۵-۱۱۳.

[۲۷] کاروانی، عبدالطیف (۱۳۹۷). تعامل در فضای مجازی و تأثیر آن بر هویت ملی دانشجویان دانشگاه سیستان و بلوچستان. مطالعات ملی، ۱۹(۲(۷۴))، صص. ۱۱۳-۱۲۸.

[۲۸] کوپایی، محمود؛ بشارتی فرد، اشرف (۱۳۹۸). بررسی رسانه‌های جمعی و تأثیر آن بر هویت اجتماعی جوانان (مطالعه موردی جوانان شهر اهواز)، کنگره بین‌المللی فرهنگ و اندیشه دینی، مؤسسه سفیران فرهنگی مبین، شماره ۳، صص. ۲-۱۰.

[۲۹] مازندرانی، حبیب‌الله (۱۳۹۶). تبیین ضرورت ارتقای سواد رسانه‌ای مبتنی بر سنتزپژوهی، ماهنامه علمی تخصصی مدیریت رسانه، شماره ۳۸، صص. ۲-۴.

[۳۰] معینی علمداری، جهانگیر (۱۳۸۳). هویت، تاریخ و روایت در ایران، تهران، مؤسسه تحقیقات و توسعه‌ی علوم انسانی، شماره ۱۰، صص ۱-۵.

[۳۱] مقدس‌زاده، حسن؛ صفاهیه، هاجر (۱۳۹۶). سواد رسانه‌ای و آگاهی از آسیب‌های شبکه‌های اجتماعی، مطالعات رسانه‌ای، سال ۱۲، صص. ۲۶-۳۰.

[۳۲] ملکی، امیر؛ عباس‌پور، علیرضا (۱۳۸۷). بررسی جامعه‌شناختی نگرش جوانان نسبت به هویت ملی و مؤلفه‌های آن (مطالعه موردی: جوانان ۱۶ تا ۲۹ ساله شهرستان رودسر – استان گیلان). دانش انتظامی، ۱۰(۲ (مسلسل ۳۹))، صص. ۱۵۲-۱۷۶.

[۳۳] مهدی‌زاده، سید محمد (۱۳۸۴). بازنمایی ایران در مطبوعات غرب، تهران: دانشگاه علامه طباطبایی، شماره ۱، صص. ۲-۶.

[۳۴] هزارجریبی، جعفر؛ صفری شالی، رضا (۱۳۹۱). آناتومی رفاه اجتماعی، تهران، انتشارات جامعه و فرهنگ، چاپ اول، صص. ۲۰-۲۵.

[35] Cho, Hyunyi . Cannon ,Julie . Lopez ,Rachel . Li ,Wenbo (2022). “Social media literacy: A conceptual framework”, Journals SAGE Pub, 10(3):3-4, doi. 10.1177/14614448211068530

[36] Derek Boles (2002). “The language of Media literacy: aglassory of terms”, 5(7):30-34.

[37] Gündüz, Uğur(2017). “The Effect of Social Media on Identity Construction”, Mediterranean Journal of Social Sciences, Vol 8, No 5 September 2017. doi: 10.1515/mjss-2017-0026.

[38] Livingstone, S. (2014). “Developing social media literacy: How children learn to interpret risky opportunities on social network sites”. Communications, 39(3):283-303.

[39] McCrone, David (1998). “The sociology of nationalism Tomorrow’s ancestors”. International library of sociology. London Routledge. 1st edition (August 20, 1998), 12-13.

[40] Newman, M. John (2015). “Image and identity: Media literacy for young adult Instagram users”, Visual Inquiry, 4(3):221–227, doi:10.1386/vi.4.3.221_1

[41] Oxstrand ,Barbro (2009). “Media Literacy Education- A discussion about media”, Nordmedia 09 Conference in Karlstad University, Sweden. August 13-15, 2009, revised after the conference, 5(4):2-6.

[42] Rani, Rohi (2022). “The Impact of Digital World on Our Identity”, The Creative Launcher, 7(1):27-32.

[43] Sherell A. McArthur (2019). “Centering Student Identities in Critical Media Literacy Instruction”, Journal of Adolescent & Adult Literacy, International Literacy Association, 62(6):686-689.

تأملی در ماهیت و معنای آسیب‌زایی فضای مجازی

محمود مختاری [۱]

[۱] استادیار فلسفه علم و فناوری، پژوهشکده مطالعات بنیادین علم و فناوری، دانشگاه شهید بهشتی، تهران
ma_mokhtari@sbu.ac.ir

چکیده

در خصوص آسیب‌زایی اینترنت و فضای مجازی، عبارات و مضامینی از این قبیل دیده (یا شنیده) می‌شود که «فضای مجازی بلای خانمان‌سوز است»، «شبکه‌های اجتماعی، باعث توسعه انحرافات جنسی شده‌اند»، و غیره. این رویکرد عام به اثرگذاری فضای مجازی، حاکی از باور به چیزی است که آن را، «عاملیت فضای مجازی» می‌نامیم. مباحث و مناقشات حوزه مطالعات نظری فناوری، نشان می‌دهد که تلقی فوق از ارتباط بین فناوری و جامعه، بسیار ساده‌انگارانه است. نه‌تنها پذیرش گزاره مزبور، به‌سهولت ممکن نیست بلکه بررسی و ارزیابی آن نیز با مشکلاتی مواجه است. هدف مقاله حاضر این است که با طرح و بررسی طیف رویکردهای مطرح درباره عاملیت اجتماعی فناوری (با تأکید بر فناوری فضای مجازی) و با توجه به نتایج سیاست‌گذارانه هر رویکرد، به این پرسش پژوهشی پاسخ دهد که «آیا و به چه معنا می‌توان از آسیب‌زایی فضای مجازی سخن گفت؟» ادعای مقاله آن است که در بین مهمترین دیدگاه‌ها (که شرح و بررسی خواهد شد)، «نظریه سیستمی» (یا همان سیستم‌های فنی-اجتماعی) هم از جنبه نظری و هم از جنبه سیاست‌گذارانه، پاسخ واقع‌بینانه‌تری برای پرسش پژوهشی این مقاله فراهم می‌کند.

کلمات کلیدی: فضای مجازی، تحولات اجتماعی، عاملیت فناوری، جبر فناوری، وساطت فناوری، کنش گر-شبکه، سیستم‌های فنی-اجتماعی.

۱ مقدمه

در رسانه‌های عمومی، عبارات و مضامینی از این قبیل دیده (یا شنیده) می‌شود که «فضای مجازی بلای خانمان‌سوز است»، «فضای مجازی، دین ما را نشانه گرفته است»، «شبکه‌های اجتماعی، باعث توسعه انحرافات جنسی شده‌اند»، «اینترنت رایگان، منجر به آشناشدن یک دختر نوجوان با پسری و باردار شدن او شد» و ... . این گزاره‌ها در خصوص آسیب‌زایی اینترنت و فضای مجازی، خواه بطور آگاهانه خواه به‌طور ناخودآگاه، حاکی از باور به چیزی است که آن را، عاملیت[۱] فضای مجازی می‌نامیم. فیلیپ بری (Brey, 2005)، استاد فلسفه و اخلاق فناوری در دانشگاه توئنته، در مقاله مهمی این سؤال اساسی را مطرح می‌کند

[1] agency

که «آیا مصنوعات[۲] [فناورانه] عاملیت دارند؟» و «آیا در شرح تحولات اجتماعی، باید به آنها [= مصنوعات فناورانه] عاملیت نسبت داد؟» همچنان که بری تصریح می‌کند «این، یک سؤال محوری برای مطالعات فناوری است». در واقع، مسئله عاملیت فناوری در اجتماع و پرسش از چگونگی ارتباط فناوری و اجتماع، موضوع بسیار مناقشه‌آمیزی است که پاسخ‌های مختلف و بسیار متنوعی را از سوی صاحب‌نظران حوزه مطالعات نظری فناوری دریافت کرده است.

آنچه که در بین عموم مردم (افراد غیرمتخصص) و حتی برخی از متخصصین حوزه‌های دیگر، متداول و مسبوق به سابقه است، عبارت از پذیرش اجمالی عاملیت فناوری (و از جمله عاملیت فناوری فضای مجازی) است؛ چنانکه بارها با این ادعای کلی مواجه شده‌ایم که:

- «ورود فناوری‌ها به جامعه، عامل مجموعه‌ای از تحولات اجتماعی است.» (تز عاملیت فناوری)

این ادعای عام را، که آن را «تز عاملیت فناوری» می‌نامیم، به یکی از دو روایت سخت و نَرم مطرح می‌کنند که به‌ترتیب، عبارتند از اعتقاد به انحصار عاملیت در فناوری‌ها یا باور به عاملیت توزیع‌شده فناوری‌ها در بستر اجتماعی. اگر قائلین جملات مذکور در ابتدای مقاله، فضای مجازی را به صورت عاملی مستقل و خودمختار[۳] تلقی کنند که نمی‌توان آن (و آسیب‌زایی آن) را کنترل کرد و به تنهایی و جبراً[۴]، سرنوشت جامعه را رقم می‌زند، در اینصورت معتقد به «تز سخت عاملیت فضای مجازی» هستند. اما اگر قائلین، علاوه بر عاملیت فضای مجازی، عاملیت انسان و اجتماع را نیز بپذیرند و آنرا انکار نکنند، در این صورت معتقد به «تز نرم عاملیت فضای مجازی» هستند. دیدگاه اخیر، طرفداران قابل توجهی دارد و می‌توان باور آنها را در خصوص کنترل آسیب‌های فضای مجازی در عباراتی از این قبیل سراغ گرفت که «از مسئولین می‌خواهیم که فضای مجازی را کنترل کنند» یا «باید در فضای مجازی، کسب‌وکارهای فرهنگی راه‌اندازی کنیم».

بدیهی است مواجهه دقیق و آکادمیک با مسئله عاملیت (و آسیب‌زایی) فناوری فضای مجازی، صرفاً از طریق رجوع به فهم عمومی از موضوع یا صورتبندی اجمالی از آن در قالب دو روایت سخت و نرم از تز عاملیت، امکان‌پذیر نیست و مستلزم شناخت دیدگاه‌های صاحبنظران مطالعات نظری فناوری برای اتخاذ چارچوبی مناسب و قابل دفاع است. هدف مقاله حاضر این است که با طرح و بررسی طیف رویکردهای مطرح درباره عاملیت اجتماعی فناوری (با تأکید بر فناوری فضای مجازی) و با توجه به نتایج سیاستگذارانه هر رویکرد، به این پرسش پژوهشی پاسخ دهد که «آیا و به چه معنا می‌توان از آسیب‌زایی فضای مجازی سخن گفت؟» ادعای مقاله آن است که در بین مهم‌ترین دیدگاه‌ها (که شرح و بررسی خواهد شد)، «نظریه سیستمی» (یا همان سیستم‌های فنی–اجتماعی) هم از جنبه نظری و هم از جنبه سیاست‌گذارانه، پاسخ واقع‌بینانه‌تری برای پرسش پژوهشی این مقاله فراهم می‌کند.

در بخش بعدی مقاله ضمن بررسی برخی نکات روش‌شناختی و مبانی نظری، نشان خواهیم داد که «تز عاملیت فناوری» به شکل اجمالی آن، با چه مشکلاتی مواجه است، سپس ضمن ارائه تصویری کلی از طیف

[2] artefacts
[3] autonomous
[4] deterministic

دیدگاه‌های مطرح در باب رابطه اجتماع و فناوری (با تأکید بر فناوری فضای مجازی)، در بخش‌های بعدی مقاله به تفصیل به رویکردهای مزبور و پاسخ هر یک از آنها به پرسش پژوهشی مقاله خواهیم پرداخت.

۲ مطالعات تجربی عاملیت فضای مجازی

در خصوص «تز عاملیت فناوری»، که در مقدمه مقاله معرفی شد، و نیز در خصوص مطالعات تجربی که درباره فضای مجازی انجام می‌شود، دو نکته اساسی در دو سطح «روش‌شناسی پژوهش» و نیز «مبانی نظری، پیش‌فرض‌ها و فرضیه پژوهش» قابل طرح است:

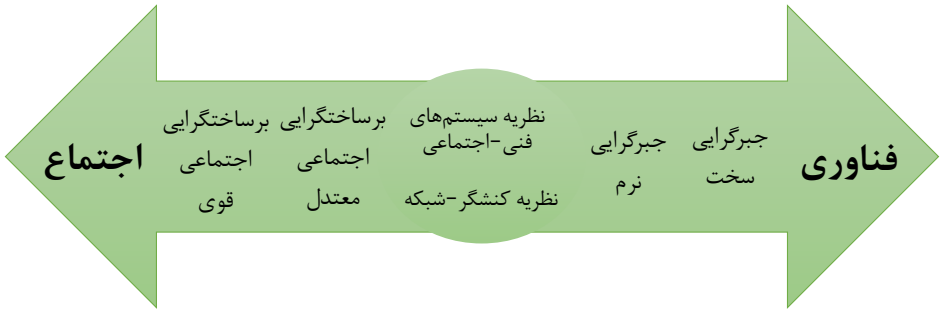
در سطح روش‌شناسی، نکته اصلی این است که اصولاً بررسی و ارزیابی «تز عاملیت فناوری» به شکل اجمالی آن، به‌سادگی امکان‌پذیر نیست. اولاً مصادیق «فناوری‌ها» بسیار گسترده و متنوع است و فناوری‌های مختلف دارای ویژگی‌های مختص خود هستند و بنابراین صدور یک حکم کلی برای «فناوری‌ها» مناقشه‌آمیز است، ثانیاً مفهوم «تحولات اجتماعی» نیز وسیع و پردامنه است و شامل پارامترهایی همچون باورها و مناسک، آداب و رسوم، سنت‌ها و آیین‌ها، زبان و گویش، پوشش و پیرایش، روابط و تعلقات، هویت، و .... می‌شود. ممکن است ادعا شود که می‌توان «تز عاملیت» را با بررسی تأثیرات یک «فناوری مشخص» بر جامعه، مورد ارزیابی قرار داد و از بین پارامترهای اجتماعی نیز فقط یک متغیر (یا چند مورد مشخص و مرتبط با یکدیگر) را مورد سنجش قرار داد. در اینجا ابتدا به چند مورد از مطالعات تجربی ارزشمندی که در کشور، بر اساس همین راهبرد انجام شده است اشاره می‌شود و سپس توضیح داده شد که چرا همچنان در سطح مبانی نظری، مشکل باقی است.

- سلطانی‌نژاد و همکاران (سلطانی‌نژاد، جمشیدی، شامیری، ۱۳۹۶) تأثیر فن‌آوری‌های اطلاعاتی را بر تحول مفهوم هویت ملی مورد بررسی قرار داده‌اند،
- کاروانی و عبدالطیف (کاروانی عبدالطیف، ۱۳۹۷) به بررسی تأثیر فضای مجازی بر هویت ملی، در بین دانشجویان دانشگاه سیستان و بلوچستان پرداخته‌اند،
- میمنت‌آبادی و تاجیک (میمنت‌آبادی تاجیک‌اسماعیلی، ۱۴۰۰) به مطالعه رابطه استفاده از شبکه‌های اجتماعی مجازی و تحول هویت قومی (زبانی و فرهنگی) در استان کردستان پرداخته‌اند،
- نعمتی‌فر و صفورایی (نعمتی‌فر، صفورایی‌پاریزی، ۱۳۹۸) تأثیر شبکه اجتماعی اینستاگرام را بر حجاب و پوشش کاربران زن مورد بررسی قرار داده‌اند،
- قراباغی و همکاران (قراباغی، یوسفی‌افراشته، صالحی، ۱۳۹۷) به‌جای یک پارامتر، چهار متغیر حجاب و عفاف، هویت دینی و فردی، تعامل با خانواده و نیز افسردگی و انزوا را مورد توجه قرار داده‌اند و پژوهشی در خصوص تأثیر شبکه‌های اجتماعی مجازی بر این چهار پارامتر، در بین جوانان استان همدان انجام داده‌اند،

- انصاری و همکاران (انصاری، کیانپور، عطایی، ۱۳۹۷) تأثیر استفاده از فضای مجازی را بر فرهنگ شفاهی در شهر اصفهان بررسی کرده‌اند،
- خانمحمدی و غازی (خانمحمدی، غازی، ۱۳۹۹) آسیب‌های زنان در اینستاگرام را مطالعه کرده‌اند.

آن مشکل جدی که در سطح مبانی نظری وجود دارد این است که مطالعات تجربی در خصوص ارتباط بین فضای مجازی و متغیرهای اجتماعی (همچون موارد فوق‌الذکر)، گرچه نوعاً و بسته به جامعه آماری و دامنه انجام تحقیق و نیز میزان دقت مطالعه و نتایج آن، پژوهش‌های بسیار ارزشمندی هستند در نهایت، آنچه که نشان می‌دهند و تأیید می‌کنند یک ارتباط آماری معنادار (مثبت یا منفی) بین استفاده از فضای مجازی و یک پارامتر اجتماعی است. بنابراین یکی از پیش‌فرض‌های بنیادین این نوع مطالعات آن است که می‌توان بین فناوری (و از جمله فناوری فضای مجازی و میزان استفاده از آن) از یکسو و افراد جامعه و تحولات اجتماعی از سوی دیگر، جدایی و تفکیک قائل شد و یکی را پارامتر مستقل و دیگری را متغیر وابسته در نظر گرفت. این در صورتی است که در حوزه مطالعات نظری فناوری، اصولاً چنین پیش‌فرضی به‌هیچ‌وجه بدیهی نیست و محل مناقشه است. بنابراین به نظر می‌رسد به‌جای اینکه نتایج پژوهش‌های نوعی مزبور را تصاویری کم‌وبیش واقعی از «تحولات اجتماعی ناشی از فضای مجازی» تلقی کنیم، دقیق‌تر آن است که آنها را به‌صورت چشم‌انداز «تحولات فناورانه–اجتماعی، در بستر فضای مجازی» تفسیر کنیم.

با توجه به این نکات، لازم است یک چارچوب نظری از بین دیدگاه‌های مطرح در حوزه مطالعات نظری فناوری، اتخاذ شود. طیف دیدگاه‌های متنوعی که در خصوص تز عاملیت فناوری و ارتباط بین فناوری و اجتماع مطرح است، بطور شماتیک در شکل ۱ نشان داده شده است. در ادامه مقاله، ضمن شرح اختصاصی هر یک از این رویکردها در باب عاملیت فناوری فضای مجازی، تبعات آنها را برای سیاست‌گذاری فضای مجازی نیز مورد بررسی قرار خواهیم داد.



شکل ۱: نمایش شماتیک طیف نظریه‌های عاملیت فناوری و اجتماع (تألیف نگارنده)

۳ جبر فضای مجازی

دیدگاه جبرگرایی فناورانه[5]، در مقاله کلاسیک رابرت هیلبرونر (Heilbroner, 1967) معرفی شد. روایت سخت از این رویکرد، در شکل ۱ به‌عنوان افراطی‌ترین رویکرد در خصوص عاملیت فناوری، در سمت راست طیف نشان داده شده است. جبرگرایی سخت فناورانه عبارت از این ایده است که صرفاً فناوری است که عاملیت دارد. در واقع مطابق این دیدگاه، فناوری و ویژگی‌های فیزیکی و ساختاری آن، «به‌خودی‌خود» و «در هر پس‌زمینه» و هر موقعیت اجتماعی که مورد استفاده قرار بگیرند، عاملِ ایجاد تغییرند. به‌عبارت دیگر، اگر فناوری به‌گونه‌ای طراحی شده باشد که منجر به تغییر و تحول خاصی در اجتماع شود، اجتماع نمی‌تواند در برابر ویژگی‌های ساختاری و طراحی فناوری مقاومت کند و اصولاً چنین مقاومتی هیچ نتیجه‌ای در بر نخواهد داشت. متداول‌ترین مثال برای این رویکرد، طراحی تبعیض‌آمیز یا ضدنژادی پل‌های لانگ‌آیلند است که لانگدون وینر (Winner, 1980) در مقاله معروف خود به تحلیل آن پرداخته است. این پل‌ها که بر روی جاده متصل‌کننده نیویورک به ساحل تفریحی لانگ‌آیلند احداث شده بودند، ارتفاعی کمتر از اندازه معمول داشتند به گونه‌ای که مانع عبور اتوبوس از زیر پل و دسترسی به ساحل می‌شدند. این پل‌ها عملاً عامل محرومیت سیاهان بودند زیرا آنها فاقد اتومبیل شخصی بودند و صرفاً از اتوبوس استفاده می‌کردند.

بر اساس روایت سخت از جبرگرایی فضای مجازی، این واقعیت که فضای مجازی آسیب‌هایی در پی دارد صرفاً ناشی از ویژگی‌های ساختاری (شامل همه جنبه‌های فناورانه سخت‌افزاری، نرم‌افزاری، زیرساختی و ...) این فناوری است و بنابراین در هر اجتماع و موقعیت اجتماعی متفاوتی هم که مورد استفاده قرار بگیرد، آن آسیب‌ها را دارد. بدین ترتیب طرفداران این دیدگاه، استفاده از فضای مجازی را اصطلاحاً «از باب اکل میته» و از روی ناچاری می‌پذیرند. یعنی صرفاً به اندازه ضرورت و برای رفع نیازهای واجب که از طریق غیرمجازی قابل برآوردن نیستند می‌توان از فضای مجازی استفاده کرد. بدیهی است روایت سخت از جبرگرایی فضای مجازی، در حوزه سیاست‌گذاری نیز منجر به سیاست‌های انقباضی و نیز محدودکردن شدید فضای مجازی خواهد شد.

بر اساس روایت سخت از جبرگرایی فضای مجازی، این واقعیت که فضای مجازی آسیب‌هایی در پی دارد صرفاً ناشی از ویژگی‌های ساختاری (شامل همه جنبه‌های فناورانه سخت‌افزاری، نرم‌افزاری، زیرساختی و ...) این فناوری است و بنابراین در هر اجتماع و موقعیت اجتماعی متفاوتی هم که مورد استفاده قرار بگیرد، آن آسیب‌ها را دارد. بدین ترتیب طرفداران این دیدگاه، استفاده از فضای مجازی را اصطلاحاً «از باب اکل میته» و از روی ناچاری می‌پذیرند. یعنی صرفاً به اندازه ضرورت و برای رفع نیازهای واجب که از طریق غیرمجازی قابل برآوردن نیستند می‌توان از فضای مجازی استفاده کرد. بدیهی است روایت سخت از جبرگرایی فضای مجازی، در حوزه سیاست‌گذاری نیز منجر به سیاست‌های انقباضی و نیز محدودکردن شدید فضای مجازی خواهد شد.

اما مطابق روایت نرم از جبرگرایی فناورانه، گرچه فناوری و ویژگی‌های فیزیکی و ساختاری آن، عاملیت دارند در عین حال، موقعیت‌ها و شرایط اجتماعی مختلف به‌کارگیری فناوری، منجر به تأثیرات و تحولات

[5] technological determinism

متفاوتی می‌شود. بنابراین غیر از فناوری، بستر اجتماعی استفاده از فناوری نیز عاملیت دارد. طرفداران این دیدگاه معتقدند که در مثال پل‌های لانگ‌آیلند، گرچه اتوبوس سیاهان به هیچ طریقی نمی‌توانست از زیر پل عبور کند، اصولاً استفاده انحصاری سیاهان از اتوبوس ناشی از آن بستر اجتماعی–اقتصادی بود که فناوری در آن بستر عاملیت داشت و بنابراین در این مثال، فناوری فی‌نفسه و به‌تنهایی عامل تحول اجتماعی نبود.

پذیرش رویکرد نرم به جبرگرایی فضای مجازی، حداقل به دو دلیل می‌تواند منجر به وضعیت متفاوتی در این زمینه شود. اول اینکه مطابق این دیدگاه، آنچه که در یک «بستر کاربری» فضای مجازی، آسیب‌زا تلقی می‌شود در یک بستر کاربری متفاوت لزوماً آسیب‌زا نیست. به عنوان مثال، محتوای آسیب‌زا برای کودکان، لزوماً برای بزرگسالان یا برای کارشناسان و پژوهشگرانی که حوزه کاری آنها مطالعات اجتماعی، یا مشخصاً آسیب‌های اجتماعی است آسیب‌زا نیست. دوم اینکه بر اساس این دیدگاه، آسیب‌های فضای مجازی در یک «بستر اجتماعی» خاص اتفاق می‌افتند و بنابراین حتی برای بستر کاربری واحد (مثلاً کاربرانی از رده سنی مشخص یا با نوع کاربری یکسان) چه بسا آسیب‌های فضای مجازی ناشی از این باشد که کاربران، آن را در یک خلأ یا نقص سیاست‌گذاری اجتماعی، فرهنگی، سیاسی و ... مورد استفاده قرار می‌دهند. بدین ترتیب، سیاست‌گذاری فضای مجازی نیز در چنین رویکردی، منجر به پیشنهادهای تا حدی متفاوت خواهد شد که ناشی از توجه به بسترهای کاربری (مثلاً محدودسازی سنی، اینترنت طبقاتی یا شغلی و ...) و نیز بسترهای اجتماعی (مثلاً تلاش برای رفع خلأ رسانه‌های سنتی همچون صداوسیما، تقویت تربیت دینی در مدارس، مساجد و هیئات، و ...) است.

۴ برساختن اجتماعی فضای مجازی

برساخت‌گرایی اجتماعی[۶] فناوری در مقاله ترور پینچ و ویبه بایکر (Pinch & Bijker, 1984) معرفی شد. روایت قوی از این دیدگاه، در شکل ۱ به‌عنوان افراطی‌ترین رویکرد در خصوص عاملیت اجتماع، در سمت چپ طیف نشان داده شده است. برساختگرایی اجتماعی قوی شامل این ادعاست که اصولاً فناوری، عاملیتی ندارد. هر جامعه یا گروه اجتماعی، بر اساس «تعبیر»ی که از یک «مشکل» یا نیاز اجتماعی خود دارد به ابداع یک فناوری می‌پردازد که صرفاً برای همان اجتماع، «راه‌حل» تلقی می‌شود زیرا افراد و گروه‌های مختلف، تعبیرهای مختلفی از راه‌حل مشکل خواهند داشت. بدین ترتیب، گروه‌های اجتماعی مختلف می‌توانند طراحی‌ها و ساختارهای با ویژگی‌های فیزیکی متفاوتی برای یک نوع از فناوری ارائه کنند. بنابراین ویژگی‌های فیزیکی و ساختاری یک فناوری، فی‌نفسه هیچ اصالت یا عاملیتی ندارد و کاملاً وابسته به تعبیر اجتماعی آن است.

در رویکرد برساخت‌گرایی اجتماعی قوی به فضای مجازی، اصولاً نمی‌توان آسیب‌زایی را به فضای مجازی نسبت داد. آنچه که آسیب فضای مجازی برای «گروه اجتماعی ما» تلقی می‌شود، ناشی از تعبیر بدیل یک «گروه اجتماعی دیگر» از «نیاز» و «راه‌حل» است که منجر به طراحی فناوری فضای مجازی موجود شده است و به تعبیر ما آسیب می‌زند. از طرفی طبق این رویکرد، اگر در جامعه ما یک (یا بیش از یک) گروه

[6] social constructivism

اجتماعی، دارای همان نیازها، تعابیر و انتخاب‌هایی باشد که منجر به فضای مجازی موجود شده است، آسیبی از فضای مجازی نخواهید دید. به علاوه مطابق این دیدگاه، هر جامعه‌ای می‌تواند فضای مجازی خود را متناسب با نیازهای خود طراحی کند زیرا از پیش، هیچ ویژگی یا ساختار واحد و معیّنی تحت عنوان فناوری فضای مجازی وجود ندارد. این دیدگاه در عرصه سیاست‌گذاری فضای مجازی می‌تواند منجر به برنامه شبکه ملی اینترنت شود، مشابه آنچه که اینترنت چینی نامیده می‌شود. در این رویکرد، «فضای مجازی» وابسته به تعبیر اجتماعی از آن است و بنابراین مثلاً «داشتن اینترنت یا فضای مجازی»، هیچ استلزامی برای داشتن شبکه‌های اجتماعی غربی ندارد.

اما بر اساس برساخت‌گرایی اجتماعی معتدل، علاوه بر تعبیر و تفسیر یا انتخاب گروه‌های اجتماعی، می‌توان برای فناوری و ویژگی‌های ساختاری آن، نوع محدودی از عاملیت را در نظر گرفت. در واقع در این روایت از برساخت‌گرایی اجتماعی، ویژگی‌های فناوری دارای نقش و تأثیر هستند گرچه فناوری همچنان فاقد عاملیت مستقل از عاملیت اجتماع است و نقشی که ایفا می‌کند تجسّم تعابیر، انتخاب‌ها، و سیاست‌های گروه‌های اجتماعی است. بنابراین اگر رویکرد برساختگرایی اجتماعی معتدل به فضای مجازی را بپذیریم نمی‌توانیم بالکل، از انتساب آسیب‌زایی به فضای مجازی دست برداریم ولی در نهایت آن را ناشی از تقابل و تعارض انتخاب‌ها و جهت‌گیری‌ها در نظر خواهیم گرفت. در حوزه سیاست‌گذاری فضای مجازی، تفاوت رویکرد معتدل به برساخت‌گرایی اجتماعی در مقایسه با رویکرد قوی، این است که در اینجا نمی‌توان گفت که ویژگی‌های ساختاری فناوری فضای مجازی، هیچ محلی از اعراب ندارند و هر تعبیری از فضای مجازی ممکن است. در واقع مطابق رویکرد معتدل، ما امکان‌های محدودتری برای طراحی فضای مجازی بدیل داریم گرچه همه این امکان‌ها و آن محدودیت‌ها وابسته به تعابیر، نیازها و انتخاب‌های ماست.

۵ عملگر فضای مجازی

مهم‌ترین پیش‌فرض در هر دو دیدگاه جبرگرایی فناورانه و برساخت‌گرایی اجتماعی فناوری، تفکیک و جدایی بین جامعه و فناوری بود چنانکه گویی «جامعه»، به یک شکل خاص و مشخص وجود دارد و دارای حدود و ثغور معیّنی است که «فناوری» از بیرون، وارد آن می‌شود یا اینکه جامعه، آن را برمی‌سازد. اما در نظریه کنشگر–شبکه[۷] که توسط برونو لتور و همکارانش در مرکز جامعه‌شناسی نوآوری پاریس (Callon, 1987; Callon & Latour, 1992; Callon, Law, & Rip, 1986; Latour, 1987) ارائه شد، اساساً به‌جای تفکیک و تمایز بین فناوری و مصنوعات فناورانه از یکسو و اجتماع و کنش‌های اجتماعی از سوی دیگر، نقش و وزن کاملاً یکسان، همگن و متقارنی را در شبکه‌ای از کنش‌ها و تحولات، به فناوری و اجتماع نسبت می‌دهند. در واقع، در این دیدگاه همهٔ کنشگران (شامل مؤلفه‌های طبیعی و فناورانه، و نیز انسانی و اجتماعی) «عملگر[۸]»های یک شبکه هستند و از این جهت، هیچ تمایزی با یکدیگر ندارند. در خصوص نسبت‌دادن عاملیت به فناوری و اجتماع نیز باید توجه داشت از آنجا که این دو نوع مؤلفه در شبکه، هیچ تفاوت ماهوی با هم

[7] actor-network theory
[8] actant

ندارند بنابراین عاملیت یا عدم‌عاملیت آنها، از پیش قابل تعیین نیست و نسبت‌دادن عاملیت فقط از طریق تحلیل «کلّ موقعیت»ی که عملگر در آن عمل می‌کند ممکن است.

بر اساس رویکرد کنشگر–شبکه به فضای مجازی، نمی‌توان هیچ تمایزی بین نقش و عاملیت انسان و اجتماع و فناوری فضای مجازی (شامل سخت‌افزار و زیرساخت، نرم‌افزار و محتوا و ...) قائل شد و هر یک از این مؤلفه‌ها دقیقاً همچون دیگری، یک عملگر فضای مجازی است و هویت خود را کاملاً از شبکه عملگران فضای مجازی (شامل انسان و فناوری) می‌گیرد. بنابراین در این چارچوب نظری، اگر استفاده از فضای مجازی موجب آسیب‌زایی است، این آسیب را نه می‌توان به فضای مجازی نسبت داد و نه به اجتماع، بلکه آسیب‌زایی را باید محصول کل موقعیتی دانست که از تعامل شبکه‌ای همه کنشگران یا عملگرهای (فناورانه و اجتماعی) فضای مجازی شکل گرفته است. بدین ترتیب در عرصه سیاست‌گذاری فضای مجازی نیز، این رویکرد مستلزم نگاهی شبکه‌ای است و نمی‌توان با یک نگاه موضعی و تک‌ساحتی به ایجاد تغییر در بخش‌های فناورانه فضای مجازی یا بخش‌های اجتماعی–فرهنگی آن دست زد زیرا نتیجه آن، می‌تواند کل شبکه را دستخوش تحول کند.

۶ سیستم فنی–اجتماعی فضای مجازی

دیدگاه سیستمی به رابطه فناوری و اجتماع[۹] توسط توماس هیوز (Hughes, 1969, 1987) معرفی شد. در این رویکرد، هر فناوری را به صورت یک سیستم فناورانه تعریف می‌کنند که شامل مصنوع فناورانه، ساختار سیستم و قوانین طبیعی، فرایندها، افراد و نظام سازمانی، و دانش و مهارت‌هاست. مهم‌ترین وجه تمایز رویکرد هیوز در مقایسه با رویکردهای قبلی، علاوه بر نگاه سیستمی به فناوری و اجتماع، این است که عاملیت فناوری و اجتماع را تابع زمان تحول سیستم می‌داند. مطابق دیدگاه هیوز، رابطه فناوری و اجتماع را می‌توان به رابطه طفل و والدین تشبیه کرد زیرا سیستم فناورانه در ابتدای ابداع و معرفی (دوره طفولیت[۱۰]) بیشتر تحت تأثیر اجتماع است ولی هنگامیکه به رشد و توسعه‌یافتگی (دوره بلوغ[۱۱]) می‌رسد، اجتماع را تحت تأثیر خود قرار می‌دهد. هیوز معتقد است در دوره اول، عاملیت اجتماع غلبه دارد و نظریه برساخت‌گرایی اجتماعی (معتدل)، توصیف بهتری برای وضعیت است اما در دوره دوم که سیستم فناورانه، تکانه (یا مومنتوم) کافی بدست می‌آورد به‌سختی قابل کنترل و تغییر مسیر خواهد بود و بنابراین عاملیت فناوری غلبه دارد و نظریه جبرگرایی فناورانه (نرم)، توصیف درست‌تری از اوضاع بدست می‌دهد.

فلاسفه فناوری مکتب هلندی (Vermaas, Kroes, van de Poel, Franssen, & Houkes, 2011) رویکرد سیستمی با ارتباط فناوری و اجتماع را تحت عنوان نظریه سیستم‌های فنی–اجتماعی توسعه دادند. در این رویکرد، همچون دیدگاه هیوز و بر خلاف نظریه کنشگر–شبکه، تمایز بخش‌های فناورانه از بخش‌های اجتماعی سیستم، امکان‌پذیر است ولی همچنان باید این دو بخش را در ارتباط با یکدیگر و صرفاً در قالب یک سیستم فنی–اجتماعی، تعریف و ترسیم و درک کرد. سیستم فنی–اجتماعی، سیستم ترکیبی (یا دورگه)

[9] sociotechnical system
[10] infancy
[11] maturity

شامل دو دسته مؤلفه است: یکی مؤلفه‌های فنی که از قوانین طبیعت پیروی می‌کنند و توسط علوم طبیعی و مهندسی توصیف یا طراحی می‌شوند؛ و دیگری مؤلفه‌های انسانی–اجتماعی که قادر به درک قوانین و هنجارها و متابعت (عدم متابعت) از آنها هستند و توسط علوم اجتماعی و انسانی توصیف یا طراحی می‌شوند.

دستاورد به‌کارگیری رویکرد سیستمی و زمانمند هیوز برای فضای مجازی این است که تعیین می‌کند که عاملیت فناوری و اجتماع در هر مرحله از تحول و توسعه سیستم، به چه میزان است. بنابراین برای بحث در خصوص آسیب فضای مجازی و نیز سیاست‌گذاری در این حوزه چشم‌انداز واقعی‌تری نسبت به رویکردهای قبلی بدست می‌دهد. مثلاً اگر یک اپلیکیشن یا شبکه اجتماعی در فضای مجازی، در مراحل ابتدایی ابداع و معرفی آن به اجتماع باشد طبق دیدگاه هیوز دارای تکانه اندکی است و تأثیرگذاری بر آن (از جمله توقف یا تغییر مسیر آن) انرژی کمتری می‌طلبد. اما اگر کاربران زیادی به این اپلیکیشن یا شبکه اجتماعی مجازی، متصل شوند و از امکانات و قابلیت‌های آن رضایت داشته باشند و آن را به بقیه نیز معرفی کنند (اثر شبکه (Volti, 2017)) اپلیکیشن مزبور دارای تکانه بالایی می‌شود و بنابراین عاملیت و تأثیر بالایی در جامعه خواهد داشت و بنابراین توقف آن، اگر غیرممکن نباشد بسیار مشکل و مستلزم هزینه و انرژی زیادی خواهد بود.

از دیدگاه نظریه سیستم‌های فنی–اجتماعی نیز، عاملیت فضای مجازی و اجتماع را باید در یک سیستم مورد بررسی قرار داد با تمرکز بر این نکته که بخش فنی فضای مجازی، تابع قوانین علوم طبیعی و مهندسی و اصول معماری فضای مجازی و شبکه‌سازی و ... است ولی بخش انسانی به این سادگی قابل کنترل و به قید درآوردن نیست. عاملیت بخش انسانی در سیستم فنی–اجتماعی فضای مجازی می‌تواند کلّ سیاست‌گذاری و نیز مهندسی بخش فنی را بی‌اثر یا کم‌اثر کند. تنها راه هدایت بخش انسانی، به‌کارگیری یافته‌های علوم انسانی–اجتماعی و تجربه‌های جهانی در این زمینه است. البته همچنان ممکن است کاربر و جامعه ایرانی، به خاطر تفاوت‌های فرهنگی، اجتماعی و سیاسی، رفتار و عاملیتی متفاوت نسبت به کاربران جوامع دیگر داشته باشد.

۷ نتیجه‌گیری

چنانکه در این مقاله نشان داده شد مطالعات تجربی درباره تأثیرات اجتماعی فضای مجازی مبتنی بر برخی مبانی نظری، پیش‌فرض‌ها و فرضیه‌هایی است که در حوزه مطالعات نظری فناوری محل مناقشه است. بنابراین لازم است تز عاملیت فضای مجازی از منظر رویکردهای مختلف ناظر به رابطه فناوری و اجتماع، مورد بررسی قرار بگیرد و پاسخ هر یک از آنها به مسئله خاص فضای مجازی و آسیب‌زایی اجتماعی آن، استنباط شود. مطالعه حاضر نشان می‌دهد که رویکرد سیستمی زمانمند به فضای مجازی، بهترین پاسخ را از منظر جامعیت و واقع‌بینی فراهم می‌کند. اهمیت اتخاذ این رویکرد در آن است که:

- عاملیتی که برای فضای مجازی در نظر می‌گیرد در مراحل مختلف از تحول و توسعه سیستم، متفاوت است و بنابراین برای بررسی آسیب‌زایی فضای مجازی و سیاست‌گذاری در این خصوص، چشم‌انداز واقعی‌تری نسبت به رویکردهای دیگر، پیشِ روی قرار می‌دهد. مثلاً آن شبکه اجتماعی مجازی که در مراحل ابتدایی است عاملیت کمتری دارد نسبت به شبکه اجتماعی‌ای که کاربران زیادی دارد و

توقف یا تغییر مسیر آن، تقریباً غیرممکن یا بسیار مشکل است.

- نکته دیگر در رویکرد سیستم‌های فنی-اجتماعی این است که اصولاً عاملیت فضای مجازی را در چارچوب یک سیستم متشکل از بخش‌های فنی و اجتماعی مورد ارزیابی قرار می‌دهد که هر یک از این دو بخش سیستم نیز تابع قوانین خاص خود هستند. بخش فنی فضای مجازی، تابع قوانین علوم طبیعی و مهندسی و اصول معماری فضای مجازی و شبکه‌سازی و ... است و بخش انسانی نیز تابع علوم انسانی و اجتماعی است. مطابق این رویکرد به عاملیت فضای مجازی، میزان عاملیت فضای مجازی اصولاً وابسته به نحوه تعامل بخش انسانی و اجتماعی سیستم است و عاملیتِ بخش انسانی، ممکن است کلّ سیاست‌گذاری و نیز مهندسی بخش فنی را بی‌اثر یا کم‌اثر کند. به عبارت دیگر، بخش انسانی سیستم را نمی‌توان از طریق مهندسی «به قید» درآورد و تنها راه کنترل آن، به‌کارگیری یافته‌های علوم انسانی-اجتماعی و تجربه‌های جهانی در این زمینه است. گرچه همچنان ممکن است کاربران در یک جامعه، به خاطر تفاوت‌های فرهنگی، اجتماعی و سیاسی، رفتار و عاملیتی متفاوت نسبت به کاربران جوامع دیگر داشته باشد.

بدین ترتیب بر اساس رویکرد سیستمی، آسیب‌زا بودن/نبودن فضای مجازی همواره و صرفاً با توجه به بستر یا چارچوب اجتماعی، فرهنگی، سیاسی و ... بخش انسانی (جامعه کاربران و سیاستگذاران)، قابل ارزیابی است. با تغییر هر بخش از سیستم، فضای مجازی می‌تواند آسیب‌زا شود/نشود. هر تغییر یا کنش انسانی و اجتماعی در سیستم، می‌تواند آسیب‌زایی فضای مجازی را کاهش/افزایش دهد؛ مثلاً چه بسا در بستر یک (یا مجموعه‌ای از چند) سیاست‌گذاری یا کنش خاص سیاستگذاران و کارگزاران، آسیب‌زایی فضای مجازی افزایش/کاهش یابد.

مراجع

[۱] انصاری، کیانپور، عطایی (۱۳۹۷). تحلیل جامعه‌شناختی تأثیر استفاده از فضای مجازی بر فرهنگ شفاهی (مورد مطالعه: شهر اصفهان).

[۲] خانمحمدی، غازی (۱۳۹۹). آسیب‌های اجتماعی نوظهور زنان در فضای مجازی با تأکید بر اینستاگرام. دوفصلنامه مطالعات اسلامی آسیب‌های اجتماعی، ۲(۱)، ۱۲۹-۱۴۴.

[۳] سلطانی‌نژاد، جمشیدی، شامیری (۱۳۹۶). نقش فن‌آوری اطلاعات بر تحول مفهوم هویت ملی. فصلنامه علمی مطالعات قدرت نرم، ۷(۲)، ۲۲-۴۱.

[۴] قراباغی، یوسفی‌افراشته، صالحی (۱۳۹۷). تأثیر شبکه‌های اجتماعی مجازی بر حجاب و عفاف، هویت دینی و فردی، تعامل با خانواده و افسردگی و انزوا در بین جوانان. مطالعات راهبردی ورزش و جوانان، ۴۲(۱۷)، ۳۲۸-۳۴۶.

[۵] کاروانی، عبدالطیف (۱۳۹۷). تعامل در فضای مجازی و تأثیر آن بر هویت ملی دانشجویان دانشگاه سیستان و بلوچستان. مطالعات ملی، ۷۴(۱۹)، ۱۱۳-۱۲۸.

[۶] میمنت‌آبادی، تاجیک‌اسماعیلی (۱۴۰۰). رابطه استفاده از شبکه‌های اجتماعی مجازی با تحول هویت زبانی و فرهنگی در استان کردستان. مطالعات فرهنگ-ارتباطات، ۸۶(۲۲)، ۱۸۳-۲۱۲.

[۷] نعمتی‌فر، صفورایی‌پاریزی (۱۳۹۸). بررسی تأثیر استفاده از شبکه‌های اجتماعی بر حجاب و پوشش کاربران با تأکید بر ابعاد دین‌داری (مورد مطالعه: کاربران زن شبکه اجتماعی اینستاگرام). دین و ارتباطات (دانشگاه امام صادق/نامه صادق)، ۲۶(۵۵)، ۳۳۵-۳۶۲.

[8] Brey, P. (2005). Artifacts as Social Agents Inside the Politics of Technology. Agency and Normativity in the Co-Production of Technology and Society (pp. 61-84): Amsterdam University Press.

[9] Callon, M. (1987). Society in the making: The study of technology as a tool for sociological analysis. The social construction of technological systems: New directions in the sociology and history of technology, 83-103.

[10] Callon, M., & Latour, B. (1992). Don't throw the baby out with the bath school! A reply to Collins and Yearley. Science as practice and culture, 343(368).

[11] Callon, M., Law, J., & Rip, A. (1986). Mapping the Dynamics of Science and Technology Sociology of Science in the Real World. Basingstoke, UK: MacMillan.

[12] Heilbroner, R. L. (1967). Do machines make history? Technology and culture, 8(3), 335-345.

[13] Hughes, T. (1969). Technological momentum in history: Hydrogenation in Germany 1898-1933. Past & Present(44), 106-132.

[14] Hughes, T. (1987). The evolution of large technological systems. The social construction of technological systems: New directions in the sociology and history of technology, 82, 51-82.

[15] Latour, B. (1987). Science in action: How to follow scientists and engineers through society: Harvard university press.

[16] Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. Social studies of science, 14(3), 399-441.

چالش‌های رفتاری به‌کارگیری کلان‌داده در فضای سایبر

سید کمال واعظی[۱]، فرانک پاشایی[۲]

[۱] دانشیار، دانشکدگان مدیریت دانشگاه تهران، تهران
vaezi_ka@ut.ac.ir
[۲] دانشجوی دکتری، پردیس بین‌المللی کیش دانشگاه تهران، کیش
faran.pahaei@gmail.com

چکیده

این مقاله تلاش می‌کند تا سهمی انتقادی در بحث چالش‌های رفتاری بکارگیری کلان‌داده در فضای سایبر ارائه دهد و برای بررسی این موضوع از بینش‌های اقتصاد رفتاری استفاده کرده تلنگرها را به عنوان ابزاری برای اصلاح چالش‌های رفتاری معرفی می‌کند. علاوه بر مطالعه فرصت‌ها و چالش‌های استراتژی‌های کلان‌داده برای دولت، جامعه و سیاست‌گذاری، این مقاله بررسی می‌کند که چگونه کلان‌داده پتانسیل سوءاستفاده یا همسوبودن با اهداف سیاست‌گذاران را دارد یا ممکن است تأثیرات منفی بر جامعه داشته باشد و نتیجه‌گیری می‌کند با اینکه کلان‌داده یک جایگزین کاربردی در محیط‌های نامطمئن تصمیم‌گیری با ایجاد بینش عمیق‌تر در مورد مسائل اجتماعی و تصمیم‌گیری است، ممکن است نتواند بین مهم‌ترین ارزش‌های انسانی مانند حریم خصوصی، برابری، محرمانه بودن، شفافیت، هویت، انتخاب آزاد و تبعیض و استفاده قانع‌کننده از کلان‌داده تعادل برقرار کند. این موضوع در کشورهای درحال‌توسعه به‌دلیل شکاف دیجیتالی در کاربردهای کلان‌داده، با خطر افزایش نابرابری بین نهادهایی که به داده‌ها دسترسی دارند و آنان که دسترسی ندارند، جدی‌تر است. این تحقیق، چهار نوع تلنگر سنتی، دیجیتال، بیش‌تلنگر و تاریک در سه ساختار مختلف سوگیری بازخورد، طرفدار اجتماع و طرفدار خود معرفی می‌کند تا راه‌حل مناسب چالش‌های رفتاری نسبت به کلان‌داده را معرفی کند و در انتها بر بیش‌تلنگرها تأکید دارد.

کلمات کلیدی: کلان‌داده، تلنگر، سوگیری شناختی، رفتار، فضای سایبر.

۱ مقدمه

کلان‌داده (Big Data) به حجم بسیار بالایی از داده‌های متنوع اشاره دارد که از منابع مختلف تولید، پردازش و متعاقباً با سرعت زیاد مبادله می‌شود. هر کلیک، اشتراک‌گذاری، پسند (Like)، کلان‌داده ایجاد می‌کند. هر روز، میلیاردها نفر که از طریق دستگاه‌های خود و اینترنت در تعامل هستند، در خلق دنیایی از اطلاعات ارزشمند مشارکت می‌کنند [۲۷]. در سال ۲۰۲۳، هر روز تقریباً ۷۷.۳۲۸ میلیون ترابایت داده با سرعت فعلی ایجاد می‌شود [۱۹]. کلان‌داده به عنوان یک برادر بزرگ ما را تماشا می‌کند [۲۵] و مفهوم حفظ حریم

خصوصی تغییر کرده است زیرا از طریق پردازش داده‌ها، مکان سکونت، سلیقه و علایق، ذهنیت و سبک زندگی ما به خوبی شناسایی می‌شود. نهادهایی که نحوه تولید اطلاعات از داده‌ها را کشف می‌کنند، بیشتر از خودمان در مورد ما می‌دانند و می‌توانند با ایجاد تکنیک‌هایی ما را به مسیری که می‌خواهند سوق دهند [۲]. این موضوع در تبلیغات هدفمند و شخصی‌شده برای ما در صفحات وب و گوشی‌های هوشمند که براساس داده‌های شخصی و کلان که از جستجوهای قبلی جمع‌آوری شده‌اند، منعکس می‌شود. بنابراین، داده‌ها فقط اطلاعات جمع‌آوری شده ساده در مورد موضوعات مختلف نیستند، بلکه انقلاب اطلاعات انبوه طبقه‌بندی‌شده، سازمان‌یافته و ذخیره‌شده هستند، انقلابی که نحوه زندگی، کار و تفکر ما را متحول می‌کند [۵۲]. سهم کلیدی کلان‌داده توانایی کشف همبستگی‌های ناشناخته بین مجموعه داده‌هایی است که با ارزیابی عادی انسان قابل کشف نیستند برای مثال، کلان‌داده حاصل از ضبط، پردازش و تجزیه‌وتحلیل محتوای تولیدشده کاربران رسانه‌های اجتماعی، می‌تواند احساسات کاربران را در مورد محصولات، انتخابات یا سیاست‌ها نشان دهد [۵۴].

همچنین پذیرش فناوری جدید مستلزم تغییرات گردش کار افراد، سازمان‌ها، دولت‌ها و بر این اساس، تغییرات فرهنگی، اقتصادی و اجتماعی است. افراد ادراکات منحصر به فرد و در عین حال انعطاف‌پذیری از فناوری می‌سازند که بر پذیرش آنان تأثیر می‌گذارد. بنابراین، برای تسهیل موفقیت‌آمیز پذیرش فناوری باید به نگرانی‌های شناختی، عاطفی و زمینه‌ای رسیدگی شود [۴۴].

در سال ۲۰۰۸، ریچارد تالر، اقتصاددان رفتاری (Behavioral) و کاس سانستاین حقوق‌دان، کتابی منتشر کردند که در آن رویکردی بدیع به خط‌مشی‌گذاری عمومی مبتنی بر مفهوم تلنگر (Nudge) را معرفی کردند. مفهوم تلنگر بحث‌های فراوانی در رشته‌های مختلف ایجاد کرد و در بین بسیاری از سیاست‌گذاران سراسر جهان محبوبیت یافت. تلنگر هر جنبه‌ای از معماری انتخاب[۱] (Choice Architecture) است که رفتار افراد را تحت سوگیری‌هایی (Bias) مانند در دسترس بودن، نزدیک‌بینی، شواهد متناقض، تایید و کلیشه، به روشی قابل پیش‌بینی بدون منع هیچ گزینه یا تغییر قابل‌توجهی در انگیزه‌های اقتصادی آنان تغییر می‌دهد [۴۷]. دولت‌ها برای اصلاح جنبه‌های رفتاری سوگیری‌ها «واحدهای تلنگر» ایجاد کرده‌اند. «تیم بینش رفتاری» بریتانیا، در تلاش است تا با کمک کلان‌داده، بهترین تلنگرها را طراحی کند [۴۶، ۱، ۱۸]. این واحد متشکل از متخصصان علوم رفتاری، وظیفه طراحی مداخلات رفتاری را دارد که پتانسیل تشویق رفتار مطلوب را بدون محدودیت انتخاب داشته باشد، آن مداخلات را سریع و کم هزینه آزمایش کند و سپس مؤثرترین راهبردها را به طور گسترده اجرا کند [۱۰]. تیم علوم رفتاری بانک جهانی، واحد ذهن، رفتار و توسعه[۲]، زمان زیادی را صرف تفکر در مورد اینکه چگونه سیاست‌گذاران در سراسر جهان علم رفتاری را برای مشکلات حل نشدنی سیاست بکار می‌برند، می‌کند. در علوم رفتاری در سراسر جهان: نمایه‌های ۱۰ کشور، استرالیا، کانادا، دانمارک، فرانسه، آلمان، هلند، پرو، سنگاپور، بریتانیا، ایالات متحده، بانک جهانی گسترش و

[۱] اصطلاح «معماری انتخاب» را ریچارد تالر و کاس سانستاین در سال ۲۰۰۸ در کتاب تلنگر: بهبود تصمیمات در مورد سلامت، ثروت و شادی ابداع کردند. تالر و سانستاین طراحی متفکرانه معماری انتخاب را به‌عنوان وسیله‌ای برای بهبود تصمیم‌گیری مصرف‌کننده با به حداقل رساندن سوگیری‌ها و خطاهای ناشی از عقلانیت محدود تأیید کرده‌اند.

[2] Mind, Behavior, and Development Unit (eMBeD)

نیز شکل علم رفتاری را در نوآوران یا پذیرندگان اولیه در میدان بررسی کرده است [۱]. در سال ۲۰۱۳، کاخ سفید تیم علوم اجتماعی و رفتاری را راه‌اندازی کرد که بسیاری از روش‌های اقتصاد رفتاری را وارد دولت اوباما کرد [۲۱]. در اینجا یک تناقض وجود دارد، سیاست‌گذاران نیز تحت تأثیر همان سوگیری‌های شناختی (Cognitive Biases) هستند که به دنبال آن هستند در دیگران، چه در حوزه اجتماعی و چه در حوزه فنی، به آن بپردازند [۵۰]. در عصر آشفته حاکمیت کلان‌داده و مفاهیمی مانند رفاه و آزادی، باید به تلنگرزنندگان برای تصمیم‌گیری بهینه در مورد کلان‌داده تلنگر زد و این تحقیق سعی دارد به دو سوال متناقض اساسی براساس چارچوب نظریه تلنگر پاسخ دهد:

۱. چه سوگیری‌هایی در بهره‌برداری از کلان‌داده تأثیر می‌گذارد؟

۲. کدام راهبردها یا راهبردهای مبتنی بر تلنگر می‌تواند ابزار مؤثرتری برای اصلاح سوگیری‌های شناختی در بهره‌برداری از کلان‌داده باشد؟

در ادامه مروری خواهیم داشت بر فرصت‌ها و چالش‌های کلان‌داده، سپس با استفاده از رویکرد تلنگر، تلاش خواهیم کرد سوگیری‌ها به سوی کلان‌داده را اصلاح نماییم.

۲ فرصت‌ها و چالش‌های کلان‌داده

کلان‌داده فرصت‌های قابل توجهی برای رشد اقتصادی، بهره وری، مالی، مراقبت‌های بهداشتی، امنیت، آموزش، بخش‌های اجتماعی–فرهنگی و سایر مفاهیم حکمرانی پیشنهاد می‌کند [۲۷]. ارزش کلان‌داده به دلیل شناسایی الگوها، روندها و ارتباطات پیچیده در مجموعه داده‌های عظیم بدون ساختار است که پیوندهای بین داده‌های متفاوت را طبقه‌بندی می‌کند.

برای مثال رمزگشایی اولین توالی ژنوم انسانی ۱۰ سال طول کشید اما امروز یک هفته طول می‌کشد. تعیین توالی ژنوم برای انسان ممکن است بر تصمیمات مراقبت‌های بهداشتی تأثیر بگذارد، زیرا افراد بیشتری توالی‌یابی می‌شوند، دانشمندان به مجموعه بزرگتری از داده‌های ژن‌ها از جمله روابط ژنومی خاص با بیماری‌ها برای شخصی‌سازی داروها دسترسی خواهند داشت [۲۷]. مطالعه اخیر روی شهرهای هوشمند دانمارک نشان داد که استفاده از کلان‌داده برای نظارت بر آلودگی هوا موثرتر و کم‌هزینه‌تر از نظارت بر سیستم‌های قدیمی است و استفاده از تجزیه‌وتحلیل کلان‌داده را برای مدیریت آلودگی هوا در آینده پیشنهاد می‌کند [۴۰]. کلان‌داده فرصتی برای تولید آمار رسمی به موقع فراهم می‌کند، به عنوان اثبات، ارائه آمار فصلی (مانند تولید ناخالص داخلی)، ممکن است به جای چند هفته زمان چند دقیقه یا ساعت طول بکشد. در همان مقیاس زمانی، کلان‌داده پیش‌بینی احتمالی زمان حال یا پخش کنونی را فراهم می‌کند [۱۶]. محققان دریافته‌اند که در زمان شیوع آنفولانزا، جستجوهای گوگل برای عباراتی مانند «درمان‌های آنفولانزا» و «علائم آنفولانزا» تنها چند هفته قبل از افزایش تعداد بیماران مراجعه‌کننده به بیمارستان‌ها برای آنفولانزا انجام می‌شود. بنابراین، بیمارستان‌ها می‌توانند برای مقابله با هجوم بیماران در طول فصول همه‌گیری، آمادگی بهتری داشته باشند

[۳۸]. در سال ۲۰۲۱، ارزش افزوده اقتصاد دیجیتال در ۴۷ کشور در سراسر جهان ۱.۳۸ تریلیون دلار بود که ۴۵ درصد از تولید ناخالص داخلی آنها را تشکیل می‌داد [۳۹].

اهمیت، فرصت‌ها و چالش‌های کلان‌داده به قدری حیاتی است که در بسیاری از کشورها مقررات مدیریت و سازماندهی کلان‌داده از جمله اتحادیه اروپا از سال ۲۰۱۸ ایجاد شد که مقررات عمومی حفاظت از داده‌ها را تصویب کرد و منجر به تحمیل میلیاردها دلار جریمه علیه شرکت‌های آمریکایی گوگل، اپل و آمازون شد. بنابراین، جمع‌آوری و پردازش گسترده کلان‌داده، نگران‌کننده است، نه تنها به دلیل پیامدهای آن برای حفظ حریم خصوصی، بلکه به این دلیل که استفاده از ابزارهای تصمیم‌گیری الگوریتمی می‌تواند تأثیر قابل‌توجهی بر افراد یا جامعه داشته باشد بنابراین نیاز به پاسخگویی شفاف در استفاده و تأثیر آنها وجود دارد [۱۵].

۳ تلنگر برای اصلاح سوگیری‌های شناختی

تلنگر مفهومی در اقتصاد رفتاری است که رویکردی را برای اصلاح رفتار، بدون اجبار توصیف می‌کند. اصطلاح تلنگر را تالر و سانستاین ابداع کردند، آنان استدلال می‌کنند که «تأثیر فعالانه» بر رفتار نه تنها ممکن، بلکه مشروع نیز هست و در عین حال به آزادی انتخاب افراد احترام می‌گذارد. هنر تأثیرگذاری بر رفتار موضوع جدیدی نیست، اما ترکیب جدیدی از بینش‌های اقتصاد رفتاری، روانشناسی شناختی و روانشناسی اجتماعی به آن افزوده شده است. این رویکرد، قیم‌مابی آزادیخواهانه را به عنوان قلب تلنگر تعریف می‌کند [۱۵]. زیرا هدف هدایت انتخاب‌ها به سمت رفاه فردی و اجتماعی است. به عبارت دیگر، تلنگر به معنای طراحی مجدد محیط تصمیم‌گیری برای القای رفتارهای بهینه مالی، سالم و زیست‌محیطی برای تصمیم‌گیرنده است.

ایده اصلی نظریه تلنگر بر این فرض اساسی استوار است که افراد عموماً رفتار غیرمنطقی دارند و فاقد خودکنترلی و دیدگاه بلندمدت مناسب هستند و پیامدهای رفتارهای غیرمنطقی می‌تواند آنان را به انتخابی سوق دهد که باعث ایجاد مشکلات مختلف با اثرات منفی طولانی‌مدت شود. برای مثال در مورد رفاه فردی و اجتماعی، برای تشویق مشتریان به انتخاب مواد غذایی سالم‌تر، آنان به مدیران رستوران‌ها پیشنهاد می‌کنند که گزینه‌های سالم را در معرض دید مشتریان قرار دهند – مانند قراردادن میوه در مقابل کیک شکلاتی – [۴۷]. با توجه به «در دسترس بودن» و تأثیر «انتخاب اول»، مشتریان به صورت پیش‌فرض تمایل دارند اقلام سالم‌تر «در دسترس» را انتخاب کنند. بنابراین، تلنگر رفتارهای بهینه‌ای را برای تصمیم‌گیرندگان ایجاد می‌کند تا سوگیری‌های شناختی آنان را اصلاح کند. سوگیری شناختی به معنای یک خطای ذهنی نظام‌مند است که منجر به پردازش و تفسیر نادرست باوری می‌شود که به طور غیرقابل پیش‌بینی بر تصمیمات و قضاوت‌هایی که افراد می‌گیرند، تأثیر می‌گذارد [۴۷].

حتی نوزادان یک، دو و سه ساله سوگیری درون‌گروهی نشان می‌دهند (ترجیح دادن و پسندیدن آنان که شبیه ما هستند بر دیگران). نوزادان علاوه بر حمایت از کسانی که شبیه خود هستند، از کسانی که شبیه آنان نیستند بیزار هستند. برای یک نوزاد انسان، دو گروه ما و دیگران وجود دارد. در بزرگسالی، سوگیری‌های اجتماعی و شناختی مختلفی وجود دارد [۵۳]. در مکتب اقتصاد رفتاری، رفتار انسان از جنبه‌های مختلف محدود شده است. در این دیدگاه، انسان ظرفیت‌های فکری و ذهنی محدودی دارد مانند

عدم کنترل نفس در برابر وسوسه‌ها و به سختی متعهد به برنامه‌ای خاص شدن (خودکنترلی محدود) و برای غلبه بر این محدودیت‌ها به راه‌های میانبر ذهنی متوسل می‌شود (عقلانیت محدود) و حاضر است منافع خود را قربانی کنند یا به خاطر بی‌عدالتی‌ها به خود آسیب برساند (منفعت شخصی محدود) [۴۸]. در واقع، براساس محدودیت‌ها و سوگیری‌های شناختی، افراد تمایل دارند تصمیماتی بگیرند که ناشی از محدودیت‌های زیر به نفع رفاه آنان یا جامعه نیست:

- بهینه‌سازی ناقص (ضعف در توجه و استدلال): انسانی با دیدگاه رفتاری متفاوت با انسان با دیدگاه منطقی، تمرکز محدودی دارد، مانند فراموشی، غفلت، حواس پرتی، رها شدن، ناتوانی در انجام چند کار، نابینایی در تغییر و توهم. علاوه بر این، انسان‌ها در ظرفیت محاسبات ذهنی دارای محدودیت‌هایی مانند نادیده گرفتن اطلاعات مربوطه، خطای نمونه‌گیری، خطای برنامه‌ریزی، سردرگمی، بیش از حد برآورد کردن و دست‌کم‌گرفتن، اتکای بیش از حد به اکتشاف هستند و در نهایت، اگر استدلال بیاورند اغلب توسط احساسات و احتمال هدایت می‌شود.

- ترجیحات غیراستاندارد (ضعف در انتخاب): انسان دارای دیدگاه رفتاری است، گاهی اوقات ترجیحات به مراجع بستگی دارد، مانند تأثیر مالکیت، اجتناب از ضرر و حفظ وضع موجود. انسان گاهی اوقات دارای ترجیحات ناشی از محیط است، مانند ترجیحات ناشی از هنجارهای اجتماعی، چارچوب‌بندی، نوع‌دوستی و ترجیحات بین‌فردی.

- خودکنترلی محدود (ضعف در اراده): انسان‌ها از دیدگاه رفتاری از محدودیت‌هایی مانند ناهماهنگی شناختی، خستگی ذهنی، اعتیاد، وسوسه و اغواگری، تنبلی و اهمال‌کاری رنج می‌برند [۱۰، ۳۵].

جدول ۱ مهم‌ترین سوگیری‌های شناختی را در سه دسته مختلف رفتار سازمانی، اجتماعی و فردی خلاصه می‌کند و در سه ساختار مختلف بازخورد (Feedback)، طرفدار اجتماع (Pro-social) و طرفدار خود (Pro-self) برای تغییر جهت آنها، چهار نوع تلنگر سنتی، دیجیتالی (تلنگرهای دیجیتالی را می‌توان به عنوان یک نمایش دیجیتالی از تلنگرها در اقتصاد رفتاری درک کرد. قدرت و فرصت‌های تلنگر دیجیتال تحت تأثیر ویژگی‌های منحصربه‌فرد معماری‌های انتخاب دیجیتال و پاسخ‌های رفتاری کاربران به‌صورت آن‌لاین، متمایز کردن آن از سلف آف‌لاین‌اش قرار می‌گیرند)، بیش‌تلنگر (Hyper Nudge) و تاریک (Dark) مثلاً با بهره‌برداری از سوگیری‌های شناختی ریسک‌کنندگان یا تشویق به مصرف محصولات مضر) را معرفی می‌کند.

بازخورد دقیق و شخصی‌سازی شده به عنوان یک تلنگر اطلاعاتی، اطلاعات را برای عموم قابل درک‌تر می‌کند [۴۷، ۴۸]. به منظور تأثیرگذاری بر سوگیری‌ها برای تصمیم‌گیری بهتر در مورد کلان‌داده، بازخورد مقوله مناسبی برای رسیدگی به برخی سوگیری‌ها است.

هدف تلنگرهای «طرفدار اجتماع» در درجه اول افزایش رفاه جامعه از طریق دورکردن افراد تلنگرخورده از رفتارهایی است که منفعت عمومی را کاهش می‌دهد [۲۴، ۲۲، ۲۳، ۳۳].

هاگمن و همکاران «طرفدار خود» را به‌عنوان تلنگرهایی تعریف می‌کنند که «به افراد کمک می‌کند از رفتار غیرمنطقی که بهزیستی بلندمدت آنان را کاهش می‌دهد، دوری کنند» [۲۴].

جدول ۱: سوگیری‌ها نسبت به کلان‌داده و تلنگر برای تغییر جهت آنها

ماهیت سوگیری	نوع سوگیری	ساختار تلنگر
رفتار سازمانی	**دسترس‌پذیری**(Availability)	بازخورد
	نزدیک‌بینی (Myopia)	
	توهم کنترل (Illusion of Control)	
	بین‌گروهی (In-group)	
	اتوماسیون (Automation)	
	تاخر (Recency)	
اجتماعی	**نمایندگی** (Representativeness)	طرفدار اجتماع
	انتخاب (Selection)	
	کلیشه (Stereotype)	
	بیش‌تعمیم (Overgeneralization)	
	خوش‌بینی (Optimism)	
فردی	**لنگرانداختن** (Anchoring)	طرفدار خود
	چارچوب‌بندی (Framing)	
	تایید (Confirmation)	
	بیش‌اعتماد (Overconfidence)	
	آبشار دسترس‌پذیری (Availability Cascade)	

۴ نتیجه‌گیری

براساس ارتباط کلان‌داده با اقتصاد، تخمین زده می‌شود که هزینه‌های بازار جهانی کلان‌داده در سال ۲۰۲۴ به ۴.۲۹۸ میلیارد دلار برسد [۳۹]. بنابراین کلان‌داده به یک ارزش مهم برای شرکت‌ها، صنایع و اقتصاد تبدیل می‌شود. همچنین کلان‌داده برای رفاه اجتماعی مزایای فراوانی دارد، سیاست‌های دولت در کشف تقلب و تجزیه‌وتحلیل بازار مالی، مراقبت‌های بهداشتی و سلامت عمومی، نظارت و آموزش دولتی، مبارزه با جرم و جنایت، حفاظت از محیط‌زیست و اکتشاف انرژی، کشاورزی، پیش‌بینی آب‌وهوا و مدیریت اکوسیستم و سیاست‌های جامعه مانند شهرهای هوشمند را بهبود می‌بخشد. با این حال، با چالش‌های بزرگ کلان‌داده، از جمله نقض حریم خصوصی، ابهام مالکیت داده، عدم استانداردسازی و مسائل حقوقی و سیاستی داده‌های یکپارچه، استراتژی داده‌های نامشخص و غیرقابل اعتماد مواجه هستیم. همچنین خطراتی در تصمیم‌گیری خودکار وجود دارد که منجر به انتخاب محدود و تبعیض می‌شود، علاوه بر این خطر که برنامه‌های کلان‌داده در آینده دارای تجزیه‌وتحلیل غیرقابل پیش‌بینی باشند، قوانین فعلی هنوز حفاظت کافی برای کلان‌داده در مقابل سوءاستفاده غیرمجاز اشخاص ثالث ارائه نکرده است. این واقعیت که برخی از کاربران نهایی و شرکت‌ها دسترسی کافی به کلان‌داده ندارند نیز باعث ایجاد شکاف دیجیتالی شده است. برخی بیش از حد به داده‌ها وابسته هستند و برخی نیز از سوی خطرات امنیت سایبری (Cyber Security) تهدید می‌شوند. علاوه بر این، محاسبات و پیچیدگی سیستم نیز وجود دارد. بسیاری از مردم به دلیل زبان، فقر، فقدان آموزش، فقدان

زیرساخت فناوری، دور بودن یا تعصب و تبعیض از دنیای جدید داده‌ها و اطلاعات کنار گذاشته شده‌اند. طیف وسیعی از اقدامات مورد نیاز است، از جمله ایجاد ظرفیت‌های همه کشورها به‌ویژه کشورهای کمتر توسعه‌یافته.

یافته‌های نظری شناختی و رفتاری از سوی دیگر، انسان را متأثر از سوگیری‌های شناختی و به دور از عقلانیت کامل توصیف می‌کند. انسان‌ها ممکن است هرگز زمان کافی و اطلاعات مورد نیاز برای تصمیم‌گیری‌های خود نداشته باشند، بنابراین همیشه در مورد تأثیر تصمیمات آنان عدم اطمینان وجود دارد. بحران‌هایی مانند همه‌گیری کووید-۱۹، اطلاعات و زمان عمل را به‌طور چشمگیری کوتاه می‌کند بنابراین براساس سوگیری‌های خود تصمیم می‌گیرند. کارکردهای انسانی و محدودیت‌های فیزیکی باعث حساسیت به دستکاری و اجبار پنهان کلان‌داده می‌شود و بدیهی است که الگوریتم‌های کلان‌داده به روش‌های مختلف بر تصمیم‌گیری انسان تأثیر می‌گذارند و پتانسیل دستکاری، اگر نگوییم فریب و اجبار دارند. این اثرات باید به دلیل عدم توجه به خطرات کلان‌داده در رفتار سازمانی، اجتماعی و سوگیری‌های فردی مانند در دسترس بودن، درک نادرست از کلان‌داده به عنوان منبع قدرت، منافع شخصی یا گروهی که از طریق دسترسی به دست می‌آیند، اعتماد بیش از حد به کلان‌داده، حفظ اتوماسیون به عنوان بهترین راه‌حل و بنابراین تصمیم جدیدی در مورد چالش‌های کلان‌داده اصلاح شوند که در این تحقیق، سه دسته مختلف تلنگر، بازخورد، طرفدار اجتماعی و طرفدار خود، که به چهار نوع تلنگر سنتی، دیجیتال، بیش‌تلنگر و تاریک تقسیم می‌شوند، در سه ساختار معرفی شدند تا تلنگرهای مرتبط با سوگیری‌ها را نسبت به کلان‌داده مقایسه کنند و در نهایت بر بیش‌تلنگر تاکید می‌شود.

مراجع

[1] Afif, Zeina; Islan, William Wade; Calvo-Gonzalez, Oscar; Dalton, Abigail Goodnow (2019) Behavioral Science Around the World: Profiles of 10 Countries (English) eMBeD brief. Washington, D.C.: World Bank Group.

[2] Andrew Leonard. (2013) How Netflix Is Turning Viewers into Puppets, Salon (Feb. 1, 2013, 7:45 AM EST), http://www.salon.com/2013/02/01/how_netflix_is_turning_viewers_into_puppets

[3] Ards, Sheila; Chung, Chanjin; Myers, Samuel L. (1998) "The effects of sample selection bias on racial differences in child abuse reporting". Child Abuse & Neglect. 22 (2): 103–115. Doi:10.1016/S0145-2134(97)00131-2. PMID 9504213.

[4] Ariely, D. (2009) Predictably irrational: The hidden forces that shape our decisions. London: Harper Collins.

[5] Aronson, E., Wilson, T. D., & Akert, R. (2010) Social psychology. 7th ed. Upper Saddle River: Prentice Hall.

[6] Asiamah, Nestor & Mensah, Henry Kofi & Oteng-Abayie, Eric Fosu. (2017) Do Larger Samples Really Lead to More Precise Estimates? A Simulation Study. American Journal of Educational Research. 5. 9-17. 10.12691/education-5-1-2.

[7] Athamena, Belkacem & Houhamdi, Zina. (2018) Model for decision-making process with big data. Journal of Theoretical and Applied Information Technology. 96. 5951-5961.

[8] Barocas, S., & Nissenbaum, H. (2014) Big Data's End Run around Anonymity and Consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), Privacy, Big Data, and the Public Good: Frameworks for Engagement (pp. 44-75) Cambridge: Cambridge University Press. Doi:10.1017/CBO9781107590205.004.

[9] Batko, K., Ślęzak, A. The use of Big Data Analytics in healthcare. J Big Data 9, 3 (2022) https://doi.org/10.1186/s40537-021-00553-4.

[10] Benartzi, S., Beshears, J., Milkman, K. L., Sunstein, C. R., Thaler, R. H., Shankar, M., Tucker-Ray, W., Congdon, W. J., & Galing, S. (2017) Should Governments Invest More in Nudging? Psychological Science. https://doi.org/10.1177/0956797617702501.

[11] Bholat D. (2015) Big data and central banks, Big Data Soc., 2 (1) (2015), pp. 1-6, 10.1177/2053951715579469.

[12] Bovens, L. (2008) The ethics of nudge. In T. Grune-Yanoff and S. O. Hansson (Eds.), Preference change: Approaches from philosophy, economics and psychology (pp. 207–219) Dordrecht: Springer.

[13] Buckee, Caroline. (2020) Improving epidemic surveillance and response: big data is dead, long live big data. The Lancet Digital Health, Volume 2, Issue 5, 2020, Pages e218-e220, ISSN 2589-7500, https://doi.org/10.1016/S2589-7500(20)30059-5.

[14] Cao, X., & Yousefzadeh, R. (2023) Extrapolation and AI transparency: Why machine learning models should reveal when they make decisions beyond their training. Big Data & Society, 10(1) https://doi.org/10.1177/20539517231169731.

[15] Centre for Data Ethics and Innovation. (2020) Review into bias in algorithmic decision-making. assets.publishing.service.gov.uk.

[16] Choi, H. and H. Varian. (2012) Predicting the present with Google Trends. Economic Record, 88, pp. 2-9.

[17] Diakopoulos, N. (2013, October 3) Race against the algorithms. The Atlantic. Retrieved from http://www.theatlantic.com/world/

[18] Dewies, M., Denktaş, S., Giel, L. et al. (2022) Applying Behavioral Insights to Public Policy: An Example from Rotterdam. Glob Implement Res Appl 2, 53–66 (2022). https://doi.org/10.1007/s43477-022-00036-5

[19] Duarte, Fabio (April 3, 2023) Amount of Data Created Daily (2023), https://explodingtopics.com/blog/data-generated-per-day

[20] Garoufallou, Emmanouel & Gaitanou, Panorea. (2021) Big Data: Opportunities and Challenges in Libraries, a Systematic Literature Review. College & Research Libraries. 82. 410. 10.5860/crl.82.3.410

[21] Halpern, D., & Sanders, M. (2016) Nudging by government: Progress, impact, & lessons learned. Behavioral Science & Policy, 2(2), pp. 53–65.

[22] Hands, D. W. (2020) Libertarian paternalism: Taking Econs seriously. International Review of Economics, 67(4), 1–23.

[23] Hands, D. W. (2021) Libertarian paternalism: Making rational fools. Review of Behavioral Economics, Forthcoming.

[24] Hagmann, D., Ho, E. H., & Loewenstein, G. (2019) Nudging out support for a carbon tax. Nature Climate Change, 9(6), 484– 489.

[25] Henrik Skaug Sætra, (2019) Freedom under the gaze of Big Brother: Preparing the grounds for a liberal defense of privacy in the era of Big Data, Technology in Society, Volume 58, 2019, 101160, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2019.101160

[26] Jeble, Shirish & Kumari, Sneha & Patil, Yogesh. (2018) Role of Big Data in Decision Making. Operations and Supply Chain Management: An International Journal. 11. 36. 10.31387/oscm0300198

[27] Jung Wan LEE (2020) Big Data Strategies for Government, Society and Policy-Making, Journal of Asian Finance, Economics and Business, Vol. 7 No. 7 (2020) 475–487.

[28] Kahneman, D. (2011) Thinking Fast and Slow. London. Penguin Books.

[29] Kahneman, D., & Tversky, A. (1972) Subjective probability: A judgment of representativeness. Cognitive Psychology, 3, 430-454.

[30] Karen Yeung (2017) Hypernudge': Big Data as a mode of regulation by design, Information, Communication & Society, 20:1, 118-136, DOI:10.1080/1369118X.2016.1186713.

[31] Kuran, Timur, and Sunstein, Cass. (1999) Availability Cascades and Risk Regulation, Stanford Law Review, Vol. 51, No. 4.

[32] Michael, K., & Miller, K. W. (2013) Big data: new opportunities and new challenges. Computer, 46(6), 22–24.

[33] Nagatsu, M. (2015) Social nudges: Their mechanisms and justification. Review of Philosophy and Psychology, 6(3), 481–494.

[34] Nikolopoulou, K. (2023, June 19) What Is Optimism Bias? Definition & Examples. Scribbr. Retrieved July 10, 2023, from https://www.scribbr.com/research-bias/optimism-bias/

[35] OECD. (2019) OECD Behavioral Insights Toolkit and Ethical Framework. OECD.

[36] Omoyiola BO. The social implications, risks, challenges, and opportuniti es of big data [version 1; peer review: 2 approved with reservations]. Emerald Open Res 2022, 4:23, https://doi.org/10.35241/emeraldopenres.14646.1

[37] Petticrew M, Maani N, Pettigrew L, et al. (2020) Dark nudges and sludge in big alcohol: behavioral economics, cognitive biases, and alcohol industry corporate social responsibility. Milbank Q 98, 1290–1328.

[38] Philip D. Waggoner, Ryan Kennedy, Hayden Le and Myriam Shiran. (2019) Big Data and Trust in Public Policy Automation, Stat Polit Pol 2019; 10(2): 115–136.

[39] Qiaohong Pan, Wenping Luo, Yi Fu. (2022) A csQCA study of value creation in logistics collaboration by big data: A perspective from companies in China, Technology in Society, Volume 71,2022,102114, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2022.102114

[40] Shahbaz, Muhammad, Changyuan Gao, LiLi Zhai, Fakhar Shahzad, Imran Khan. (2020). Environmental air pollution management system: Predicting user adoption behavior of big data analytics, Technology in Society, Volume 64,2021,101473, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2020.101473

[41] Simone Fanelli, Lorenzo Pratici, Fiorella Pia Salvatore, Chiara Carolina Donelli and Antonello Zangrandi. (2022) Big data analysis for decision-making processes: challenges and opportunities for the management of health-care organizations. Management Research Review Vol. 46 No. 3, 2023 pp. 369-389 Emerald Publishing Limited 2040-8269, DOI 10.1108/MRR-09-2021-0648.

[42] Skitka, L.J., Mosier, K. L., Burdick, M., & Rosenblatt, B. (2000) Automation bias and errors: Are crews better than individuals? International Journal of Aviation Psychology, 10, 85-97.

[43] Trytten, Deborah & Lowe, Anna & Walden, Susan. (2012) "Asians are Good at Math. What an Awful Stereotype" The Model Minority Stereotype's Impact on Asian American Engineering Students. Journal of Engineering Education.

[44] Straub, E. T. (2009). Understanding Technology Adoption: Theory and Future Directions for Informal Learning. Review of Educational Research, 79(2), 625–649. https://doi.org/10.3102/0034654308325896

[45] Sunstein, Cass Robert. 2014a. Why Nudge? The Politics of Libertarian Paternalism. New Haven: Yale University Press.

[46] Sunstein, Cass Robert. (2015) Foreword: The Ethics of Nudging. In Nudge and the Law: A European Perspective. Edited by Alberto Alemanno and Anne-Lise Sibony. Oxford: Hart, pp. v–xviii.

[47] Thaler, R., & Sunstein, C. (2008) Nudge. London: Penguin Books.

[48] Thaler, R. H., Sunstein, C. R. & Balz, J. P. (2014) Choice architecture, The Behavioral Foundations of Public Policy, ch. 25, pp.428-439.

[49] Tversky, A., & Kahneman, D. (1981) The framing of decisions and the psychology of choice. Science, 211, 453–458.

[50] Vaezi, Seyyed Kamal, Dargahi, Sahel, Anvari, Zohra and Ali Esfahani, Zahireh. (2023) Investigating the ability of behavioral nudges in correcting policy makers' biases, Modiriat Dowlati, 1402; 15(1): 41-66. doi: 10.22059/jipa.2023.350572.3236.

[51] Van Dooren, W., De Bock, D., Hessels, A., Janssens, D., & Verschaffel, L. (2005) Not Everything Is Proportional: Effects of Age and Problem Type on Propensities for Overgeneralization. Retrieved October 26, 2015.

[52] Viktor Mayer-Schönberger and Kenneth Cukier (2013) Big Data: A Revolution That Will Transform How We Live, Work, and Think. Boston: Houghton Mifflin Harcourt, 2013. 242 pp.

[53] Wynn, Karen. (1992) Addition and subtraction by human infants. Nature. 358 (6389): 749–750. Bibcode:1992, Nature. 358-749.

[54] Xing Yunfei, Xiwei Wang, Chengcheng Qiu, Yueqi Li, Wu He (2022) Research on opinion polarization by big data analytics capabilities in online social networks, Technology in Society, Volume 68, 2022, 101902, ISSN 0160-791X, https://doi.org/10.1016/j.techsoc.2022.101902

[55] Zhao, Liang. (2020) Event Prediction in the Big Data Era: A Systematic Survey, 1, 1 (August 2020), 40 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

تشخیص میزان خطر امنیتی برنامه‌های موبایل با استفاده از مفهوم آنتروپی

محمود دی‌پیر [۱]، تکتم ذوقی [۲]

[۱] دانشیار دانشکده رایانه و فناوری اطلاعات، دانشگاه هوایی شهید ستاری، تهران، ایران
mdeypir@ssau.ac.ir
[۲] استادیار گروه مهندسی کامپیوتر و برق، دانشکده شریعتی، دانشگاه فنی و حرفه‌ای، تهران، ایران
t.zoughi@shariaty.ac.ir

چکیده

امنیت دستگاه‌های همراه با توجه به افزایش کاربرد آنها نقش مهمی در امنیت فضای سایبری دارد. با گسترش کاربرد آنها، بدافزارهای زیادی نیز برای سوء استفاده از کاربران آنها توسط نفوذگران ارائه شده است. شناختن سطح خطر امنیتی هر نرم‌افزار می‌تواند در اطلاع‌رسانی به کاربر درباره استفاده از نرم‌افزارهای مخرب، تأثیرگذار باشد. می‌توان به‌صورت تقریبی خطرات امنیتی نرم‌افزارهای اندروید را از طریق بررسی مجوزهایی که آنها درخواست می‌دهند، تخمین زد. در این بررسی بر اساس تعریف مجوزهای بحرانی و با تجزیه و تحلیل مجوزهای درخواستی توسط نرم‌افزارهای خبیث و نرم‌افزارهای قابل اعتماد و شناخته شده، معیار جدیدی به منظور اندازه‌گیری خطر امنیتی برنامه‌های اندروید ارائه شده است. در این معیار مجوزهایی اثر بیشتری در محاسبه مقدار خطر امنیتی دارند که آنتروپی بیشتری در تشخیص برنامه‌های مخرب از برنامه‌های کاربردی داشته باشند. همچنین میزان خطر هر برنامه موبایل برابر با مجموع بهره اطلاعاتی مجوزهای درخواستی آن است. آزمایش‌های صورت گرفته روی داده‌های واقعی نشان‌دهنده نرخ تشخیص بالاتر معیار پیشنهادی در مقایسه با استانداردهای گذشته قرار دارد.

کلمات کلیدی: مجوز، ارزیابی ریسک امنیتی، معیار امنیتی، داده کاوی، آنتروپی، بهره اطلاعاتی، تحلیل ایستا، تحلیل پویا.

۱ مقدمه

بین تمام سیستم‌های عامل ایجاد شده برای گوشی‌های موبایل و ابزارهای هوشمند قابل حمل، اندروید به‌شکل گسترده‌تری به کار گرفته شده است. برای این پلتفرم، تعداد زیادی برنامه تاکنون توسعه یافته‌اند. اکثریت این برنامه‌ها توسط افراد نامشخص و توسعه‌دهندگان ناشناس عرضه شده‌اند [۲۶-۲۷]. مدل امنیتی برنامه‌ها در سیستم عامل اندروید بر پایه مجوزها استوار است. این مجوزها در ابتدای نصب هر نرم‌افزار یا در زمان اجرای

آن از کاربر پرسیده می‌شوند و غیر از آن، کاربر چندان دخالتی در امنیت نرم افزار مورد استفاده خود ندارد. معمولاً کاربران به‌ندرت زمان کافی را برای مطالعه و توجه به لیست مجوزها در صفحه نصب اولیه نرم‌افزار یا هنگام اجرا تخصیص می‌دهند. علاوه بر این، کاربران عادی معمولاً دانش فنی برای شناخت تأثیر استفاده از هر مجوز و امکان سوء استفاده از آن توسط نفوذگران را ندارند. لذا، این رویکرد امنیتی در افزایش امنیت کاربران به‌منظور حفاظت از داده‌های شخصی و حریم خصوصی آنها کمتر مؤثر است [۲۸-۲۹]. نرم‌افزارهای مخرب، نظیر تروجان‌ها، جاسوس‌افزارها، باج‌افزارها و تبلیغ‌افزارها می‌توانند با فریفتن کاربران، خود را به‌عنوان یک برنامه مفید و بدون خطر ارائه دهند و اطلاعات حساس شرکت‌ها و مراکز حساس دولتی را بدزدند. این نوع بدافزارها همچنین می‌توانند با دزدیدن داده‌های شخصی افراد و فاش کردن آنها، حریم خصوصی آنها را نقض کنند [۳۰-۳۱]. بر اساس آمارهای غیررسمی اخیر، در میان هر ۵ برنامه توسعه‌یافته اندروید، یکی بدافزار بوده است. بنابراین شناسایی و مقابله با این بدافزارها، بسیار ضروری است. تا به حال تحقیقاتی به‌منظور افزایش آگاهی کاربران در زمینه امنیت نرم افزارها در اندروید انجام شده است [۱]. استفاده از عناوین مناسب‌تر برای مجوزها، دسته‌بندی مجوزها، کاهش تعداد عنوان‌های مجوز، بهره‌برداری از نظرات کاربران علاوه بر مجوزها، نمونه‌هایی از راه‌کارهای ارائه شده در این تحقیقات هستند. همچنین، تاکنون معیارهای مختلفی نیز برای سنجش خطر امنیتی یک نرم‌افزار اندرویدی ارائه شده است. تعداد مجوزهای حساس درخواستی و تعداد جفت مجوزهای حساس درخواستی نمونه‌هایی از این معیارها هستند [۲]. با بهره‌گیری از این استانداردها و وجود یک حد مرجع، پس از ارزیابی ریسک امنیتی یک برنامه مظنون، اگر ریسک آن افزایش یافته باشد، اخطاری به لحاظ امنیتی منتشر می‌شود. در این نوشتار، یک استاندارد نوآورانه برای ارزیابی ریسک یک برنامه اندرویدی مطرح شده که نسبت به استانداردهای پیشین کارکرد بهینه‌تری دارد.

در ادامه، تعدادی از پژوهش‌های انجام شده که با امنیت اندروید ارتباط دارند، معرفی می‌شوند. در بخش سوم، استاندارد تازه پیشنهادی ارائه و روش محاسبه آن توضیح داده شده است. در قسمت چهارم، تجربیاتی به‌منظور ارزیابی و تطبیق استاندارد پیشنهادی با استانداردهای پیشین، عرضه شده‌اند. در این بخش، با بهره‌گیری از دسته داده‌هایی شامل صدها بدافزار و هزاران برنامه مفید شناخته شده اندروید، معیار پیشنهادی با معیار ارائه شده قبلی از نظر اندازه‌گیری میزان خطر و توان تشخیص بدافزارها از نرم‌افزارها مقایسه خواهد شد. در نهایت این مقاله در بخش پنجم جمع‌بندی و نتیجه‌گیری می‌شود.

۲ مروری بر کارهای دیگران

با نگاه به ساختار امنیتی خصوصی اندروید و محدودیت‌های آن، تعدادی تحقیق در این زمینه صورت گرفته است. مطالعات اشاره دارند که کاربران اکثراً از بررسی مجوزهای پیشنهادی برنامه‌ها در اندروید چشم‌پوشی می‌کنند. در برخی تحقیقات انجام‌شده، سعی شده تا بر این مشکل غلبه شود [۳-۶]. فلت و همکاران [۳] راهکارهایی نظیر تغییر طبقه‌بندی مجوزها، تأکید بر مفهوم ریسک امنیتی و روش تخصیص مجوزها مطرح کرده‌اند. در [۷] اطلاعات سطح بالا شامل عناصر حفظ حریم شخصی همچون اطلاعات شخصی، مکان و دفترچه تلفن، به‌جای لیست مجوزها در صفحه توصیف برنامه پیشنهاد شده است. به‌منظور کاهش فضای

لازم برای نمایش چنین اطلاعاتی و کمک به کاربر در تصمیم‌گیری بهینه‌تر هنگام انتخاب و نصب، در [۱] عوامل ریسک و غیر ریسک که نتایج کمی آنها با توجه به مجوزها قابل محاسبه است، ارائه گردیده‌اند. با بررسی کاربران معلوم شد که این استانداردها نسبت به اطلاعات متنی تأثیر بیشتری دارند. پنگ و همکاران [۸] یک روش اصلی بر اساس مدل احتمالاتی را به‌منظور رتبه‌بندی برنامه‌های اندروید بر پایه مجوزهای مورد نیاز، عرضه کردند. برخی از تحقیقات با استفاده از مجوزهای پیشنهادی برنامه‌ها، به تشخیص برنامه‌های زیان‌آور یا مشکوک می‌پردازند [۹-۱۱]. برخی دیگر نیز با استفاده از تحلیل استاتیکی کد برنامه، توابع استفاده شده در برنامه‌نویسی و هم‌خوانی آن با برخی الگوهای موجود بدافزارها، برای تشخیص بدافزارهای جدید اقدام کرده‌اند [۱۲-۱۵]. تعدادی از پژوهشگران ترکیبی از تحلیل ایستا و پویا را به‌منظور تخمین خطر امنیتی نرم‌افزارهای اندروید مورد توجه قرار داده‌اند [۲۱]. اخیراً یادگیری عمیق به‌صورت گسترده به‌منظور تشخیص بدافزارهای اندروید مورد توجه قرار گرفته است [۲۲-۲۴]. در این دسته از تحقیقات عمدتاً محتوای برنامه‌های اندروید اعم از نرم‌افزار و بدافزار مانند تصاویر دو بعدی فرض می‌شوند و از آنها، ویژگی‌هایی به‌منظور آموزش یک مدل عمیق دسته‌بندی استفاده می‌گردد [۳۲-۳۳].

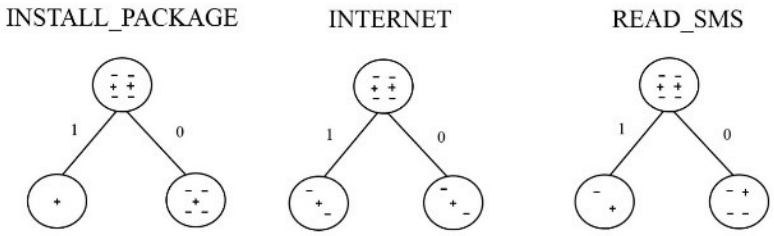
۳ روش پیشنهادی

یک مجوز بحرانی، مجوزی است که پیشتر در نرم‌افزارهای زیان‌آور اندروید مورد شناسایی و استفاده قرار گرفته است، یا به منابع حساس نرم‌افزاری و سخت‌افزاری دستگاه دسترسی پیدا می‌کند. از این استانداردها می‌توان برای ارائه هشدار در مورد اپلیکیشن‌های مظنون یا تشخیص نرم‌افزارهای زیان‌آور ناشناس جدید، بهره برد. ما در جستجوی یک استاندارد، برای ارزیابی ریسک‌های امنیتی نرم‌افزارهای اندروید هستیم که هم ساده باشد و هم توصیف دقیق‌تری از ریسک امنیتی اپلیکیشن در اندروید ارائه دهد. علاوه بر این، توانایی داشته باشد تا به نرم‌افزارهای سودمند، میزان ریسک امنیتی کم و به نرم‌افزارهای زیان‌آور، نسبت به نرم‌افزارهای سودمند، میزان ریسک امنیتی بالایی اختصاص دهد. استاندارد پیشنهادی ما بر مبنای نظریه اطلاعات و اصول آنتروپی که در یادگیری ماشین به‌کار برده شده است، ارائه شده است. در این استاندارد، بهره‌گیری اطلاعاتی از مجوزها محاسبه می‌شود. این بهره‌گیری اطلاعاتی با توجه به مفهوم آنتروپی قابل محاسبه است. در حقیقت، ما با توجه به اصول حوزه نظریه اطلاعات، آنتروپی مجموعه کل اپلیکیشن‌ها از لحاظ مفید و زیان‌آور بودن را محاسبه می‌کنیم و سپس با توجه به نقش هر مجوز در تفکیک اولیه نرم‌افزارها از بدافزارها، بهره‌گیری اطلاعاتی را برای هر مجوز به دست می‌آوریم. از دیدگاه ما، یک مجوز حیاتی است که بهره‌گیری اطلاعاتی بالایی در تفکیک نرم‌افزارها از بدافزارهای دارد. مجموع بهره اطلاعاتی که مجوزهای مورد استفاده یک اپلیکیشن اندروید دارند، میزان ریسک امنیتی آن را پیش‌بینی می‌کند. ما روش کار را با استفاده از مثال زیر نشان می‌دهیم.

مثال: فرض کنید مجموعه شش نرم‌افزار مفید و مخرب (بدافزار) مورد تحلیل ما به صورت جدول ۱ باشد. در این چارت، برای هر اپلیکیشن اندروید، شناسه، فهرست مجوزهای آن، و همچنین ویژگی مفید یا زیان‌آور

جدول ۱: اطلاعات وابسته به مثال ۱: اپلیکیشن‌های سودمند (−) و برنامه‌های مخرب (+)

ID	Permissions	Malware
1	INTERNET, READ_PROFILE	-
2	BATTERY_STATS, BLUETOOTH	-
3	BROADCAST_SMS,WRITE_SMS	+
4	INTERNET,INSTALL_PACKAGE, READ_SMS	+
5	READ_SMS, WRITE_EXTERNAL_STORAGE	-
6	BATERY_STATS, INTERNET	-



شکل ۱: تأثیر بهره‌گیری از سه مجوز نمونه در تفکیک برنامه‌های بدخواه (+) از اپلیکیشن‌ها (−)

بودن آن مشخص شده است.

باید برای هر مجوز، بهره اطلاعاتی را با استناد به داده‌های جدول فوق محاسبه نماییم و از این داده‌ها و معیار ارائه شده، به‌منظور ارزیابی ریسک امنیتی اپلیکیشن‌های اندروید بهره ببریم. مسلماً هر مجوز، با توجه به اطلاعات ارائه شده در جدول ذکر شده، بهره‌ای متفاوت از اطلاعات خواهد داشت و با توجه به این بهره‌گیری اطلاعاتی، در تعیین ریسک امنیتی یک برنامه تازه تاثیرگذار خواهد بود. به‌عنوان نمونه، بهره اطلاعاتی را برای سه مجوز نمونه با استفاده از شکل ۱ محاسبه کرده‌ایم. در این شکل، نماد مثبت نشان‌دهنده‌ی برنامه‌های مخرب و نماد منفی، نمایانگر تست منفی یا به‌عبارتی اپلیکیشن‌های مفید است.

همان‌گونه که در شکل ۱ آشکار است، برای هر مجوز، بر اساس استفاده (داشتن مقدار ۱) و عدم استفاده (مقدار ۰)، برنامه‌ها به دو گروه تقسیم شده و یک درخت شامل یک ریشه و دو زیرشاخه تشکیل می‌شود. زیرشاخه سمت چپ نمایانگر گروهی از برنامه‌هاست که این مجوز را خواستار شده‌اند و زیرشاخه سمت راست برنامه‌هایی را نشان می‌دهد که نیازی به این مجوز برای اجرای خود ندارند. در هر گروه، ممکن است هم برنامه‌های بدخواه و هم اپلیکیشن‌های مفید وجود داشته باشد. میزان آنتروپی مجموعه اپلیکیشن‌ها، با دسته‌بندی انجام شده توسط هر مجوز، می‌تواند کاهش یابد و در نتیجه بهره‌گیری اطلاعاتی بیشتر از صفر به‌دست آید. به‌عنوان مثال، بهره اطلاعاتی را برای مجوز INSTALL_PACKAGE محاسبه می‌کنیم. از آنجا که مجموعه اپلیکیشن‌های تحت تجزیه و تحلیل در اینجا ۶ است و از این تعداد ۲ نمونه برنامه‌های بدخواه

هستند، آنتروپی ریشه درخت یعنی مجموعه کل اپلیکیشن‌ها مساوی خواهد بود با:

$$\text{ParentEntropy} = -\frac{۲}{۶}\log_۲\left(\frac{۲}{۶}\right) - \frac{۴}{۶}\log_۲\left(\frac{۶}{۶}\right) = ۰/۷۹۸۶ \quad (۱)$$

بر اساس مجموعه اپلیکیشن‌های نمونه ما در جدول ۱، فقط یک نوع نرم‌افزار مخرب از این مجوز استفاده نموده است. یک نرم‌افزار مخرب و چهار اپلیکیشن مفید از این مجوز بهره نبرده‌اند. در نتیجه، آنتروپی این فرزندان به‌شکل متوالی برابر خواهد بود با:

$$\text{Entropy}(\text{INSTALL\_PACKAGES} = ۱) = -\frac{۱}{۱}\log_۲\left(\frac{۱}{۱}\right) = ۰ \quad (۲)$$

$$\text{Entropy}(\text{INSTALL\_PACKAGES} = ۰) = -\frac{۱}{۵}\log_۲\left(\frac{۱}{۵}\right) - \frac{۴}{۵}\log_۲\left(\frac{۴}{۵}\right) = ۰/۶۴۲۹ \quad (۳)$$

میانگین وزنی آنتروپی گره‌های فرزند با توجه به تعداد هر کدام به‌صورت زیر محاسبه می‌شود:

$$\text{WeightedAverageEntropyofChildren} = \frac{۱}{۶} \times ۰ + \frac{۵}{۶} \times ۰/۶۴۲۹ = ۰/۵۳۵۸ \quad (۴)$$

با توجه به آنتروپی‌های محاسبه شده، میزان بهره اطلاعاتی برای این مجوز، معادل با تفاوت بین آنتروپی کل نرم‌افزارها و میانگین وزن‌دار آنتروپی زیردرخت‌ها می‌باشد:

$$\text{IG}(\text{INSTALL\_PACKAGES}) = ۰/۷۹۸۶ - ۰/۵۳۵۸ = ۰/۲۶۲۸ \quad (۵)$$

در معیار ارائه شده توسط ما، این رقم، میزان ریسک امنیتی مربوط به این مجوز را ارائه می‌دهد. مقدار بهره اطلاعاتی یا سطح خطر امنیتی دو مجوز INTERNET و READ_SMS به‌شکل زیر تعیین می‌شود، که ما از جزئیات محاسباتی صرف نظر می‌کنیم و این محاسبات را به عهده مطالعه‌گر می‌گذاریم:

$$\text{IG}(\text{INTERNET}) = ۰ \quad (۶)$$

$$\text{IG}(\text{READ\_SMS}) = ۰/۰۳۹۲ \quad (۷)$$

با توجه به اعداد می‌توان گفت که در استفاده از مجوز INTERNET هیچ تفاوتی بین بدافزار و نرم‌افزارها نیست. اگرچه مجوز READ_SMS یک بهره اطلاعاتی کمتر نسبت به INSTALL_PACKAGES دارد، اما باعث تمایز بدافزارها از نرم‌افزارهای عادی می‌شود و به زبان دقیق‌تر، خطر امنیتی کمتری را داراست. باید به این نکته توجه داشت که خطر امنیتی برای تمامی مجوزهای اندروید بر اساس نرم‌افزارها و بدافزارهای شناسایی شده محاسبه می‌شود. ما این فرایند را برای تمامی مجوزها انجام داده‌ایم. هرچند که ایده ما از

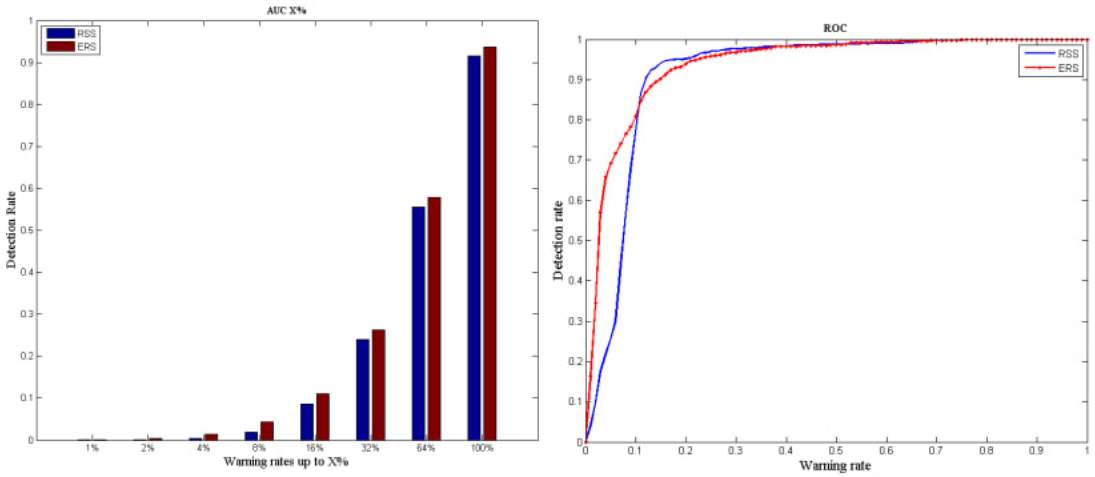
یادگیری ماشین و ساخت درخت تصمیم براساس بهره اطلاعاتی مشتق شده است، اما معیار ما یک هدف کاملاً متفاوت دارد. نخست، هدف ما در این‌جا دسته‌بندی نیست، بلکه محاسبه یک مقدار عددی برای خطر امنیتی برنامه بر اساس آنتروپی و بهره اطلاعاتی مجوزها می‌باشد و ما در این‌جا داده‌ها را لیبل نمی‌زنیم. دوم، ما بهره اطلاعاتی را به‌صورت جداگانه برای همه مجوزها محاسبه می‌کنیم، در حالی که در یک مدل دسته‌بندی، از یک ویژگی شروع به ساخت یک درخت تصمیم کرده و در سطوح مختلفی ساخته می‌شود. فرض کنید با توجه به محاسبات انجام شده، یک برنامه اندرویدی با نام A داریم که از تمامی سه مجوز فوق استفاده کرده است. میزان خطر امنیتی این برنامه به شرح زیر می‌باشد:

$$\text{Risk(A)} = ۰٫۲۶۲۸ + ۰٫۰۳۹۲ + ۰ = ۰٫۳۰۲۰ \quad (۸)$$

این عدد با احتمال مخرب بودن نرم‌افزارِ در دست بررسی، متناسب است. به این معنا که هر چقدر مقدار خطر امنیتی بیشتر باشد، احتمال آسیب‌پذیری برنامه نیز بالاتر است. البته، داشتن یک ریسک امنیتی برای یک برنامه حتماً به معنی آلوده بودن آن به بدافزار نیست، بلکه یک هشدار برای کاربران می‌باشد و یا می‌تواند به عنوان یک پردازش پیشین برای تجزیه و تحلیل‌های دقیق‌تر به‌منظور شناسایی دقیق تهدیدات به کار برده شود. علاوه بر این، میزان خطر امنیتی نسبی است و می‌تواند به انتخاب یک برنامه بهتر و کم‌ریسک‌تر کمک کند. به این ترتیب که با وجود چندین برنامه با قابلیت‌های مشابه و ریسک‌های امنیتی متفاوت، منطقی است که برنامه‌ای با خطر امنیتی کمتر انتخاب شود.

۴ ارزیابی

به‌منظور ارزیابی، با استفاده از مجموعه داده‌های متنوع، روش پیشنهادی با معیارهای مختلف مقایسه شده است. معیارها در نرم‌افزار متلب پیاده‌سازی شده و مورد ارزیابی قرار گرفته‌اند. با توجه به محدودیت صفحات مقاله، تنها نتایج به‌دست آمده از یک مورد از آزمایش‌ها در اینجا گزارش می‌شود. در اینجا، یک مجموعه داده بدافزار و یک مجموعه داده نرم‌افزار برای مقایسه استفاده می‌شوند. مجموعه داده بدافزار شامل ۲۱۲۸ برنامه مفید است که از پلتفرم‌های داخلی فروش برنامه، دانلود و استخراج مجوز شده‌اند. مجموعه داده بدافزار شامل ۱۰۱۴ برنامه اندروید مخرب است است که از منابع مختلف گردآوری و استخراج مجوز شده‌اند. با استفاده از این دو مجموعه داده روش پیشنهادی مبتنی بر آنتروپی ERS (Entropy Based Risk) با روش RSS (Rarity Based Risk Score) که در مرجع [۳] ارائه شده، از نظر نرخ تشخیص بدافزار، مقایسه شده است. در این تجربه، تمرکز بر روی قابلیت شناسایی این معیارها است. یعنی یک معیار موفق است که بتواند به‌طور متناسب برای تهدیدات مقدار خطر امنیتی بیشتری ارزیابی کند. به‌عبارتی، اگر ما برای همه برنامه‌های کاربردی و تهدیدات مقدار ریسک را بر اساس یک معیار محاسبه کنیم و سپس فهرست کلی برنامه‌ها را به‌صورت نزولی بر اساس مقدار ریسک مرتب کنیم، برنامه‌های مخرب بیشتری نسبت به برنامه‌های مفید در بالای فهرست قرار خواهند گرفت. به این منظور، ما در این آزمایش مجموعه‌ای از برنامه‌های مفید و



(الف) نمودار ROC (ب) سطح زیر نمودار (AUC)

شکل ۲: مقایسه نرخ تشخیص معیار پیشنهادی ERS با معیار قبلی RSS بر حسب سطح هشدار

مجموعه‌ای از برنامه‌های مخرب را در یک فهرست یکپارچه قرار داده و با استفاده از ۹۰ درصد فهرست حاصل مدل خود را به وجود آورده‌ایم. سپس با استفاده از ۱۰ درصد باقی‌مانده، به آزمون روش خود می‌پردازیم. به این صورت که با استفاده از مدل تهیه شده، خطر امنیتی آنها را محاسبه کرده و سپس به صورت نزولی مرتب کرده‌ایم. حالا، در هر دوره، درصدهای مختلفی از برنامه‌های برتر فهرست مربوطه را انتخاب کرده و بررسی می‌کنیم که چه نسبتی از تهدیدات در این بخش از فهرست قرار دارند. به درصدهای انتخاب شده از فهرست، سطح هشدار و به درصدهای شناسایی شده تهدیدات، نرخ شناسایی می‌گویند. واضح است که هرچه معیار قدرتمندتر باشد، درصد بیشتری از تهدیدات در بالای فهرست قرار خواهند گرفت و نرخ شناسایی بالاتری خواهد داشت. شکل ۲، بخش‌های الف و ب، به ترتیب منحنی‌های ROC به دست آمده، و سطح زیر نمودار AUC را برای معیار پیشنهادی ERS و معیار RSS [۳] نمایش می‌دهند. در این شکل، محورهای افقی و عمودی به ترتیب نرخ هشدار (Warning Rate) و نرخ شناسایی (Detection Rate) می‌باشند.

همان‌طور که در بخش (الف) شکل ۲ دیده می‌شود، برای مقادیر کم سطح هشدار، روش پیشنهادی ERS از RSS بهتر عمل می‌کند. اما با افزایش سطح هشدار، RSS بهتر عمل کرده است. در بخش (ب) شکل ۲ مشاهده می شود که سطح کلی زیر نمودار به‌ازای مقادیر مختلف نرخ هشدار بیشتر است، زیرا روش پیشنهادی در سطوح هشدار کمتر، برتری قابل توجه‌تری به‌دست آورده است. علت برتری روش پیشنهادی را می‌توان در استفاده از آنتروپی برای متمایز کردن بدافزارها از نرم‌افزارهای مفید، جستجو کرد.

۵ جمع‌بندی و نتیجه‌گیری

معمولاً، برنامه‌های مخرب در سیستم عامل اندروید تلاش می‌کنند تا خود را به عنوان یک اپلیکیشن مفید جلوه دهند. در این زمینه، آنها باید از تعدادی مجوز برای انجام وظایف مفیدشان استفاده کنند، همچنین، برای

اجرای عملیات‌های زیان‌آور نیز به برخی دیگر از مجوزها نیاز دارند. این مسئله باعث می‌شود که کل الگوی استفاده‌شان از مجوزها با اپلیکیشن های مفید متفاوت باشد و در نتیجه، خطر امنیتی ایجاد شده توسط آنها افزایش یابد. ولی ممکن است برخی نرم‌افزارها وجود داشته باشند که مجوزهایی که از آنها استفاده می‌کنند، به‌شدت به بدافزارها شبیه باشد. در این وضعیت، حتی با استفاده از یک معیار امنیتی، برای آنها نیز یک خطر امنیتی بالا تخمین زده می‌شود و معیار پیشنهادی نیز از این قانون استثنا نیست، هرچند که نسبت به سایر معیارها کارآیی بهتری دارد. برای شناسایی دقیق‌تر بدافزارها، استفاده از روش‌های تکمیلی نظیر تجزیه و تحلیل کدهای ایستا و پویا و همچنین تکنیک‌های داده‌کاوی ضروری است. معیار پیشنهادی ما که از ایده‌های آنتروپی و بهره اطلاعات مجوزها برای تشخیص مجوزهای حساس استفاده می‌کند، به نظر می‌رسد که نسبت به معیارهای پیشنهادی پیشین به‌شکل بهتری عمل کند. آزمایش‌ها بر روی مجموعه داده‌های واقعی نشان داده‌اند که معیار پیشنهادی، نسبت به نرم‌افزارهای مفید، مقدار خطر قابل توجه‌تری را ارائه می‌دهد.

مراجع

[1] C. Wilson, “Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress”, Washington, DC, 2008.

[2] C. S. Gates, J. Chen, N. Li, and R. W. Proctor, “Effective risk communication for android apps”, Dependable and Secure Computing, IEEE Transactions on, 11(3), 2014, pp. 252-265.

[3] C. S. Gates, N. Li, H. Peng, B. Sarma, Y. Qi, R. Potharaju, and I. Molloy, “Generating summary risk scores for mobile applications”, Dependable and Secure Computing, IEEE Transactions on, 11(3), 2014, pp. 238-251.

[4] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, “Measuring user confidence in smartphone security and privacy”, In Proceedings of the Eighth Symposium on Usable Privacy and Security, ACM, July 2012. P.1.

[5] [5] A. P. Felt, K. Greenwood, and D. Wagner, “The effectiveness of application permissions,” In Proceedings of the 2nd USENIX conference on Web application development, June 2011, p.7.

[6] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, “Android permissions: User attention, comprehension, and behavior”, Tech. Rep. UCB/EECS-2012-26, UC Berkeley, 2012.

[7] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall, “A conundrum of permissions: installing applications on an android smartphone”, In Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2012, pp. 68-79.

[8] P. G. Kelley, L. F. Cranor, and N. Sadeh, “Privacy as part of the app decision-making process”, In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, April 2013, pp. 3393-3402.

[9] H. Peng, C. Gates, B. Sarma, N. Li, Y. Qi, R. Potharaju, R., and I. Molloy, "Using probabilistic generative models for ranking risks of android apps", In Proceedings of the 2012 ACM conference on Computer and communications security, ACM, October 2012, pp. 241-252.

[10] D. Geneiatakis, I. N. Fovino, I. Kounelis, and P. Stirparo, "A Permission verification approach for android mobile applications", Computers & Security, 49, 2015, pp.192-205.

[11] B. P. Sarma, N. Li, C. Gates, R. Potharaju, C. Nita-Rotaru, and I. Molloy, "Android permissions: a perspective combining risks and benefits", In Proceedings of the 17th ACM symposium on Access Control Models and Technologies, June 2012, pp. 13-22.

[12] L. Cen, C. Gates, L.Si, and N. Li, "A probabilistic discriminative model for android malware detection with decompiled source code", In Dependable and Secure Computing, IEEE Transactions on, vol.12, no.4, 2015, pp.400-412.

[13] A. Desnos, "Android: Static analysis using similarity distance", In System Science (HICSS), 2012 45th Hawaii International Conference on, January 2012, pp. 5394-5403.

[14] A. D. Schmidt, R. Bye, H. G. Schmidt, J. Clausen, O. Kiraz, K. Yüksel, and S. Albayrak, "Static analysis of executables for collaborative malware detection on android", In Communications, 2009. ICC'09. IEEE International Conference on, June 2009, pp. 1-5.

[15] Y. Zhou, Z. Wang, W. Zhou, and X. Jiang, "Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets", In NDSS, Vol. 25, No. 4, February 2012, pp. 50-52.

[16] Y. Aafer, W. Du, and H. Yin, "DroidAPIMiner: Mining API-level features for robust malware detection in android", In Security and Privacy in Communication Networks, 2013, pp. 86-103.

[17] M. Christodorescu, S. Jha, C. Kruegel, "Mining specifications of malicious behavior", In Proceedings of the 1st India software engineering conference, ACM, February 2008, pp. 5-14.

[18] K. Rieck, T. Holz, C. Willems, P. Düssel, and P. Laskov, "Learning and classification of malware behavior", In Detection of Intrusions and Malware, and Vulnerability Assessment, 2008, pp. 108-125.

[19] A. Shabtai, and Y. Elovici, "Applying behavioral detection on android-based devices", In Mobile Wireless Middleware, Operating Systems, and Applications, 2010, pp. 235-249.

[20] I. Burguera, U. Zurutuza, and S. Nadjm-Tehrani, "Crowdroid: behavior-based malware detection system for android", In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, October 2011, pp. 15-26.

[21] H. X. Son, B. Carminati, and E. Ferrari, "A Risk Estimation Mechanism for Android Apps based on Hybrid Analysis", Data Science and Engineering, 2022, pp.1-11.

[22] K. Bakour, and H.M. Ünver, "DeepVisDroid: android malware detection by hybridizing image-based features with deep learning techniques", Neural Computing and Applications, 33, 2021, pp. 11499-11516.

[23] J. Geremias, E. K. Viegas, A. O. Santin, A. O., A. Britto, and P. Horchulhack, "Towards multi-view android malware detection through image-based deep learning", In 2022 International Wireless Communications and Mobile Computing (IWCMC), 2022, pp. 572-577.

[24] I. Almomani, A. Alkhayer, and W. El-Shafai, "An automated vision-based deep learning model for efficient detection of android malware attacks", IEEE Access, 10, 2022, pp. 2700-2720.

[25] R. Quinlan, "Learning efficient classification procedures", Machine Learning: an artificial intelligence approach, Michalski, Carbonell & Mitchell (eds.), Morgan Kaufmann, 1983, pp. 463-482.

[26] Ali, Atif, Nafees Ahmed Somroo, Umer Farooq, Muhammad Asif, Iman Akour, and Wathiq Mansoor. "Smartphone Security Hardening: Threats to Organizational Security and Risk Mitigation". In 2022 International Conference on Cyber Resilience (ICCR), 2022, pp. 1-12. IEEE.

[27] Lin, Wenjun, Ming Xu, Jingyi He, and Wenjun Zhang. "Privacy, security and resilience in mobile healthcare applications". Enterprise Information Systems 17, no. 3, pp.1939896, 2023.

[28] Gull, Hina, Saqib Saeed, Sardar Zafar Iqbal, Yasser A. Bamarouf, Mohammed A. Alqahtani, Dina A. Alabbad, Madeeha Saqib, Saeed Hussein Al Qahtani, and Albandary Alamer. "An empirical study of mobile commerce and customers security perception in Saudi Arabia". Electronics 11, no. 3, pp 293, 2022.

[29] Cinar, Ahmet Cevahir, and Turkan Beyza Kara. "The current state and future of mobile security in the light of the recent mobile security threat reports". Multimedia Tools and Applications. pp. 1-13, 2023.

[30] Kambar, Mina Esmail Zadeh Nojoo, Armin Esmaeilzadeh, Yoohwan Kim, and Kazem Taghva. "A survey on mobile malware detection methods using machine learning". In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0215-0221, 2022.

[31] Kim, Yu-kyung, Jemin Justin Lee, Myong-Hyun Go, Hae Young Kang, and Kyungho Lee. "A systematic overview of the machine learning methods for mobile malware detection". Security and Communication Networks, 2022.

[32] Sk, Heena Kauser. "A literature review on android mobile malware detection using machine learning techniques". In 2022 6th international conference on computing methodologies and communication (ICCMC), pp. 986-991, 2022.

[33] Ullah, Farhan, Xiaochun Cheng, Leonardo Mostarda, and Sohail Jabbar. "Android-IoT Malware Classification and Detection Approach Using Deep URL Features Analysis." Journal of Database Management (JDM), 2023, vol. 34, no. 2, pp. 1-26.

چالش‌های اجتماعی و امنیتی در توسعه متاورس

جمشید نصرت آبادی[۱]، مجید سلیمانی ساسانی[۲]، امیرمحمدشیرخدا[۳]

[۱]استادیار و عضو هیئت علمی دانشگاه فارابی، تهران، ایران
dr.nosratabadi110@gmail.com
[۲]استادیار و عضو هیئت علمی دانشگاه تهران، تهران، ایران
msoleimani@ut.ac.ir
[۳]دانشجوی کارشناسی ارشد، دانشگاه فارابی، تهران، ایران
ariadata@ymail.com

چکیده

با توجه به گسترش روز افزون دانش و فناوری، مفاهیم و واژگان جدیدی جای واژگان قدیمی را پر می‌کنند. پس از شکست پروژه زندگی دوم، آرزوها و دست‌نیافتنی‌های واقع در ذهن بشر تمام نشد، بلکه جای خود را با مفهومی کامل‌تر و جامع‌تر به نام متاورس تکمیل کرد. توجه به پیوست اجتماعی و اخلاقی تکنولوژی‌های نوظهور از مهم‌ترین عوامل رشد و توسعه آنها می‌باشد. اما در متاورس فعلی فقط شاهد تغییر در تجارت دارایی‌های مجازی به‌صورت آنلاین و در بازی‌های آنلاین هستیم، جایی که کاربران می‌توانند دارایی‌های دیجیتال مانند لوازم جانبی برای آواتارها را ایجاد و یا خرید و فروش کنند. ما در این پژوهش ضمن بازخوانی مفاهیم مطرح شده برای کلیدواژه متاورس و تکنولوژی‌های در دسترس، به بیان چالش‌ها و مشکلات اجتماعی و امنیتی که در راه تکامل این تکنولوژی و یا مفهوم آن به‌کار می‌آید با دسته‌بندی کپی‌رایت، حریم‌خصوصی، نگهداری و حفاظت از داده‌ها در بخش امنیتی و هویت افراد، تبعیض و سوگیری، سلامت افراد، قطبیت در جامعه، آزادی، قوانین و حکومت‌ها در بخش اجتماعی می‌پردازیم. لازم به ذکر است این مقاله با استفاده از مطالعات کتابخانه‌ای مقالات معتبر متعدد در این حوزه تنظیم شده است.

کلمات کلیدی: متاورس، چالش‌های متاورس، اخلاق در متاورس، فراجهان، دنیاهای مجازی، واقعیت مجازی، هوش‌مصنوعی، حریم‌خصوصی.

۱ مقدمه

شاید بتوانیم فیلم‌ها و داستان‌های علمی خیلی، از فیلم‌های سفر به اعماق زمین گرفته تا موضوعات مرتبط با تکامل تکنولوژی از قبیل ماتریکس (The Matrix) در سال ۱۹۹۹، بازیکن شماره یک (Ready Player One) در سال ۲۰۱۸ و ... را اولین نمایش و تعریف از تکامل خواسته‌ها و آرزوهای بشر دانست [Hutson ،۷ and other, 2023: 2]. در طول ۲۰ تا ۳۰ سال گذشته، الگوی رابط کاربری محصولات تکنولوژی، به تدریج

از مردم سازگار با فن‌آوری به فن‌آوری سازگار با مردم تغییر کرده است. در این میان زبان‌های برنامه‌نویسی پیچیده به متن‌های ساده، که غنی از رابط‌های گرافیکی مانند پنجره‌ها، مرورگرها، برنامه‌ها و صداها است و باعث ایجاد تکامل در رابط‌های شناختی می‌شود، تغییر یافت [۴، Benjamins and other, 2023: 691].

رابط‌های سه بعدی تنها تکامل بعدی همین مفهوم هستند که از تکنولوژی‌های جدید (واقعیت مجازی – VR، واقعیت افزوده – AR، واقعیت ترکیبی – MR) و قابلیت‌های (به‌عنوان مثال، محاسبات با کارایی بالا، فضای ابری و اتصال با سرعت بالا) بهره می‌برند. در آینده، علاوه بر بینایی و شنوایی، رابط کاربری ممکن است شامل عناصری از سه حس دیگر مانند لمس (تا حدی که در حال حاضر از طریق رابط‌های لمسی در دسترس است)، چشایی و بویایی نیز باشد (همان).

متاورس اخیرا اهمیت خود را در فضای وب افزایش داده است. پلتفرم‌های آنلاین مانند دسنترالند و سندباکس، اولین دنیای مجازی مستقر شده با استفاده از ابزارهای غیرمتمرکز (به عنوان مثال، بلاک‌چین) را به نمایش می‌گذارند. همچنین پلتفرم‌های متعددی در این مسیر وجود دارند که در علاقه‌مندی‌های اخیر به متاورس نقش داشته‌اند؛ مانند: سکندلایف، ماینکرفت و روبلاکس؛ و شرکت‌هایی مانند نیانتیک، مایکروسافت (با مش) و اخیرا متا (که قبلا با نام فیسبوک شناخته می‌شد) [۱، Fernandez and other, 2022: 1].

با وجود علاقه‌مندی‌های بوجود آمده و گسترش روزافزون این پلتفرم‌ها، همواره در کنار چالش تکنولوژی برای دستیابی به جهانی فراتر از جهان فعلی، چالش‌های اجتماعی و امنیتی نیز وجود داشته است. شناسایی و معرفی چالش‌های موجود در تکنولوژی خود مقدمه‌ای برای بهبود بهره‌برداری کامل از متاورس است. در این مطلب به چالش‌های مهمی می‌پردازیم که متاورس از نظر امنیت و حریم‌خصوصی، اخلاقی و اجتماعی با آن‌ها مواجه خواهد شد.

۲ امنیت در متاورس

متاورس برای ارائه تجربه‌های همه جانبه، از داده‌های جمع‌آوری شده‌ی دنیای واقعی استفاده می‌کند و کاربران با سنسورهای متصل شده (مثلا ژیروسکوپ برای ردیابی حرکات سر) می‌توانند به صورت واقع‌گرایانه آواتار خود را کنترل کنند. علاوه بر این، متاورس چالش‌های جدیدی را نیز در دنیای مجازی عظیم خود باز می‌کند که در آن کاربران می‌توانند در معرض حملات حریم خصوصی مانند استراق سمع توسط دیگر کاربران پلتفرم قرار بگیرند [۱، Fernandez and other, 2022: 1].

۱.۲ کپی رایت

چه کسی حق چاپ و فروش یک اثر هنری تولید شده توسط یک سیستم هوش مصنوعی را دارد؟ مانند یک آهنگ یا یک نقاشی ایجاد شده توسط Dall.e2.4[۱] یا یک متن توسط LaMDA[۲] یا حتی یک قطعه کد برنامه

[۱] یکی از جدیدترین پیشرفت‌ها در حوزه هوش‌بصری، هوش مصنوعی Dall-E است؛ هوش مصنوعی‌ای که می‌تواند تصاویر منحصربه‌فردی را بر اساس دستور متنی شما ایجاد کند.

[۲] مخفف عبارت Language Model for Dialog Application می‌باشد. به زبان ساده‌تر، یک مدل یادگیری ماشینی زبان بوده که به‌طور خاص برای ایجاد گفتگوی طبیعی طراحی شده است.

نویسی توسط Copilot۵ که بصورت کاملا طبیعی و با استفاده از تکنولوژی در حال تکامل هوش‌مصنوعی تولید شده است [۴، Benjamins, 2023: 693].

برای مثال، در سپتامبر ۲۰۲۲ یک نقاشی با نام Theatre D'opera Spatial در مسابقه‌ی سالانه هنرهای زیبای نمایشگاه ایالت کلرادو برنده می‌شود، درحالی که داوران و تحسین‌کنندگان آن زمان نمی‌دانستند که این محصول تخیل یک نقاش نبوده است و محصول یک هوش مصنوعی است.

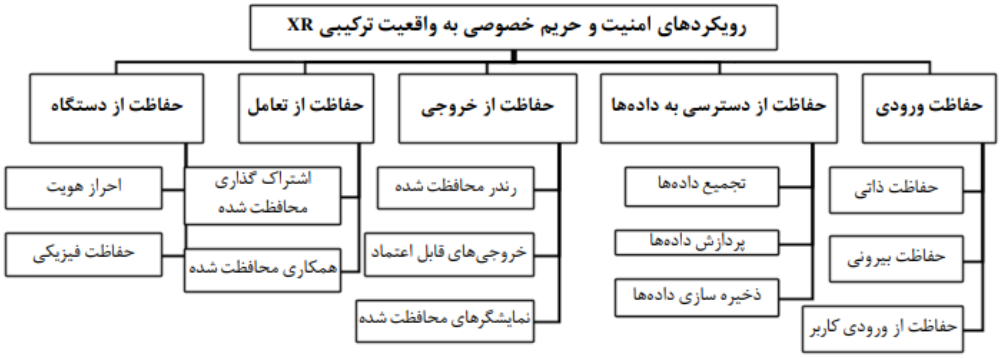
پس از آنکه طوفان اعتراضات و بحث‌های داغ در نشریه‌ای به راه افتاد و در آن به تقلب و ارسال اثری بدون مهارت، هنر یا پیام متهم شد، جیسون ام آلن خالق اثر این واقعیت را آشکار کرد. یکی از جدیدترین مدل‌های هوش مصنوعی با کیفیت «تصویر مبتنی بر متن» برنده این جایزه بود. تنها کاری که باید انجام دهید این است که یک نمای کلی به‌صورت مکتوب از آنچه می‌خواهید ترسیم کنید را به هوش مصنوعی بدهید. رایانه همه کارها را انجام خواهد داد [۱۰، Roose, 2022].

در مثال‌هایی دیگر؛ برخی از کشورهای اطراف ساحل مدیترانه مدعی مالکیت تصاویر تاریخی در کشورهای خود هستند. تلاش بنگلادش برای ساختن ماکت تاج محل با مخالفت هند مواجه شد. شیکاگو عکاسان حرفه‌ای را از عکاسی از پارک هزاره شهر بدون اجازه منع کرد و ادعا کرد که این پارک توسط قوانین کپی رایت محافظت می‌شود (Chen, 2023:5). علاوه بر تولیدات هوش مصنوعی، بحث فروش مالکیت برندها و یا آثار تولید شده توسط اشخاص در متاورس هم مطرح است، که البته با وجود NFT بخشی از این موضوع قابل حل است و در موارد کمی هم قوانین تجارت الکترونیکی در کشورها راه‌گشا خواهند بود. [۴، Benjamins, 2023: 696]

۲.۲ حریم خصوصی

رابطه و تعاملات اجتماعی می‌تواند برای استنباط عادات، فعالیت‌ها و انتخاب‌های کاربران در متاورس ارزشمند باشد. مشابه داده‌های بیومتریک، این اطلاعات می‌تواند روان کاربران را توصیف کنند. علاوه بر این، فراداده‌های ذاتی در هر تعامل اجتماعی با سایر آواتارها (مانند: مکالمات، واکنش‌ها) خطرات حریم‌خصوصی را برای کاربران به همراه دارند. این اطلاعات می‌تواند برای ردیابی و تنظیم رفتار کاربران مفید باشد. چه کسی کنترل همه این اطلاعات را در دست دارد [۱، Fernandez and other, 2022: 4]؟ تبلیغات هدفمند و نگرانی‌های مربوط به حفظ حریم‌خصوصی داده‌ها سر به فلک کشیده و این باور وجود دارد که این اطلاعات می‌توانند بسیار مزاحم شوند [۴، Benjamins, 2023: 693].

فناوری‌های XR چندین تهدید حریم‌خصوصی و امنیتی را برای کاربران و تماشاگران ایجاد می‌کنند. این فناوری‌ها معمولاً از حسگرها برای اسکن و نظارت بر محیط اطراف کاربران استفاده می‌کنند. این اسکن‌ها می‌توانند اطلاعاتی را جمع‌آوری کنند که ممکن است برای کاربران و تماشاگرانی که در منطقه تحت پوشش مانیتورینگ قرار دارند، محسوس باشد. نمایشگرهای روی سر (HMDها) که معمولاً برای نمایش متاورس استفاده می‌شوند، می‌توانند برخی از داده‌های بیومتریک (حرکت سر، ردیابی چشم) را جمع‌آوری کنند که برای کاربران محسوس نیست. به عنوان مثال، زل زل نگاه کردن به کاربران دیگر می‌تواند ترجیحات جنسی کاربران را از بین ببرد. داده‌های بیومتریک جمع‌آوری شده، شخصی‌ترین جنبه‌های روان ما را در معرض خطر



شکل ۱: دسته بندی داده محور از کارها یا رویکردهای مختلف امنیت و حریم خصوصی در واقعیت ترکیبی و فناوری‌های مرتبط [De Guzman, 2019: 9 ،۸]

قرار می‌دهد. بنابراین، این دستگاه‌ها باید با داده‌ها مطابق اصولی رفتار کنند که از حریم‌خصوصی کاربران محافظت می‌کند. [Fernandez and other, 2022: 4 ،۱] از طرفی پیش بینی می‌شود همان شرکت‌های بزرگی که تا پیش از این نیز در نگه داشت، امنیت و فروش داده‌ها سابقه‌ی خوبی نداشته‌اند وارث این اطلاعات باشند که خود از موانع و چالش‌های مهم گسترش و پذیرش متاورس در میان افراد می‌باشد.

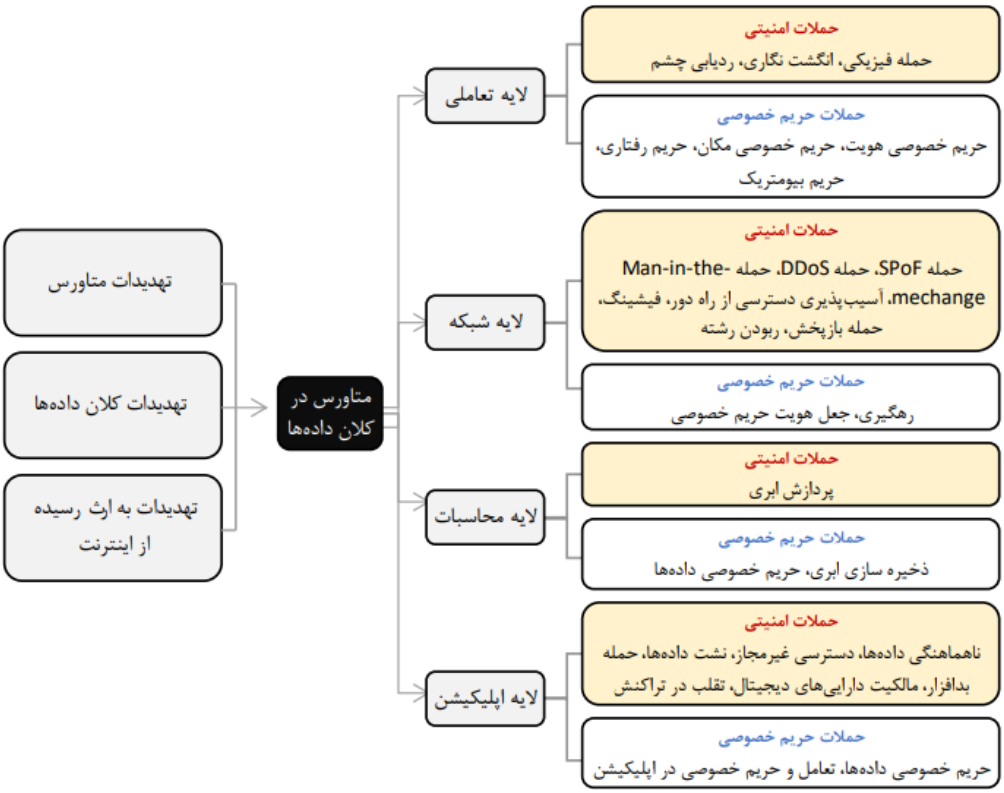
۳.۲ حفاظت و نگهداری از داده‌ها

از آنجایی که متاورس جدیدترین فناوری‌ها و سیستم‌های ساخته شده را ادغام می‌کند، آسیب‌پذیری‌ها و نقص‌های ذاتی آن فناوری‌ها نیز ممکن است به ارث برسد. حوادثی از فناوری‌های نوظهور مانند ربودن دستگاه‌های پوشیدنی یا فضای ذخیره‌سازی ابری، سرقت ارزهای مجازی و سوء رفتار هوش مصنوعی برای تولید اخبار جعلی وجود داشته است. ثانیاً، با درهم آمیختن فناوری‌های مختلف، تأثیرات تهدیدات موجود می‌تواند در دنیای مجازی تقویت شده و شدیدتر شود، در حالی که تهدیدهای جدیدی که در فضاهای فیزیکی و سایبری وجود ندارند، می‌توانند مانند تعقیب مجازی و جاسوسی مجازی و ... در متاورس ایجاد شوند [wang and others, 2022: 1 ،۱۱].

باید توجه داشته باشیم روش‌های فعلی ذخیره ابری اطلاعات حساس به حریم خصوصی، در سرورهای ابری و رایانش مرزی (Edge computing) نیز تهدیداتی برای حفظ حریم خصوصی در حفاظت از اطلاعات دارد. به‌عنوان مثال، پایگاه داده Second Life (یک بازی متاورس) هک شده بود و مقدار زیادی از اطلاعات کاربران، از جمله جزئیات پرداخت و رمز عبور، به بیرون درز پیدا کرده بود [Chen, 2023: 7 ،۵].

متاورس دارای ویژگی‌های اجتماعی قوی مانند: بازی‌های چند نفره و همکاری از راه دور است و کاربردهای آن معمولاً چند کاربره است. نحوه دستیابی به اشتراک گذاری محتوای ایمن و کارآمد در محیط XR در متاورس به چالشی در استفاده از داده تبدیل می‌شود. علاوه بر این، به اشتراک گذاری و پردازش محتوای تولید شده توسط کاربر (UGC) نیز در متاورس مهم است. چگونگی کاهش بار ارتباطی، بدون تأثیر

بر اعتبارسنجی محتوا نیز چالشی برای متاورس است [همان].



شکل ۲: جدول تهدیدات امنیتی و حریم خصوصی و دسته‌بندی در کلان‌داده‌ی متاورس برای لایه‌های مختلف [Sun, 2022: 10 ،۳]

۳ اجتماع در متاورس

متاورس علاوه بر این‌که انواع جدیدی از فعالیت‌ها را ممکن می‌سازد، می‌تواند میزبان تقریباً تمام فعالیت‌هایی (مانند: معاشرت، کار، یادگیری، سرگرمی، خرید، تولید محتوا و ...) باشد که ما به‌صورت روزمره در آن‌ها شرکت داریم [Benjamins, 2023: 690 ،۴]. متاورس این پتانسیل را دارد که جامعه فعلی ما را متحول کند، جایی که کانال‌های جدیدی برای بیان خود و تعامل با دیگران بدون هیچ محدودیتی (مکان، زمان، نژاد، جنسیت) وجود دارد [Fernandez and other, 2022: 4 ،۱]. اما در این‌میان چالش‌هایی نیز وجود دارد، که در ادامه به بررسی آنها می‌پردازیم.

۱.۳ هویت افراد

در متاورس می‌توانید به جهان‌های مجازی مختلف با هویت یکسان دسترسی داشته باشید، بنابراین پیامدهای منفی جعل هویت بسیار شدیدتر از آن چیزی است که در حال حاضر در سرویس‌های دیجیتال وجود دارد و هر سرویس نام کاربری متفاوتی دارد [۴، Benjamins, 2023: 695].

اگر هویت شما ربوده شود، در برابر باج‌افزارها و اخاذی آسیب‌پذیرتر هستید. با سرویس‌های دیجیتال می‌توانید رمز عبور خود را تنظیم کنید؛ با این حال، در متاورس نمی‌توانید به سادگی آواتار خود را تغییر دهید چرا که مستقیما به وجود مجازی شما متصل است و تکنیک‌های جعل عمیق در سرقت هویت شما نقش خواهند داشت [همان].

۲.۳ سلامت افراد

علاوه بر اینکه ممکن است دستگاه‌های پوشیدنی در متاورس از نظر سلامتی، به متخصصان پزشکی کمک کند تا داده‌های فیزیولوژیکی بیماران مانند: دمای بدن، ضربان قلب و فشار خون را بررسی و نظارت کنند، این توانایی را نیز دارد که فرد متوفی را با استفاده از داده‌های بیومتریک او «احیا کند» [۵، Chen, 2023: 2]. اما باید بدانیم در این بین چالش‌هایی وجود دارد که در ادامه به آن می پردازیم:

برخی الگوریتم‌های پیشنهاد به قدری خوب هستند که کاربران نمی‌توانند از محتوای ارائه شده توسط آن‌ها جدا شوند. از نمونه‌های خاص می‌توان به اینستاگرام و تیک‌تاک اشاره کرد که ویدئو را به صورت کاملاً شخصی‌سازی شده به علاقه‌مندان ارائه می‌دهند. برخی از افراد به خصوص جوانان ممکن است به این اپلیکیشن‌های شبکه‌های اجتماعی اعتیاد پیدا کنند. آنها می‌توانند ساعت‌های زیادی در روز را صرف این موارد کنند و زمانی که در نهایت قطع ارتباط می‌کنند، احساس اضطراب می‌کنند و باید در اسرع وقت دوباره به هم متصل شوند. گیمینگ هم چالش مشابهی دارد، زمانی که هوش‌مصنوعی تجربه را بسیار بهینه می‌کند، مردم نمی‌توانند بازی را متوقف کنند و وقتی این کار را می‌کنند، احساس ناراحتی می‌کنند [۴، Benjamins, 2023: 694 as cited in Merkx, 2021]. اعتیاد به فن‌آوری را در سلامتی نباید دست‌کم گرفت، زیرا قدرت الگوریتم‌های تعامل (توصیه) در یک محیط همه جانبه مانند متاورس بسیار زیاد است؛ توصیه‌ها در یک پلتفرم متاورسی می‌توانند به قدری خوب باشند که فراتر از یک نقطه خاص، افراد ممکن است ترک فضا را در زمانی که باید/ می‌خواهند (بیش از حد) دشوار بدانند.

استفاده وسواسی از متاورس برای فرار از دنیای واقعی: افرادی که در دنیای واقعی شاد نیستند، ممکن است جایگزین جذابی در دنیای مجازی پیدا کنند که بتوانند همان کسی باشند که می‌خواهند باشند. آنها به‌جای اینکه برای بهبود زندگی واقعی خود تلاش کنند، از آن فرار می‌کنند و زندگی واقعی را به‌طور فزاینده‌ای بدتر می‌بینند.

کودکان به‌خصوص در برابر فناوری‌های فراگیر آسیب‌پذیر هستند، زیرا احتمال دارد واقعیت را با دنیای مجازی اشتباه بگیرند.

آزار و اذیت سایبری احتمالاً افزایش می‌یابد و تأثیر منفی بزرگ‌تری از طریق تجربه دیجیتالی پیشرفته و

فراگیر خواهد داشت که تقریباً به عنوان واقعیت درک می‌شود.

ناراحتی پس از واقعیت مجازی ایجاد می‌شود به‌طوری که دنیای واقعی ناامید کننده می‌شود و مردم احساس غم و اندوه را تجربه می‌کنند. واقعیت مجازی «خماری» یا بیماری سایبری، حتی گاهی با نشانه‌های فیزیکی همراه است که نشان‌دهنده احساس تهوع، خستگی، سرگیجه و بی‌نظمی بدنی است [۴، Benjamins, 2023: 694].

۳.۳ تبعیض و سوگیری

صدها مقاله در مورد این موضوع نوشته شده است که در آن سیستم‌های هوش مصنوعی، ممکن است براساس سوگیری، به تبعیض نامطلوب/غیرقانونی گروه‌های آسیب‌پذیر منجر شوند. در سیستم قضایی آمریکا با سیاه‌پوستان متفاوت از سفیدپوستان رفتار می‌شود، زنان وام‌های کمتری از بانک‌ها دریافت می‌کنند و کمتر توسط شرکت‌ها استخدام می‌شوند، فقط به خاطر جنسیتشان، و ... [۴، Benjamins, 2023: 692].

متاورس پر از اپلیکیشن‌هایی خواهد بود که از هوش مصنوعی برای پیش‌بینی و طبقه‌بندی استفاده می‌کنند و بنابراین این چالش نیز چالشی برای متاورس است [همان].

۴.۳ قطبیت در جوامع

الگوریتم‌های پیشنهاد می‌توانند حباب‌های فیلتری (Filter Bubbles) ایجاد کنند که در آن افراد تنها آنچه را که به آن علاقه دارند ببینند، تفکر خود را تقویت کنند و آن‌ها را از دیدگاه‌های جایگزین دور کنند. همان‌طور که در برخی از انتخابات‌ها و دیگر رویدادهای مهم دموکراتیک دیده‌ایم، الگوریتم‌های هوش‌مصنوعی می‌توانند در زمان نزدیک بودن انتخابات در بینش افراد تفاوت ایجاد کنند. باتوجه به تجربه همه‌جانبه متاورس، این ریسک احتمالا افزایش خواهد یافت [۴، Benjamins, 2023: 694].

۵.۳ آزادی

اگر متاورس ملزم به پیروی از قوانین محلی باشد، ماژول‌ها بر این اساس عوض می‌شوند؟ سؤال این است که چگونه با کاربران سایر مکان‌های جغرافیایی رفتار می‌شود و چگونه می‌توان این قوانین محلی را در متاورس اعمال کرد و دنیای مجازی جهانی را هدف گرفت. آیا تعاریف کشورهای مختلف از آزادی یکسان است؟ آیا کشورهای مدعی آزادی باید به قوانین سایر کشورها در این حوزه احترام بگذارند [۱، Fernandez and other, 2022: 4]؟

همان‌طور که دیدیم، یک عنصر کلیدی متاورس، واقعیت ترکیبی (MR) است، ترکیبی از دنیای دیجیتال و واقعی با استفاده از فناوری‌های واقعیت مجازی (VR) و واقعیت افزوده (AR). در نهایت، این ترکیب ممکن است آنقدر فراگیر شود که زندگی مجازی و واقعی مردم به هم گره بخورد و قابل تشخیص نباشد. اگر این اتفاق بیفتد، هر کسی که (بخش قابل توجهی از) متاورس را کنترل کند، می‌تواند بخش قابل توجهی از واقعیت را کنترل کند [۴، Benjamins, 2023: 695] و باید در نظر داشته باشیم ایجاد تعادل مناسب بین

آزادی بیان و پرهیز از محتوای مخرب برای انتشار در متاورس بسیار سلیقه‌ای و پیچیده است. [۵، Chen، ۲۰۲۳:۴]

۶.۳ قوانین و حکومت‌ها

اینترنت حقوق حاکمیت دولت‌ها را به چالش کشیده است، درنتیجه دولت‌ها می‌کوشند تا از روش‌های گوناگون حقوق حاکمیتی خود را بر اینترنت افزایش دهند [۱۳، حسنی، ۱۴۰۱: ۱۶۵ برگرفته از Puyvelde and Brantly,2019]. باتوجه به قوانین مختلف حاکم بر کشورها و فرهنگ و آداب و رسوم خاص هر حاکمیتی، چشم‌انداز متاورس تنها در یک مدل چندذی‌نفعی، با چندین طرف و ارائه‌دهندگان خدمات که برای ارائه طیف ارزش کاربران نهایی همکاری می‌کنند، تحقق می‌یابد. یکی از جنبه‌های مهم، که بر پذیرش گسترده متاورس حاکم است، امنیت و همچنین نگرانی‌های مرتبط با آن مانند اعتماد، حریم خصوصی و کنترل است [۹، Gupta and others, 2023: 2].

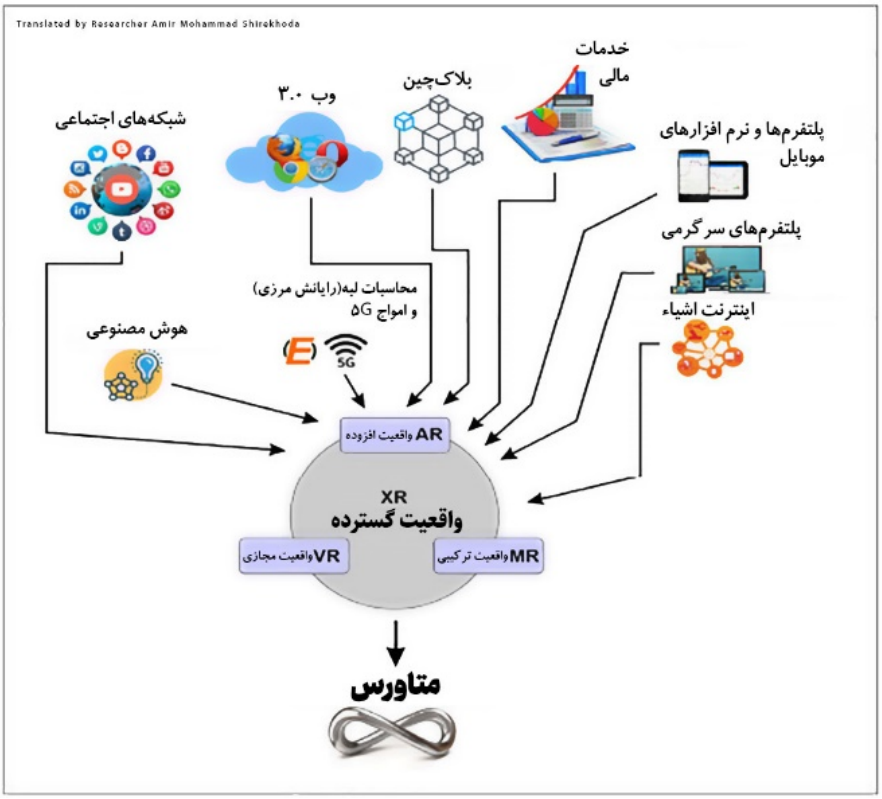
بنابراین ذی‌نفعان چندین کشور که باهم در ارتباط هستند، دور هم جمع می‌شوند، تا در مورد این که چگونه فن‌آوری می‌تواند یک ریسک اجتماعی یا اخلاقی را شکل دهد گفتگو کنند و توصیه‌هایی را به شرکت‌ها و دولت‌ها برای مقابله با آن‌ها صادر کنند. مثال‌هایی از چنین ابتکاراتی برای هوش‌مصنوعی عبارتند از: اصول هوش‌مصنوعی OECD و توصیه هوش‌مصنوعی یونسکو. سپس سازمان‌های فردی می‌توانند به دستورالعمل‌ها پایبند باشند. ما به شدت بر اهمیت چنین بحث‌های بین رشته‌ای و جهانی در مورد ریسک‌های اجتماعی و اخلاقی متاورس، از جمله مشارکت‌های عمومی خصوصی تاکید می‌کنیم. این بحث‌ها ورودی ضروری مقررات بالقوه هستند [۴، Benjamins, 2023: 695]. از آنجایی که دنیای متاورس بزرگتر از وب ۰.۲ است، هزینه نظارت نیز یک مشکل کلیدی است که باید حل شود. ما می‌توانیم از مقررات ضعیف فعلی رسانه‌های اجتماعی یاد بگیریم که شرکت‌های بزرگ فناوری همیشه سود را بر حقوق یا اخلاق ترجیح می‌دهند. بنابراین، شرکت‌هایی که بسترهای آموزشی متاورس را ارائه می‌دهند، تنها می‌توانند اپراتور باشند و نباید رگولاتور مطلق باشند. اینکه آیا تخلفی وجود دارد یا خیر، باید توسط اکثریت قریب به اتفاق کاربران درگیر تعیین شود. باید بین منافع شرکت و کاربران تعادل ایجاد کند [۶، lin، ۲۰۲۲:۸].

رگولاتوری و یا مقررات‌گذاری به این معنی است که برخی از کاربردهای این فن‌آوری توسط قانون کنترل شود. GDPR (مقررات حفاظت از داده اروپا) و قانون AI (مقررات آتی هوش مصنوعی اروپا) نمونه‌هایی از این موارد هستند. و البته یک رویکرد مبتنی بر ریسک به مقررات نشان می‌دهد که هر چه ریسک بالاتر باشد، قوانین بیشتری اعمال می‌شود. با توجه به تأثیر گسترده بالقوه متاورس، عاقلانه است که در مورد خطرات مهمی که ما - به عنوان جوامع - می‌خواهیم مطمئناً از آن‌ها اجتناب کنیم، فکر کنیم. اگر تنظیم متاورس خیلی زود انجام شود، این خطر وجود دارد که هنوز تجربه واقعی کمی از تأثیر اجتماعی و اخلاقی آن داشته باشیم [۴، Benjamins, 2023: 695].

۷.۳ مدل سامانه و فرضیات

اگرچه متاورس همان‌طور که پیش‌بینی می‌شد امروزه وجود ندارد، اما بسیاری از تکنولوژی‌های پشتیبانی کننده در حال رشد و توسعه آن می‌باشند. ادغام این فناوری‌ها همراه با پیشرفت‌های جدید، به تحقق چشم‌انداز آینده متاورس کمک خواهد کرد.

اکوسیستم فن‌آوری که در شکل ۳ نمایش داده شده است، متاورس را فعال می‌کند. کاملاً واضح است که فن‌آوری AR / VR / MR و XR بسترهای متاورس هستند و به کاربران اجازه می‌دهند به یک دنیای مجازی سه بعدی دسترسی داشته باشند. متاورس ممکن است در اولین دیدار، مجموعه‌ای از برنامه‌های کاربردی وب ۳.۰ با یک روکش واقعیت گسترده باشد که تجربه واقعیت مجازی محدودی را فراهم می‌کند. انتظار می‌رود شبکه‌های اجتماعی جزو اولین شبکه‌هایی باشند که به متاورس مهاجرت می‌کنند و به کاربران اجازه اشتراک‌گذاری و مصرف محتوای فراگیر همراه با وب ۳.۰ را می‌دهند. همچنین این فن‌آوری به کسب‌وکارها اجازه می‌دهد تجربه جدیدی از محصول را به کاربران ارائه دهند [۹، Gupta and others, 2023: 5].



شکل ۳: اکوسیستم فن‌آوری که متاورس را فعال می‌کند. [۹، Gupta،۲۰۲۳:۶]

۴ نتیجه‌گیری

متاورس در حال تکامل است و هنوز به بلوغ مورد انتظار خود نرسیده است و دولت‌ها و شرکت‌های مختلفی درصدد ایجاد و تکامل آن هستند. اما در این میان چالش‌هایی با توجه به تکنولوژی‌ها و فن‌آوری‌های فعلی برای ایجاد آن از لحاظ اجتماعی و امنیتی وجود دارد.

کپی رایت و این که چه کسی حق چاپ و فروش یک اثر هنری تولید شده توسط یک سیستم هوش مصنوعی را دارد؟ و یا جعل‌های آثاری که توسط هوش مصنوعی در دنیای فیزیکی فعلی و دنیای متاورسی قرار دارد از چالش‌های متاورس است. جمع‌آوری داده‌ها و اطلاعات شخصی افراد توسط سخت‌افزارهای پوشیدنی متاورس، دزدیده شدن ابزار، پول‌ها و اعتبار مجازی، حملات امنیتی در لایه تعامل، شبکه، محاسبات و اپلیکیشن، جعل هویت و اخاذی سایبری، تبعیض‌های نژادی، جنسیتی و ... هوش مصنوعی در متاورس، از بین رفتن سلامتی با استاده نادرست از پوشیدنی‌ها و یا ابزارهای متاورسی، اعتیاد نوجوانان و جوانان به الگوریتم‌های پیشنهاد قوی و وقت گذرانی دائمی در این فضا و عدم توانایی در برنامه‌ریزی صحیح و درست در زندگی فیزیکی واقعی، آزار و اذیت سایبری، شکل‌دهی به افکارعمومی و ایجاد قطبیت در جامعه، تعریف متفاوت حکمرانان از آزادی در این فضا، در نظر گرفته نشدن قوانین کشورها، احترام نگذاشتن به آداب و رسوم و فرهنگ جوامع و الزام به رعایت قوانین محلی اپلیکیشن در سطح جهانی از چالش‌های اجتماعی و امنیتی متاورس با توجه به سخت‌افزارها و نرم‌افزارهای موجود می‌باشد.

مراجع

[۱] حسنی، حسین، ۱۴۰۱، چالش‌های نوظهور دولت‌ها برای حکمرانی فضای سایبر، پیامدهای پلتفرمی شدن و پیدایش متاورس، نشریه علوم سیاسی، سال بیست و پنجم، شماره نود و هشتم، تابستان ۱۴۰۱.

[2] C. B. Fernandez and P. Hui, “Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse”, 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW), Bologna, Italy, 2022, pp. 272-277, doi: 10.1109/ICDCSW56584.2022.00058.

[3] Sun, J., Gan, W., Chen, Z., Li, J. and Yu, P.S., 2022. Big data meets metaverse: A survey. arXiv preprint arXiv:2210.16282.

[4] Benjamins, R., Rubio Viñuela, Y. and Alonso, C. Social and ethical challenges of the metaverse. AI Ethics 3, 689–697 (2023). https://doi.org/10.1007/s43681-023-00278-5

[5] Chen, C., Li, Y., Wu, Z., Mai, C., Liu, Y., Hu, Y., Zheng, Z. and Kang, J., 2023. Privacy Computing Meets Metaverse: Necessity, Taxonomy and Challenges. arXiv preprint arXiv:2304.11643.

[6] Lin, H., Wan, S., Gan, W., Chen, J., & Chao, H.C., 2022, December. Metaverse in education: Vision, opportunities, and challenges. In 2022 IEEE International Conference on Big Data (Big Data) (pp. 2857-2866). IEEE.

[7] Hutson, J., Banerjee, G., Kshetri, N., Odenwald, K., & Ratican, J., 2023. Architecting the Metaverse: Blockchain and the Financial and Legal Regulatory Challenges of Virtual Real Estate. Journal of Intelligent Learning Systems and Applications, 15.

[8] De Guzman, J.A., Thilakarathna, K., & Seneviratne, A., 2019. Security and privacy approaches in mixed reality: A literature survey. ACM Computing Surveys (CSUR), 52(6), pp. 1-37.

[9] Gupta, A., Khan, H.U., Nazir, S., Shafiq, M., & Shabaz, M., 2023. Metaverse Security: Issues, Challenges and a Viable ZTA Model. Electronics, 12(2), p. 391.

[10] Roose, K., 2022. An AI-generated picture won an art prize. Artists aren't happy. The New York Times, 2 September.

[11] Wang, Yuntao, Zhou Su, Ning Zhang, Dongxiao Liu, Rui Xing, Tom H. Luan, & Xuemin Shen, 2022. A Survey on Metaverse: Fundamentals, Security, and Privacy.

[12] Merkx, C., Jeroen, N. 2021. Virtual reality tourism experiences: addiction and isolation. Tour. Manag. 87, 104.

[13] Puyvelde, D.V. and Brantly, A.F., 2019. Cybersecurity: Politics, Governance and Conflict in Cyberspace. Cambridge: Polity Press.

مدیریت داده‌های پزشکی با کمک زنجیره بلوکی

زهرا امین مهر [۱]، فضل الله ادیب نیا [۲]

[۱] دانشجوی کارشناسی ارشد شبکه‌های کامپیوتری، فناوری اطلاعات، دانشگاه یزد، یزد
zahraaminmehr@stu.yazd.ac.ir
[۲] دانشیار دانشکده مهندسی کامپیوتر، فناوری اطلاعات، دانشگاه یزد، یزد
fadib@yazd.ac.ir

چکیده

در سال‌های اخیر، صنعت مراقبت‌های بهداشتی شاهد تحولی انقلابی با ادغام دستگاه‌های پزشکی به هم پیوسته، تجزیه و تحلیل داده‌ها و اتصال به اینترنت بوده است. اینترنت اشیاء پزشکی به شبکه‌ای از دستگاه‌های پزشکی، حسگرها، برنامه‌های کاربردی نرم‌افزاری و سیستم‌هایی اشاره دارد که برای بهبود ارائه مراقبت‌های بهداشتی، نظارت بر بیمار و رفاه کلی، به هم مرتبط هستند. این زیست‌بوم به هم پیوسته به دستگاه‌های پزشکی اجازه می‌دهد تا به طور یکپارچه با یکدیگر ارتباط برقرار کنند، اطلاعات مهم سلامتی را جمع آوری و تبادل کنند. با این حال، این داده‌ها بسیار حساس هستند و به یک سیستم ذخیره‌سازی و مدیریت ایمن و قابل اعتماد، نیاز دارند. در اینترنت اشیاء پزشکی چالشی که وجود دارد بحث امنیت و صحت داده‌ها و همچنین احراز هویت پزشکان و بیماران است. جهت برطرف نمودن این چالش، روش‌های مختلفی ارائه شده که هرکدام مزایا و معایبی دارند. معماری پیشنهادی در این مقاله ترکیبی از زنجیره بلوکی و پایگاه‌داده MongoDB است و معایب روش‌های دیگر را بهبود می‌بخشد. از جمله مزایای این مدل پیشنهادی مقیاس‌پذیری، کاهش سربار محاسباتی، حفظ حریم خصوصی و افزایش امنیت است.

کلمات کلیدی: امنیت، اینترنت اشیاء پزشکی، زنجیره بلوکی، محاسبات مه، MongoDB.

۱ مقدمه

اینترنت اشیاء پزشکی [۱] چشم‌انداز مراقبت‌های بهداشتی را با ترکیب قدرت دستگاه‌های متصل به هم و فناوری پیشرفته پزشکی متحول می‌کند. این فناوری شامل شبکه‌ای از دستگاه‌های پزشکی هوشمند، حسگرهای پوشیدنی و ابزارهای سلامت دیجیتال است که داده‌های بیمار را در زمان واقعی جمع‌آوری و به اشتراک می‌گذارد و تجزیه و تحلیل می‌کند. با اینترنت اشیاء پزشکی، متخصصان مراقبت‌های بهداشتی می‌توانند از راه دور بیماران را تحت نظر داشته باشند، علائم حیاتی را ردیابی کنند و اعلان‌هایی را در مورد مسائل

[1] Internet of Medical Things (IoMT)

بالقوه سلامت دریافت کنند. بیماران به لطف ابزارهای اینترنت اشیاء در مواقع ضروری قابل رصد هستند و همچنین ضرورت انجام معاینات روتین بهداشتی در بیمارستان‌ها کاهش می‌یابد. همچنین می‌توان اقامت در بیمارستان و هزینه‌های بستری مجدد را به حداقل رساند [۱]. از آنجا که داده‌ها در چندین موسسه پزشکی پراکنده هستند پردازش پرونده‌های پزشکی بیمار و احراز هویت بیماران و پزشکان به روشی ایمن بسیار دشوار است. از دست دادن اطلاعات شخصی و حساس بیمار و تشخیص احراز هویت نادرست، ممکن است پیامدهای قابل توجهی داشته باشد. علاوه براین، سیستم‌های پزشکی فعلی قادر به ایجاد شفافیت، قابلیت ردیابی، قابلیت اعتماد، تغییرناپذیری، حفظ حریم خصوصی و امنیت در هنگام رسیدگی به این پرونده‌ها نیستند [۲]. فناوری زنجیره بلوکی[۲] توانایی غلبه بر این مشکلات را در سیستم‌های مراقبت‌های بهداشتی امروز دارد [۱]. با این حال مقیاس‌پذیری، برگشت‌ناپذیری، هزینه زیاد و محاسبات فوق‌العاده بالا و غیره، چالش‌ها و نگرانی‌هایی هستند که زنجیره بلوکی با آن روبه‌رو است. در نتیجه، ایده‌ی پیشنهادی در این مقاله، ترکیبی از پایگاه‌داده توزیع‌شده MongoDB با فناوری زنجیره بلوکی و گره‌های مه است. بخش دوم مقاله به بررسی کارهای قبلی در حوزه زنجیره بلوکی می‌پردازد. در بخش سوم به پیش زمینه‌ای از زنجیره بلوکی، ساختار و مسائل آن و تعریفی از MongoDB پرداخته می‌شود. در بخش چهارم روش پیشنهادی بررسی شده است. و سرانجام، در بخش پنجم در مورد نتیجه‌گیری بحث می‌شود.

۲ کارهای انجام شده

اخیراً تحقیقات گسترده‌ای برای اطمینان از مراقبت‌های بهداشتی هوشمند با استفاده از اینترنت اشیاء پزشکی انجام شده است. با این حال، به دلیل جدید بودن اینترنت اشیاء پزشکی، در حال حاضر تحقیقات کمی در مورد بررسی امنیت در این زمینه در دسترس است. در این قسمت خلاصه ای از تلاش‌های قبلی در این زمینه بررسی می‌شود و به محدودیت‌ها و چالش‌های آنها اشاره می‌شود.

نویسندگان در سال ۲۰۱۷ در مقاله [۴-۳] پیشنهاد می‌کنند که حفظ حریم خصوصی داده‌های پزشکی تقریباً در اولویت قرار دارد، زیرا باعث به خطر افتادن وضعیت بیمار می‌شود. اگر این نقض اتفاق بیفتد، بر همه بیماران، ذی‌نفعان و اعتبارسنج‌ها تأثیر منفی می‌گذارد. برای جلوگیری از چنین وضعیتی، نویسندگان یک چارچوب مبتنی بر زنجیره بلوکی را برای محافظت از استقلال داده‌ها با استفاده از یک محیط ابری پیشنهاد می‌کنند. چارچوب پیشنهادی فقط به کاربران یا ذینفعان تایید شده اجازه دسترسی به یک سیستم را می‌دهد. اقدامات کاربران را می‌توان توسط چارچوب پیشنهادی مبتنی بر زنجیره بلوکی نظارت کرد. به اشتراک‌گذاری داده‌های بیمار با اتخاذ تکنیک‌های رمزنگاری تأیید می‌شود. این سیستم ارتباط بین کاربران و داده‌های حساس مراقبت‌های بهداشتی است. سیستم پیشنهادی آنها از یک زنجیره بلوکی سبک استفاده می‌کرد که تراکنش‌های سریع و کارایی مناسب را تضمین می‌کند. نویسندگان، پروتکل‌های ارتباطی و احراز هویت را به عنوان مطالعه بیشتر نگه داشته‌اند. سه لایه را در اینجا نگه داشته‌اند، یعنی لایه کاربر، لایه مدیریت سیستم و لایه ذخیره‌سازی. لایه کاربر شامل همه آن نهادها یا استخراج‌کنندگان زنجیره بلوکی است که سعی

[2] Blockchain

می‌کنند به داده‌ها دسترسی یا درخواست کنند. لایه مدیریت سیستم، مرکزی و مهم‌ترین لایه‌ای است که در آن تمامی ارتباطات برای تراکنش‌های امن برقرار می‌شود. آخرین لایه، یعنی لایه ذخیره‌سازی شامل کل داده‌هایی است که به‌طور ایمن در ابر برای کاربردهای متنوع بیشتر ذخیره می‌شوند. مشکل این پژوهش این است که احراز هویت و پروتکل ارتباطی کامل بررسی نشده است.

Muhammad Asif Habib و همکاران [۵] در سال ۲۰۱۹ یک مدل کنترل دسترسی برای اطمینان از حریم خصوصی داده‌های پزشکی در برابر تهدیدات داخلی در سیستم سلامت هوشمند پیشنهاد کردند. این روش ارتباط بین پزشکان و بیماران را به روشی ایمن، خصوصی و کارآمد تضمین می‌کند. این سیستم در مقایسه با سایر مدل‌های کنترل دسترسی اخیر، عملکرد بهتری دارد. با این حال سیستم، انجام عملیات کپی و انتقال روی منبع دایرکتوری را تسهیل نمی‌کند.

Tarek Farikha و همکاران [۶] در سال ۲۰۲۱ بر روی ذخیره سوابق سلامت الکترونیکی تمرکز کردند که در آن داده‌های جمع‌آوری‌شده توسط دستگاه‌های مستقر شده حیاتی هستند. هدف آنها ارائه دسترسی توزیع‌شده، ایمن و مجاز به این داده‌های حساس با استفاده از فناوری زنجیره بلوکی در حال ظهور بود. در این مطالعه، یک معماری تعبیه‌شده در زنجیره بلوکی و اینترنت اشیاء برای یک برنامه مراقبت‌های بهداشتی برای ذخیره و بررسی پرونده الکترونیک بیمار طراحی شد. مشکل این روش این است که ابتدا بدون اعتبارسنجی و رمزنگاری داده‌ها در زنجیره بلوکی ذخیره می‌شوند که این موجب بروز تهدیدات امنیتی می‌شود.

۳ پیش زمینه

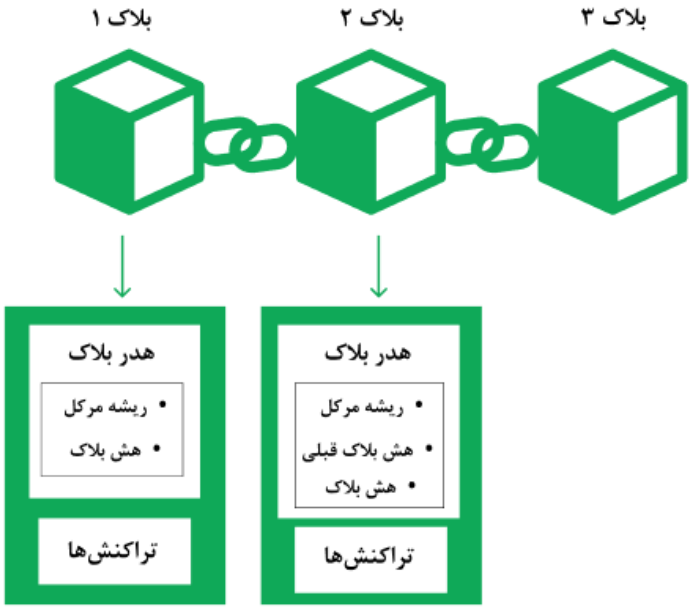
۱.۳ زنجیره بلوکی

این فناوری در سال ۲۰۰۸ معرفی و در سال ۲۰۰۹ توسط ناکاموتو برای حل مشکل هزینه دو برابر پول دیجیتال یا ارز رمزنگاری شده خود، یعنی بیت کوین پیشنهاد داد [۷]، اما این فناوری جدید برای کاربردهای مختلف دیگر نیز مورد استقبال قرار گرفت. زنجیره بلوکی شبکه‌ای نظیر به نظیر از بلوک‌های به هم پیوسته است که با اضافه شدن تراکنش‌های جدید به شبکه، دائماً در حال گسترش است. این فناوری با استفاده از روش غیرمتمرکز، امکان توزیع دانش و مالکیت مشترک هر قطعه از داده‌های توزیع‌شده را فراهم می‌کند. از مزایای زنجیره بلوکی می‌توان به امنیت، حفظ حریم خصوصی، یکپارچگی داده‌ها، تمرکززدایی، پایداری، ناشناس بودن، تغییرناپذیری و بدون نیاز به شخص ثالث اشاره کرد. این مزایا آن را به گزینه‌ای مناسب برای ذخیره اطلاعات پزشکی بیمار تبدیل کرده است [۸]. در نتیجه، زنجیره بلوکی این امکان را دارد که هزینه‌های قابل توجهی را کاهش و در عین حال کارایی را افزایش دهد [۷].

۱.۱.۳ ساختار بلوک

بلوک یک ساختار داده است که شامل یک هدر و مجموعه‌ای از معاملات است. هدر آن شامل یک مهر زمان (لحظه تولید بلوک)، هش بلوک قبلی ، هش بلوک فعلی و ریشه مرکل است. با استفاده از هش بلوک قبلی و ریشه مرکل تراکنش‌ها، هش بلوک جدید محاسبه و یک زنجیره بلوک ایجاد می‌شود. این ساختار در شکل ۱

دیده می‌شود. معاملات ذخیره شده در این بلوک تغییر ناپذیر هستند. با دستکاری شدن یک تراکنش، هش ریشه مرکل که نمایانگر هش تمام معاملات نامزد است، نیز تغییر می‌کند. در نتیجه، کل شبکه به امنیت و یکپارچگی معاملات مربوطه کمک می‌کند [۹].



شکل ۱: ساختار بلوک زنجیره بلوکی

۲.۱.۳ پایگاه داده MongoDB

اصطلاح NoSQL اولین بار در سال ۱۹۹۸ توسط آقای کارلو استروزی برای نامگذاری پایگاه داده رابطه‌ای منبع باز سبک وزن استفاده شد. برخی از پایگاه داده‌های موجود از استانداردهای NoSQL پیروی می‌کنند. اصطلاح «نه فقط SQL» نیز برای این پایگاه داده‌ها استفاده می‌شود. آنها مکانیزم ذخیره‌سازی و بازیابی را با مدل‌های سازگاری محدودتری نسبت به پایگاه داده‌های رابطه‌ای سنتی ارائه می‌کنند. به دلیل طراحی ساده، مقیاس‌پذیری افقی و در دسترس بودن، پایگاه داده‌های NoSQL در سراسر جهان محبوبیت پیدا کرده‌اند. اخیراً آنها به طور گسترده در داده‌های بزرگ و برنامه‌های وب بلادرنگ مانند فیس بوک، یاهو، گوگل و آمازون استفاده می‌شوند [۱۰]. یکی از این پایگاه داده‌های محبوب MongoDB است.

MongoDB یک پایگاه داده اسناد منبع‌باز است که عملکرد بالا، در دسترس بودن بالا و مقیاس‌بندی خودکار را ارائه می‌دهد. رکورد در MongoDB یک سند است که یک ساختار داده‌ای است که از جفت فیلد و مقدار تشکیل شده است. اسناد MongoDB مشابه اشیاء JSON هستند. مقادیر فیلدها ممکن است شامل سایر اسناد، آرایه‌ها باشد [۱۱].

جدول ۱: مقایسه زنجیره بلوکی و پایگاه داده MongoDB

	MongoDB	زنجیره بلوکی
یکپارچگی داده	اگر اقدامات لازم انجام نشود، یک عامل مخرب به طور بالقوه می‌تواند داده‌ها را تغییر دهد.	در ساختار زنجیره بلوکی عملاً غیرممکن است که کسی بتواند بدون شکستن زنجیره، داده‌ها تغییر دهد.
معاملات	داده‌ها را می‌توان ایجاد کرد، خواند، به روز یا حذف کرد (عملیات CRUD)	داده‌ها را فقط می‌توان خواند یا به زنجیره بلوکی اضافه کرد.
عملکرد پرس و جو	پایگاه‌های داده دسترسی سریع به داده‌ها را فراهم می‌کنند.	روش‌های تأیید برای اطمینان از یکپارچگی داده‌ها می‌توانند پرس و جو و عملکرد کلی یک زنجیره بلوکی را کاهش دهند.
ساختار	پایگاه‌های داده به صورت مرکزی مدیریت می‌شوند و یک مدیر مالک و کنترل کننده داده‌ها است.	زنجیره بلوکی‌ها می‌توانند کاملا غیرمتمرکز باشند و به هیچ مرجع مرکزی تکیه نکنند.

۳.۱.۳ مقایسه زنجیره بلوکی و MongoDB

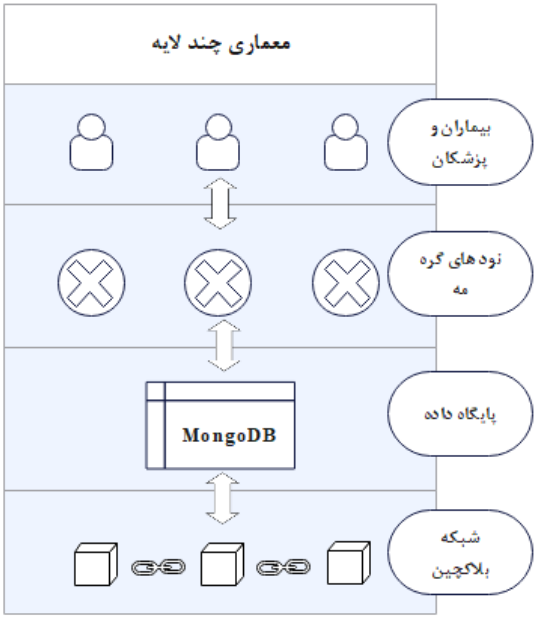
در جدول ۱، مقایسه‌ای بین MongoDB و زنجیره بلوکی انجام می‌دهیم. هدف نهایی یک زنجیره بلوکی، ذخیره اطلاعات است که آن را به یک پایگاه داده تبدیل می‌کند. زنجیره بلوکی‌ها تنها از طریق نحوه ذخیره داده‌ها با سایر انواع پایگاه داده‌ها متفاوت هستند. در حالی که زنجیره بلوکی‌ها را می‌توان یک پایگاه داده در نظر گرفت، یک پایگاه داده معمولاً یک زنجیره بلوکی نیست. پایگاه‌های داده معمولاً از بلوک‌های امضا شده برای ذخیره داده‌ها استفاده نمی‌کنند [۱۲]. زنجیره بلوکی مقیاس‌پذیری کمی دارد و هزینه ذخیره‌سازی در آن زیاد است. از طرفی پایگاه داده MongoDB نیز نمی‌تواند به اندازه زنجیره بلوکی امنیت داده‌ها را تضمین کند لذا پایگاه داده MongoDB و زنجیره بلوکی هر کدام به تنهایی قادر به ارائه یک راه حل کاملاً غیرمتمرکز نیستند و هر کدام مزایا و معایب خود را دارند. برای همین با ادغام زنجیره بلوکی و MongoDB می‌توان از مزایای آن‌ها بهره برد و محدودیت‌های آنها را برطرف کرد. خلاصه‌ای از مقایسه این دو در جدول ۱ بررسی شده است.

۲.۳ معماری روش پیشنهادی

روش پیشنهادی شامل یک معماری سه لایه جهت ادغام زنجیره بلوکی و MongoDB برای مدیریت داده‌ها در حوزه اینترنت اشیاء پزشکی است. شکل ۲ مدل پیشنهادی را نشان می‌دهد که شامل سه لایه می‌باشد و در ادامه به معرفی هر یک از این لایه‌ها پرداخته می‌شود.

لایه مه: این لایه جهت جمع‌آوری اطلاعات پزشکان و بیماران است. گره‌های مه[۳] می‌توانند اطلاعات پزشکی را با استفاده از حسگرهای مختلف جمع‌آوری کنند و در پایگاه داده ذخیره نمایند. این اطلاعات می‌توانند از طریق دستگاه‌هایی مانند سیستم‌های نظارت بر اطلاعات پزشکی به شبکه مه ارسال شوند و جهت

[3] Fog



شکل ۲: معماری روش پیشنهادی

بهبود کیفیت مراقبت از بیماران به پزشکان و پرستاران در بیمارستان کمک کنند. در کل، گره‌های مه با استفاده از حسگرهای مختلف می‌توانند به شیوه‌ای موثر در جمع‌آوری و ثبت اطلاعات پزشکی و سلامتی فرد کمک کنند.

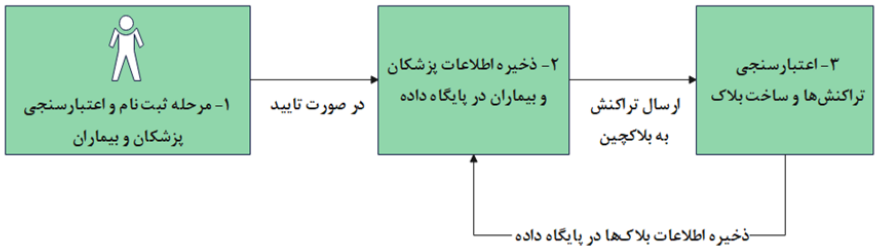
لایه پایگاه داده MongoDB: لایه پایگاه داده MongoDB در ایده پیشنهادی مسئولیت ذخیره و مدیریت داده‌های موجود در زنجیره بلوکی را برعهده دارد. این لایه جهت ذخیره‌سازی اطلاعاتی مانند اطلاعات ثبت نام، احرازهویت بیماران و پزشکان و اطلاعات بلاک‌های زنجیره بلوکی است. این لایه به صورت مستقل از زنجیره بلوکی عمل کرده و به زنجیره بلوکی ارتباطی ندارد، اما با توجه به نیازهای زنجیره بلوکی و ایده ادغام این دو فناوری، برخی امکانات، نظیر ذخیره‌سازی و هماهنگ سازی داده، مدیریت منابع، مدیریت تراکنش‌ها و حفاظت اطلاعات مورد نیاز و غیره برای ارتباط با زنجیره بلوکی را فراهم می‌کند.

لایه زنجیره بلوکی: این لایه امکان ثبت و تایید تراکنش‌ها بر روی یک سیستم غیرمترکز و معتبر را فراهم می‌کند و جهت ذخیره درهم اطلاعات و اختصاص جفت کلید عمومی و خصوصی استفاده می‌شود.

زنجیره بلوکی مورد استفاده در این پژوهش، زنجیره بلوکی بیت‌کوین است. بیت‌کوین یکی از معروف‌ترین نوع زنجیره بلوکی‌ها است و برای اینترنت اشیاء پزشکی نیز مزایای ویژه‌ای نظیر امنیت بالا، شفافیت، تقلب‌ناپذیری، مقرون به صرفه و غیره را دارد.

۴ مراحل روش پیشنهادی

در ابتدا بیماران، پزشکان و دستگاه‌های پزشکی هوشمند در گره‌های مه ثبت نام می‌کنند و سپس اطلاعات و مشخصات آنها در قالب تراکنش‌های جهت اعتبارسنجی به Mongoose ارسال می‌شوند. زمانی که هویت موجودیت‌ها تائید شد به عنوان یک معامله برای ایجاد بلاک به زنجیره بلوکی فرستاده می‌شوند و به هر موجودیت ثبت شده یک جفت کلید عمومی و خصوصی اختصاص داده می‌شود. کلید خصوصی به عنوان شناسه موجودیت‌ها عمل می‌کند و کلید عمومی موجودیت‌ها در گره‌های مه نگهداری می‌شود. در نتیجه هر موجودیتی جهت ایجاد تعامل در سیستم، نیاز به احراز هویت دارد در غیر این‌صورت اجازه ورود و تعامل ندارد که این مکانیزم تهدیدات گره‌های مخرب را برای تعامل با شبکه اینترنت اشیاء پزشکی کاهش می‌دهد. بعد از اعتبارسنجی تمامی اطلاعات بیماران و پزشکان و همچنین اطلاعات بلاک‌های زنجیره بلوکی در پایگاه داده MongoDB به دلیل مقیاس‌پذیری بالا ذخیره می‌شود و تنها کلید خصوصی و درهم اطلاعات در زنجیره بلوکی ذخیره می‌شوند. مراحل انجام روش پیشنهادی در شکل ۳ نشان داده شده است.



شکل ۳: مراحل انجام روش پیشنهادی

۱.۴ مرحله ثبت نام و اعتبارسنجی

ابتدا با استفاده از کلاس اسکیما[۴] Mongoose و تبدیل آن به مدل، یک سری بخش‌ها برای ثبت نام کاربر اعم از بخش ایمیل، بخش نام و بخش رمز در نظر می‌گیریم.

پس در ابتدا برای ثبت نام یک کاربر، نام و رمز و ایمیل کاربر باید برای Mongoose ارسال شود و با توجه به توضیحات بالا این مقادیر با اسکیما Mongoose جهت اعتبارسنجی بررسی می‌شود.

در مرحله قبل از ثبت نام کاربر جدید باید ابتدا بررسی کنیم که چنین کاربری با این آدرس ایمیل در پایگاه داده وجود دارد یا خیر. اگر وجود داشته باشد باید پیغامی حاوی متن «کاربری با این آدرس ایمیل در حال حاضر وجود دارد و ثبت نام جدید با این آدرس ایمیل امکان‌پذیر نمی‌باشد» نشان داده شود. اگر کاربر وجود نداشته باشد و اعتبارسنجی به درستی انجام شده باشد ثبت نام با موفقیت انجام می‌شود.

[4] Schema

بعد از ثبت نام و انجام فرایند اعتبارسنجی باید مشخصات کاربر در پایگاه داده ذخیره شود. اما بخش رمز به همین صورتی که از کاربر دریافت شده است در پایگاه داده ذخیره نمی‌شود بلکه قبل از ذخیره، با استفاده از روش درهم رمزنگاری می‌شود تا برای هیچ دو ورودی یکسان خروجی یکسانی نیز نداشته باشیم. در هنگام درهم کردن رمز یک Salt به درهم اضافه می‌شود تا امنیت درهم را بیشتر کند و باعث افزایش پیچیدگی شود.

در نهایت اگر اطلاعات ارسالی از کاربر برای ثبت نام مطابق با اسکیما Mongoose باشد، پیغامی حاوی متن «ثبت نام کاربر با موفقیت انجام شد» نمایش داده خواهد شد و این اطلاعات در پایگاه داده MongoDB نیز با موفقیت ذخیره می‌شود.

۲.۴ ورود کاربران

بعد از ورود موفقیت‌آمیز هر کاربر، یک Jason Web Tocken (JWT) به هر کدام از کاربران تعلق می‌گیرد. Jason Web Token در واقع یک شناسه منحصر به فرد است که به کاربر داده می‌شود تا پس از آن کاربر برای هربار ورود با استفاده از این شناسه احرازهویت گردد و اجازه ورود داشته باشد.

۳.۴ مرحله ارسال تراکنش به زنجیره بلوکی

برای اینکه زنجیره بلوکی تشکیل شود نیاز به حداقل ساخت یک بلاک داریم. اولین بلاکی که ساخته می‌شود و در زنجیره قرار می‌گیرد بلاک صفر است. این بلاک شامل بخش درهم قبلی به دلیل اینکه اولین بلاک زنجیره است نمی‌باشد. در اولین مرحله باید بررسی کنیم که بلاک صفر وجود دارد یا خیر. اگر وجود نداشته باشد باید اول این بلاک ساخته شود. بعد از اینکه این بلاک ساخته شد شبکه زنجیره بلوکی آماده دریافت تراکنش‌ها است.

بعد از ارسال تراکنش‌ها به شبکه زنجیره بلوکی، باید درهم تمامی این بلاک‌ها جهت یکپارچگی زنجیره و افزایش امنیت محاسبه، بررسی و تایید شوند. با توجه به اینکه حجم داده‌های ارسالی از اینترنت اشیاء پزشکی بالاست و مقیاس‌پذیری زنجیره بلوکی کم است ما از پایگاه داده MongoDB جهت ذخیره‌سازی اطلاعات شبکه زنجیره بلوکی استفاده می‌کنیم [۱۳]. در نهایت اطلاعات زنجیره بلوکی در MongoDB ذخیره می‌شود.

۵ نتیجه‌گیری

در این پژوهش با هدف افزایش سرعت، مقیاس‌پذیری و امنیت در شبکه‌های اینترنت اشیاء پزشکی روشی مبتنی بر ادغام زنجیره بلوکی و پایگاه داده MongoDB ارائه شد. در این پژوهش چون هزینه ذخیره‌سازی و اعتبارسنجی در زنجیره بلوکی زیاد است و همچنین مقیاس‌پذیری زنجیره بلوکی کم است از پایگاه داده MongoDB جهت حل این مشکل استفاده شد. پایگاه داده MongoDB چون یک پایگاه داده توزیع‌شده است دارای مقیاس‌پذیری و انعطاف بالایی است.

هدف این ایده، بهبود سرعت، امنیت و مقیاس‌پذیری سیستم زنجیره بلوکی با به کارگیری قدرت و کارآیی

پایگاه داده MongoDB است. با اجرای این پژوهش در این حوزه، امکان ارائه یک راهکار نوآورانه برای افزایش سرعت، امنیت و مقیاس‌پذیری سیستم‌ها وجود دارد. این ایده می‌تواند بهبود قابل توجهی در عملکرد و کارایی سیستم‌ها را به ارمغان بیاورد و در نهایت منجر به ساختاری بهتر و هماهنگ‌تر در استفاده از زنجیره بلوکی و MongoDB برای حوزه‌های مختلف شود.

مراجع

[1] Ali F, El-Sappagh S, Islam SR, Ali A, Attique M, Imran M, Kwak KS. An intelligent healthcare monitoring framework using wearable sensors and social networking data. Future Generation Computer Systems. 2021 Jan 1;114:23-43.

[2] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," Journal of Network and Computer Applications, vol. 149, p. 102481, Jan. 2020, doi: 10.1016/j.jnca.2019.102481.

[3] A. Saha, R. Amin, S. Kunal, S. Vollala, and S. K. Dwivedi, "Review on 'Blockchain technology based medical healthcare system with privacy issues,'" Security and Privacy, vol. 2, no. 5, Sep. 2019, doi: 10.1002/spy2.83.

[4] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," Information, vol. 8, no. 2, p. 44, Jun. 2017, doi: 10.3390/info8020044.

[5] M. A. Habib et al., "Privacy-based medical data protection against internal security threats in heterogeneous Internet of Medical Things," International Journal of Distributed Sensor Networks, vol. 15, no. 9, p. 155014771987565, Sep. 2019, doi: 10.1177/1550147719875653.

[6] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, "Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform," Journal of Healthcare Engineering, vol. 2021, pp. 1–12, Jul. 2021, doi: 10.1155/2021/9978863.

[7] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," IJWGS, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/IJWGS.2018.095647.

[8] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," IEEE Access, vol. 7, pp. 147782–147795, 2019.

[9] P. Pandey and R. Litoriya, "Securing E-health Networks from Counterfeit Medicine Penetration Using Blockchain," Wireless Pers Commun, vol. 117, no. 1, pp. 7–25, Mar. 2021, doi: 10.1007/s11277-020-07041-7.

[10] P. Pandey and R. Litoriya, "Securing E-health Networks from Counterfeit Medicine Penetration Using Blockchain," Wireless Pers Commun, vol. 117, no. 1, pp. 7–25, Mar. 2021, doi: 10.1007/s11277-020-07041-7.

[11] A. Chauhan, "A Review on Various Aspects of MongoDb Databases," International Journal of Engineering Research & Technology, vol. 8, no. 5, May 2019, doi: 10.17577/IJERTV8IS050031.

[12] https://www.mongodb.com/databases/blockchain-database

[13] S. Pal, "Implementation of simple Blockchain using NodeJS & MongoDB," Jun. 2020. https://www.linkedin.com/pulse/implementation-simple-blockchain-using-nodejs-mongodb-sougata-pal/

مفهوم‌شناسی هوش دیجیتالی

مرضیه پورصالحی نویده[۱]، احمدرضا متین‌فر[۲]

[۱]استادیار، گروه روان‌شناسی، دانشگاه آزاد اسلامی واحد تهران شرق، تهران
m_poursalehy@yahoo.com
[۲]استادیار، گروه فناوری، دانشگاه امام حسین(ع)، تهران
a_vizand@yahoo.com

چکیده

هدف از پژوهش حاضر معرفی چهارچوب نظری هوش‌دیجیتالی بود. هوش‌دیجیتالی مجموعهٔ کاملی از شایستگی‌های دیجیتالی است که برای پیشرفت در انقلاب‌صنعتی‌چهارم موردنیاز است. صلاحیت اساسی هوش‌دیجیتالی، شهروندی دیجتال است که افراد را قادر می‌سازد از فناوری به‌طور ایمن، مسئولانه و به روشی اخلاقی استفاده کنند.این مجموعهٔ جامع از صلاحیت‌های دیجیتالی، ریشه در ارزش‌های اخلاقی همگانی دارد تا از افراد برای استفاده، کنترل و ایجاد فناوری برای پیشبرد بشریت استفاده کنند. هوش دیجیتالی قصد دارد با تهیهٔ نسخه‌ای جهانی برای مهار فناوری برای آیندهٔ مشترک در طی انقلاب صنعتی چهارم، نیازهای سیستم‌های آموزشی، صنایع و دولت‌ها را پوشش دهد. هوش‌دیجیتالی دربرگیرنده ۸ حوزه با عنوان ۱) هویت دیجیتالی؛ ۲) مصرف دیجیتالی؛ ۳) ایمنی دیجیتالی؛ ۴) امنیت دیجیتالی؛ ۵) هوش‌هیجانی دیجیتالی؛ ۶) ارتباط دیجیتالی؛ ۷) سواد دیجیتالی و ۸) حقوق دیجیتالی است. مهارت‌های دیجیتالی ماهیتی متوالی و شرطی دارند به این معنا که آن‌ها بر یکدیگر بنا نهاده می‌شوند. هوش‌دیجیتالی، افراد را قادر به تعامل موفقیت‌آمیز در زیست‌بوم دیجیتالی نموده و حل مسائل مورد نیاز در محیط‌های مجازی را ممکن می سازد. برای تبدیل‌شدن افراد به شهروندان دیجیتالی خردمند، شایسته و آمادهٔ آینده که با موفقیت از فناوری استفاده نمایند، توجه به هوش‌دیجیتالی از ضروریات است.

کلمات کلیدی: هوش، هوش‌دیجیتالی، سواد رسانه، مهارت دیجیتالی، شایستگی دیجیتالی.

۱ مقدمه

ویژگی‌های انسان به‌ویژه هوش و فعالیت‌های هوشمندانه همواره مورد توجه روانشناسان و صاحب‌نظران مختلف بوده است. نظریه‌پردازان از دیدگاه‌های متفاوت به تعریف، طبقه‌بندی و سنجش هوش پرداخته‌اند. اگرچه تا سال‌ها پیش منظور از هوش، هوش عقلانی یا منطقی بود [۱]، امروزه در تعریف هوش به موارد دیگری اشاره می‌شود. مایر (۲۰۰۰) هوش را توانایی استدلال انتزاعی می‌داند که مستلزم انتقال‌های ذهنی است و براساس قوانین تثبیت‌شده انجام می‌گیرد. به نظر استرنبرگ (۱۹۹۷) هوش، متشکل از توانایی‌های

ذهنی لازم برای سازگاری، انتخاب و شکل‌دادن به هر نوع بافت محیطی و انعطاف‌پذیری در موقعیت‌های چالش‌انگیز است [۲]. گاردنر (۲۰۰۰) هوش را یک ظرفیت زیست‌شناختی برای تحلیل اطلاعات مختلف به‌وسیله انواع روش‌های خاص می‌داند. بنابراین می‌توان گفت هوش به‌طورکلی دربرگیرنده ظرفیت تفکر و برنامه‌ریزی، خلاقیت، سازگاری، حل‌مسئله، تأمل‌کردن، تصمیم‌گیری و یادگیری است [۳]. پس از گذشت سال‌ها از سلطهٔ بهره هوشی بر جوانب مختلف زندگی، اکنون از اهمیت آن به‌عنوان تنها عامل موفقیت کاسته شده است. هرچند که مفهوم هوش ممکن است نزد افراد مختلف معانی متفاوتی داشته باشد، بااین‌حال وقتی صحبت از هوش به میان می‌آید، بلافاصله نوعی توانایی ذهنی دربارهٔ انسان تداعی می‌شود. اکنون بهرهٔ هوشی بالا به‌تنهایی ارزش قلمداد نمی‌شود و درصد زیادی از موفقیت‌های فرد در عصراطلاعات به هوش دیجیتالی نسبت داده می‌شود. امروزه روانشناسان توجه ویژه‌ای به این قابلیت و نقش آن در زندگی نموده‌اند و هرروز بر اهمیت و نقش آن بعنوان عاملی تأثیرگذار بر موفقیت در جوانب مختلف زندگی افزوده می‌شود. بشر، سه انقلاب‌صنعتی را پشت‌سر گذاشته و اکنون درحال تجربهٔ انقلاب‌صنعتی چهارم است. هریک از این انقلاب‌های‌صنعتی، نیازمند مهارت‌ها و شایستگی‌های خاصی بوده است [۴]. انقلاب‌صنعتی‌اول نیازمند مهارت‌های‌جسمانی و استفاده از ماشین‌آلات-صنعتی [۵]؛ انقلاب‌صنعتی‌دوم نیازمند مهارت‌های‌شناختی با تمرکز بر تولید انبوه [۶]؛ انقلاب صنعتی سوم بر مهارت‌های نرم با تمرکز بر هوش‌هیجانی [۷] و انقلاب صنعتی چهارم بر تسلط بر مهارت‌های دیجیتالی تاکید دارد[۸]. انقلاب صنعتی چهارم و سرعت تغییرات فناوری، شکافی بین قابلیت‌های موجود و شایستگی‌های مورد نیاز افراد در جایگاه‌های مختلف ایجاد نموده است [۹]. انقلاب صنعتی چهارم به تغییرات اساسی در شیوهٔ زندگی، کار و ارتباط با دیگران منجر شده است. این امر مستلزم نوع جدیدی از هوش در مواجهه با این تغییرات اساسی است. این نوع جدید هوش نیازمند شایستگی‌های جدیدی است [۴]. مجموعه مهارت‌های پایه در جهت حرکت از مهارت‌های جسمانی، شناختی، هیجانی به مهارت‌های دیجیتالی نیازمند هوشی به نام هوش‌دیجیتالی است. در یک تعریف ساده، هوش‌دیجیتالی، افراد را قادر به تعامل موفقیت‌آمیز در زیست‌بوم دیجیتالی نموده و حل مسائل مورد نیاز در محیط‌های مجازی را ممکن می‌سازد [۱۰].

تغییرات فناورانه، ارزش‌ها و هنجارهای اجتماعی را تحت‌تأثیر قرار داده است. باتوجه به توسعهٔ سریع فضای دیجیتال، توانایی تبدیل‌شدن انسان به بخشی از زیست‌بوم دیجیتال، ایجاد دانش، فناوری و محتوای جدید برای تبدیل ایده‌ها به واقعیت یکی از اهداف هوش‌دیجیتالی است. توانایی حل چالش‌های جهانی، نوآوری و ایجاد فرصت‌های‌جدید در فضای نوین دیجیتال آینده نیازمند بررسی علمی هوش‌دیجیتالی است. جهت تعامل و کنشگری فعال در فضای دیجیتال، توانایی فرد در استفاده از فناوری و رسانه‌های دیجیتال به روش‌های ایمن، مسئولانه و اخلاقی در راستای مهارت‌های زندگی آینده به موضوع هوش دیجیتالی باید پرداخته شود. مقالهٔ حاضر ضمن توجه به مقتضیات زندگی در عصر دیجیتال، با تأکید بر مفهوم سواد رسانه، به معرفی چهارچوب نظری هوش دیجیتالی می‌پردازد.

۲ مطالب اصلی

در سال‌های اخیر مطالعه در حوزهٔ ناهمسانی دیجیتالی، بر دسترس‌پذیری به ابزارهای فناورانه تمرکز داشت. دسترسی‌پذیری به صورت خاص به معنای توانایی دسترسی به سخت افزارها و نرم افزارهای دیجیتالی است [۱۱]. متعاقباً ضرورت توجه به تفاوت افراد در استفاده از ابزارهای دیجیتال به جای تفاوت دسترسی‌پذیری مورد توجه قرار گرفت. این حوزه به شکاف دیجیتال سطح دوم یعنی شکاف مهارتی و نحوه استفاده معروف است. مطالعات جدیدتر، تمرکز محقیقن را بر نقص توانایی افراد در انتقال تجارب برخط به پیامدهای غیربرخط مطلوب متوجه نموده است. این حوزه به شکاف دیجیتال سطح سوم مرتبط بوده که در آن محققین بر ناهمسانی افراد در انتقال استفاده از اینترنت به فضای غیربرخط در کشورهایی با سطح بالای استفاده از فناوری می‌پردازند [۱۲]. وان‌دیجک (۲۰۰۵، ۲۰۱۷، ۲۰۲۰) به‌صورتی نظام‌مند به تألیف نظریه‌ای مبتنی بر شواهد پژوهشی در حوزه ناهمسانی دیجیتالی پرداخت. نظریه او ترکیبی از نظریه ساختاری[1] (منابع) و نظریه مقبولیت[2] (تخصیص) است. مبحث اصلی نظریه وان‌دیجک را در عبارت زیر می‌توان خلاصه نمود: ناهمسانی طبقه ای افراد در جامعه به دومقوله‌ای‌های قابل مشاهدهٔ مکرر (مانند پیر–جوان، زنان–مردان) مرتبط بوده که این امر توزیع نابرابر استفاده از منابع را موجب شده و بنابراین دسترسی‌پذیری نابرابر به فناوری دیجیتال را رقم می‌زند. علاوه بر این دسترسی‌پذیری نابرابر به فناوری دیجیتال نه‌تنها به منابع اجتماعی بلکه به ویژگی‌های این فناوری‌ها (مانند جدیدبودن یا سهولت‌استفاده) بستگی دارد. اهمیت این موضوع در واقع این است که دسترسی‌پذیری نابرابر به فناوری دیجیتال به مشارکت نابرابر در جامعه به صورت گسترده منتهی می‌شود. این موضوع در عوض ناهمسانی‌های طبقه‌ای و توزیع نابرابر منابع را تقویت می‌کند. براساس نظر وان دیجک (۲۰۰۵، ۲۰۱۷، ۲۰۲۰) در راستای ناهمسانی‌های طبقه‌ای افراد ناهمسانی‌های جایگاهی مانند جایگاه‌های شغلی، آموزشی، خانوادگی و قومیتی به‌نفع دسترسی‌پذیری دیجیتالی برتر برای افراد مرفه منتهی می‌شود. ارتقاء دیجیتالی شدن، تقویت ناهمسانی اجتماعی موجود را در پی دارد.

پژوهش های قبلی به تعدادی عوامل جمعیت‌شناختی اجتماعی[3] که بر مهارت‌های کسب اطلاعات دیجیتالی اثر می‌گذارند، اشاره کرده‌اند. در میان پژوهشگران توافق واضحی وجود دارد مبنی بر اینکه به‌صورت کلی افراد جوان از مهارت‌های دیجیتال بهتری برخوردار هستند و همچنین از مهارت‌های کسب اطلاعات دیجیتال بهتری نسبت به افراد مسن‌تر برخوردارند [۱۳] و همچنین سطح تحصیلات بالاتر پیش‌بینی‌کننده مهارت‌های بالاتر مرتبط با سواد دیجیتالی است [۱۲]. در مقابل، معمولاً تفاوت معناداری در مهارت‌های کسب اطلاعات دیجیتالی بر مبنای جنسیت وجود ندارد [۱۴]. همچنین نتایج مطالعات نشان داد که در مناطق شهری، چیرگی دیجیتالی بهتری نسبت به مناطق غیرشهری در راستای دسترسی محدودتر به خدمات اینترنتی در مناطق غیرشهری‌تر وجود دارد [۱۵].

[1] Structuration theory
[2] Acceptance theory
[3] sociodemographic

۱.۲ سواد رسانه

مفهوم سواد رسانه، مفهومی کلیدی در تلاش برای ساخت جامعه‌ای مدنی در عصر دیجیتال است [۱۶]. مفهوم سواد رسانه می‌تواند به صورت گوناگونی تعریف شود؛ اما در تعریفی ساده سواد رسانه به‌عنوان توانایی مورد نیاز هر فرد برای زندگی، یادگیری و کار در جامعهٔ دیجیتال است. یونسکو در تعریف خاص‌تری از سواد رسانه، قابلیت دسترسی، مدیریت، فهم، تلفیق، ارتباط، ارزیابی و کسب اطلاعات ایمن از طریق ابزارهای دیجیتالی و فناوری‌های شبکه‌ای را به‌عنوان شکلی از مشارکت در زندگی اجتماعی و اقتصادی تعریف می‌کند [۱۷]. برخی کشورها چهارچوبی جامع‌و نظام‌مند از سواد رسانه بعنوان مرجعی دربرنامه ارتقاء سواد دیجیتالی جامعه تدوین نموده‌اند. تلاش‌های متعددی در جهت ایجاد یک چهارچوب نظام‌مند به شناسایی عناصر مهم سواد/شایستگی دیجیتالی که هر فردی در جامعه دیجیتالی باید از آن بهره‌مند باشد، صورت گرفته است. در مطالعات مقدماتی، پژوهشگران چهار چهارچوب سواد دیجیتالی مورد توافق در کشورهای مختلف را شناسایی نمودند. چهارچوب سواد دیجیتالی حکومت استانی بریتیش کلومبیای کانادا؛ چهارچوب شایستگی‌های دیجیتالی مرکز پژوهشی جوینت اتحادیه اروپا، چهارچوب هوش دیجیتالی انجمن هوش دیجیتالی سنگاپور و چهارچوب سواد دیجیتالی اندونزی. حکومت استانی بریتیش کلومبیای کانادا، سواد دیجیتالی را بعنوان علاقه، نگرش و توانایی افراد در استفاده متناسب از فناوری‌های دیجیتالی و ابزارهای ارتباطی جهت دسترسی، مدیریت، تلفیق، تحلیل و ارزیابی اطلاعات، ایجاد دانش جدید، ایجاد و ارتباط با دیگران تعریف می‌کند. در این چهارچوب ۶ مشخصه سواد دیجیتالی عبارتند از: ۱) سواد اطلاعاتی و پژوهشی؛ ۲) تفکر نقاد، حل مسئله و تصمیم‌گیری؛ ۳) خلاقیت و نوآوری؛ ۴) شهروندی دیجتالی؛ ۵) ارتباط و مشارکت و ۶) استفاده از فناوری و مفاهیم مرتبط با آن (وزرات آموزش بریتیش کلومبیا، ۲۰۱۷). در چهارچوب بعدی مرکز پژوهشی جوینت اتحادیه اروپا مفهوم DigComp (چارچوب شایستگی دیجیتالی برای شهروندان) را معرفی نموده است. مطالعه اولیه این چهارچوب از سال ۲۰۰۵ آغاز شده و تاکنون چندین بار به‌روزرسانی شده است. در این چهارچوب ۲۱ نوع شایستگی دیجیتالی در ۵ حوزه شناسایی شده است: ۱) سواد اطلاعاتی و داده؛ ۲) ارتباط و مشارکت؛ ۳) ساخت محتوای دیجیتالی؛ ۴) ایمنی؛ ۵) حل مسئله. علاوه بر دو چهارچوب قبل، انجمن هوش دیجیتالی بر نوع جدیدی از هوش به نام بهره هوشی دیجیتالی تأکید دارد.

۲.۲ چارچوب هوش دیجیتالی

انجمن هوش دیجیتالی[۴]، هوش دیجیتالی را به صورت «مجموعه جامعی از شایستگی‌های دیجیتالی برآمده از ارزش‌های اخلاقی همگانی به منظور ارتقاء انسان در استفاده، کنترل و خلق فناوری» تعریف می کند [۸]. این تعریف دو جنبه مهم دارد. جنبه اول اینکه مهارت‌ها و شایستگی‌های دیجیتالی فرد باید نشأت‌گرفته از ارزش‌های اخلاقی باشند. جنبه دوم اینکه فناوری باید در جهت پیشرفت انسان‌ها و نه در جهت آسیب به انسان‌ها و جوامع مورد استفاده قرار بگیرد. نانان، روپلم و وانگساون (۲۰۱۹) [۱۸] شایستگی‌های دیجیتالی را به‌عنوان شایستگی‌های فنی، شناختی، اجتماعی و هیجانی که افراد را قادر به رویارویی با چالش‌ها و انطباق

[4] DQ Institute

با محیط‌های دیجیتالی می‌کند، تعریف می‌کنند. در این تعریف، تنها تأکید بر فناوری نیست بلکه تأکید بر چگونگی استفاده از شایستگی‌های شناختی، اجتماعی و هیجانی در مواجهه با پیامدها و اثرات فناوری است. این تعریف در راستای تعریف هیرچ کرینسن، کوباچ، استارک، وون‌ویچرت، هابرچت و سلدمیر (۲۰۱۹) [۱۹] است که مهارت‌های شناختی و مهارت‌های نرم را هنوز هم دارای اهمیت می‌دانند. بر اساس نظر میتاس و مک فارلین (۲۰۱۷) [۲۰] هوش دیجیتالی دربرگیرنده همگامی راهبردهای تجارت و فناوری اطلاعات است. این مزیت، مدیران پروژه‌ها را به ارتقاء مهارت‌های هوش دیجیتالی تشویق می‌کند. سیسمارا، گازولا، کوچینا و لئورادیس (۲۰۱۸) هوش دیجیتالی را به‌عنوان مهارت درک وانطباق با استفاده از مفاهیم دیجیتال/ برخط در حل مشکلات ارتباطی، اطلاعاتی و فناورانه برخط تعریف می کنند. این تعریف از نظر صرفاً مورد توجه قرار دادن حل‌مسئله برخط، از تعاریف دیگر متمایز است. تعریف فوق، این واقعیت را که فناوری می‌تواند در محیط‌های غیر برخط و در ارتباط بین انسان و ابزار هم به‌کار رود، نادیده می‌گیرد [۴].

علاوه بر چارچوب‌های پیشین، انجمن هوش دیجیتالی بر نوع جدیدی از هوش به نام بهره هوشی دیجیتالی تأکید دارد. بر اساس نظر پارک (۲۰۱۹) بنیان‌گذار انجمن هوش دیجیتالی، هوش دیجیتالی در برگیرنده ۸ حوزه با عنوان ۱) هویت دیجیتالی؛ ۲) مصرف دیجیتالی؛ ۳) ایمنی دیجیتالی؛ ۴) امنیت دیجیتالی؛ ۵) هوش هیجانی دیجیتالی؛ ۶) ارتباط دیجیتالی؛ ۷) سواد دیجیتالی و ۸) حقوق دیجیتالی است. چارچوب سواد دیجیتالی اندونزی بر سه جنبه محافظت، حقوق و قدرت تأکید دارد. جنبه محافظت دربرگیرنده محافظت از اطلاعات شخصی، امنیت برخط و حریم شخصی است. جنبه حقوق شامل آزادی بیان، استعداد عقلانی و فعالیت اجتماعی و جنبه قدرت شامل خبرنگاری شهروندی و اصول اخلاقی اطلاعاتی است. هریک از چهارچوب‌های بالا ویژگی‌های منحصربه‌فرد خود را داشته اما همگی در ویژگی اهمیت به شایستگی‌های مورد نیاز افراد در زندگی در عصر دیجیتالی تأکید دارند. جدول ۱، هشت حوزهٔ هوش دیجیتالی معرفی‌شده توسط انجمن هوش دیجیتالی (۲۰۱۹) و انجمن مهندسان برق و الکترونیک[۵] (۲۰۲۱) را نشان می‌دهد.

۳ نتیجه‌گیری

با ورود به انقلاب صنعتی چهارم، پیشرفت‌های دیجیتالی، فیزیکی، زیستی و فناوری به صورت یکپارچه گرد هم آمده‌اند. همانطور که انقلاب صنعتی دوم موجب جایگزینی نیروی جسمی انسان با ماشین شد، انقلاب صنعتی چهارم نیز موجب جایگزینی کار ذهنی انسان با هوش مصنوعی، اتوماسیون و سایر نوآوری‌های دیجیتالی شد. مشاغل جدید به مهارت‌های جدیدی نیاز دارند که به انسان اجازه می‌دهد تا به‌طورموثر از فناوری استفاده کند؛ مهارت‌هایی فراتر از مهارت‌های جسمی، شناختی و نرم؛ مهارت‌های دیجیتالی. گسترش فناوری‌های دیجیتالی در حوزه‌های اجتماعی، اقتصادی و زندگی شخصی، کسب مهارت‌های اطلاعات دیجیتالی را بعنوان عاملی مهم در موفقیت فرد در حوزه زندگی اجتماعی و مدنی در نظر می‌گیرد [۱۴]. جستجو، ارزیابی و پردازش اطلاعات، قسمت مهمی از زندگی روزمره در جامعه اطلاعاتی امروزه است. ظهور برنامه‌های کاربردی دیجیتالی پیشرفته‌تر در آینده، مهارت‌های کسب اطلاعات دیجیتالی را ضروری‌تر جلوه می‌دهد [۱۱]. براساس

[5] Institute of Electrical and Electronics Engineers (IEEE)

جدول ۱: حوزه‌های هوش دیجیتالی

حوزه‌های هوش دیجیتالی	تعریف	اصل راهنما
هویت دیجیتالی	توانایی ایجاد یک هویت برخط و غیربرخط سالم.	احترام به خود
مصرف دیجیتالی	توانایی استفاده متعادل، سالم و مدنی از فناوری.	احترام به زمان و مکان
ایمنی دیجیتالی	توانایی شناسایی، کاهش و مدیریت خطرات سایبری مختلف از طریق استفاده مسئولانه، اخلاقی و ایمن از فناوری.	احترام به زندگی
امنیت دیجیتالی	توانایی شناسایی، جلوگیری و مدیریت سطوح مختلف تهدیدات سایبری برای محافظت از اطلاعات، دستگاه‌ها، شبکه‌ها و سیستم‌ها.	احترام به دارایی
هوش هیجانی دیجیتالی	توانایی تشخیص، پیمایش و ابراز احساسات در تعاملات بین‌فردی دیجیتالی و درون‌فردی.	احترام به دیگران
ارتباطات دیجیتالی	توانایی برقراری ارتباط و همکاری با دیگران با استفاده از فناوری.	احترام به شهرت و روابط
سواد دیجیتالی	توانایی یافتن، خواندن، ارزیابی، سنتز، ایجاد، سازگاری و اشتراک‌گذاری اطلاعات، رسانه‌ها و فناوری.	احترام به دانش
حقوق دیجیتالی	توانایی درک و حمایت از حقوق بشر و حقوق قانونی هنگام استفاده از فناوری.	احترام به حقوق

نظر کستلز (۲۰۱۰ به‌نقل از مارنویک و همکاران، ۲۰۲۱)، فرایندی به نام اطلاعاتی‌شدن در همه‌ی حرفه‌ها با اشاره به اطلاعات بعنوان منبع اصلی بازدهی در بسیاری از حرفه‌ها، قابل مشاهده است. ضرورت کسب مهارت‌های اطلاعات دیجیتالی بعنوان شایستگی‌های هسته‌ای، به‌خصوص در حرفه‌هایی که پایه‌ای‌ترین وظایف آنها جستجو، ارزیابی و اشتراک اطلاعات است، نمایان است. بر اساس نظر وان‌لار، وان درسن، وان–دیجک و دی‌هان (۲۰۲۰)، برای هر یک از مهارت‌های قرن ۲۱ شامل مهارت‌های فنی، ارتباطی، مشارکت، تفکر نقاد، خلاقیت و حل‌مسئله یک الحاقیه دیجیتالی نیاز هست. برای مثال، مهارت‌های ارتباطی دیجیتالی شامل توانایی انتقال برخط اطلاعات از طریق رسانه‌های اجتماعی، ایمیل و گفتگوی‌برخط است. مهارت‌های کسب اطلاعات دیجیتال شامل توانایی جستجوی اطلاعات از منابع دیجیتال و ارزیابی سودمندی و اعتبار اطلاعات دریافتی است. وان لار و همکاران (۲۰۲۰) تأکید کردند که مهارت های دیجیتالی ماهیتی متوالی و شرطی دارند به این معنا که آنها بر یکدیگر بنا نهاده می‌شوند. بین مهارت‌های کسب‌شده دانش‌آموزان از طریق آموزش رسمی و مهارت‌های مورد نیاز برای زندگی و کار در قرن ۲۱، شکاف بزرگی وجود دارد. در واقع آموزش رسمی در ارتقاء شایستگی‌های مورد نیاز به دانش‌آموزان کافی نبوده و نیاز به آمادگی، مهارت‌مندی و حرکت به سمت ارتقاء شایستگی‌های دیجیتالی وجود دارد [۲۲].

نتایج پژوهش‌ها نشان می دهد که بافت و منابع اجتماعی در دسترس افراد برای مثال فراوانی و تنوع تکنولوژی مورد استفاده و یا تجربه استفاده مداوم، پیش‌بین سطح مهارت‌های دیجیتال است [۱۱]. دسترسی‌پذیری دیجیتالی به‌معنای استفاده یا عدم استفاده از تکنولوژی نبوده [۱۲] بلکه بیشتر به‌معنای کیفیت، آشنایی و عادات دسترسی‌پذیری است. هلسپر (۲۰۱۷) خاطر نشان کرد که محرومیت دیجیتالی،

مرکب و چندبعدی است. با تکیه بر نظریه محرومیت نسبی، وی به ضرورت تمایز بین سطوح نسبی و مطلق محرومیت اشاره می کند. محققین نه تنها باید به منابع فردی و عوامل اجتماعی منتج به ناهمسانی های دیجیتال توجه نموده بلکه همچنین باید به عوامل سطح میانی، تجارب و ارتباطات روزمره افراد که محرومیت ذهنی و نسبی را تعیین نموده و نیرومحرکه افراد و جوامع به تغییر موقعیت است نیز توجه کنند. مداخلات مؤثر هم ناهمسانی عینی و هم مؤلفه‌های شناختی و هیجانی را موردتوجه قرار می‌دهد [۲۳].

به‌طورکلی در جامعهٔ به‌طور فزاینده فناوری‌گرا، صلاحیت‌های دیجیتال مانند سواد رسانه و شایستگی‌های دیجیتال که در مجموع در قالب هوش دیجیتالی نمایان می‌شود، به نیازهای اصلی آینده تبدیل شده‌اند. درمقایسه با پیشرفت فناوری، اجرای آموزش مهارت‌های دیجیتالی، برنامه‌های آموزشی و سیاست‌گذاری‌های مؤثر با سرعت بسیار کندتری اتفاق می‌افتد و این شکاف سرعت، به‌طور فزاینده‌ای درحال رشد است. چنین شکاف‌هایی پیامدهای جدی و ناخواسته منفی برای افراد و همچنین کل جامعه به همراه دارد. لذا برای تبدیل‌شدن افراد به شهروندان دیجیتال خردمند، شایسته و آمادهٔ آینده که با موفقیت از فناوری استفاده نمایند، هوش دیجیتالی به‌عنوان مجموعه‌ای جامع از شایستگی‌های بنیادی فنی، شناختی، فراشناختی و اجتماعی‌عاطفی مشتمل بر ارزش‌های اخلاقی جهانی و عمومی جهت سازگاری افراد با چالش‌های زندگی در عصر دیجیتال باید مورد توجه سیاست‌گذاران امر قرار گیرد.

مراجع

[۱] طباطبایی، مینو. انواع هوش و کاربردهای آن در زندگی انسان. ماهنامه پیوند (تربیتی-آموزشی). نشریه انجمن اولیا و مربیان ایران. شماره ۳۶۲. صص ۲۵-۲۲، ۱۳۸۸.

[2] D.D. Nasel. Spiritual Orientation in relation to spiritual intelligence: A consideration of traditional christainity and new age/individualistic sprituality, 2004.

[3] K.D. Noble. Spritual intelligence: Anew frame of mind. Advanced Development Journal.9, 1-28, 2000.

[4] C. Marnewick, A. Marnewick. Digital intelligence: A must-have for project managers. Project leadership and Society 2, 2021.

[5] R. Drath, A. Horch. Industrie 4.0: hit or hype? [industry forum]. IEEE Indus. Electron. Mag. 8, 56–58, 2014.

[6] Y. Liu, D. B. Grusky. The payoff to skill in the third industrial revolution. Am. J. Sociol. 118, 1330–1374, 2013.

[7] R. Maqbool, Y. Sudong, N. Manzoor, N. Rashid. The impact of emotional intelligence, project managers' competencies, and transformational leadership on project success: an empirical perspective. Proj. Manag. J. 48, 58–75, 2017.

[8] Y. Park. "DQ Global Standards Report 2019: Common Framework for Digital Literacy, Skills and Readiness," p. 61, 2019.

[9] Z. Whysall, M. Owtram, S. Brittain. The new talent management challenges of industry 4.0. J. Manag. Dev. 38, 118–129, 2019.

[10] N. B. Adams. Digital intelligence fostered by technology. J. Technol. Stud. 30, 93–97, 2004.

[11] J. A. G. M. Van Dijik. Closing the digital divide. The role of digitaltechnologies on social development, well-being of all and the approach ofthecovid19pandemic, 2020.

[12] A. J. A. M. Van Deursen, J. A. G. M. Van Dijik. "Modeling traditional literacy, Internet skills and Internet usage: An empirical study". Interacting with Computers, 28(1), 13–26, 2016.

[13] M. Claro, A. Salinas, T. Cabello-Hutt, E. San Martin, et al. Teaching in a digital environment (TIDE): Defining and measuring teachers' capacity to develop students' digital information and communication skills. Computers & Education, 121, 162–174, 2018.

[14] B. Ertle, A. Canadi, C. Tarnai. Getting closer to the digital divide: An analysis of impacts on digital competencies based on the German PIAACsample.International Journal of Educational Development, 78, 2020.

[15] K. Mossberger, C. Talbert, M. Gilbert. Race, place, and information technology. Urban Affairs Review, 41(4), 583–620, 2006.

[16] O. Berg. "Nordic journal of digital literac," Nord. J. Digit. Lit., vol. 12, no. 3, pp. 51–51, 2017. Y. Eshet-Alkalai."Digital Literacy: A Conceptual Framework for Survival Skills in the Digital era," J. Educ. Multimed. Hypermedia, vol. 13, pp. 93–106, 2004.

[17] UNESCO. "A Global Framework of Reference on Digital Literacy," Inf. Pap, vol. 51, pp. 1–146, 2018.

[18] K. Na-Nan, T. Roopleam, Wongsuwan, T. Validation of a digital intelligence quotient questionnaire for employee of small and medium-sized Thai enterprises using exploratory and confirmatory factor analysis. Kybernetes, 2019.

[19] H. Hirsch-Kreinsen, U. Kubach, R. Stark, G. Wichet, L. Huberch, J. Steglich. Key Themes of Industrie 4.0 - Research and Development Needs for Successful Implementation of Industrie 4.0. acatech – National Academy of Science and Engineering, Munich, Germany, pp. 1–32, 2019.

[20] S. Mithas, F. W. McFarlin. What is digital intelligence?. In: IT Professional. IEEE, pp. 3–6, 2017.

[21] E. Van Laar, A. J. A. M. Van Deursen, et al. Determinants of 21st-century digital skills and 21st-century digital skills for workers: A systematic literature review. SAGE Open, 10(1), 1–14, 2020.

[22] I. K. R. Hatlevik, O. E. Hatlevik. Examining the relationship between teachers' ICT self-efficacy for educational purposes, collegial collaboration, lack of facilitation and the use of ICT in teaching practice. Frontiers in Psychology, 9(935), 555–567, 2018.

[23] E. J. Helsper. The social relativity of digital exclusion: Applying relative deprivation theory to digital inequalities. Communication Theory, 27(3), 223–242, 2017.

اکوسیستم متاورس با محوریت جرائم مالی در آن

عباس ترکاشوند[۱]، رضا مالکی پور[۲]

[۱] کارشناسی مهندسی فناوری اطلاعات، دانشگاه پیام نور تهران
abbas.38947@gmail.com
[۲] کارشناسی مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد ملایر
hajiradmehr2023@gmail.com

چکیده

متاورس، دریچه‌ای به روی فضاها و ایجاد هویت جایگزین برای تجربیات انسانی بازکرده است. اهمیت روزافزون متاورس در دنیای مجازی و تداوم دنیای دیجیتال برای بسیاری از کاربران به‌عنوان یک مفهوم خیالی و یا غیرممکن شناخته شده است، اما حقیقت این است که ما در حال حاضر در میان متاورس‌های اولیه زندگی می‌کنیم و آینده قبل از اینکه واقعاً برای ایجاد آن آماده باشیم، وجود دارد. اکوسیستم متاورس به‌سرعت در حال رشد است و نوآوران و شرکت‌های بزرگ فناوری در این اکوسیستم قرار دارند. اگر متاورس یک دنیای مجازی باشد، برای کنترل کلاه‌برداری‌ها و جرائم مالی به نسخه مجازی از پلیس نیاز است. با توجه به برنامه‌های متاورس، به نظر می‌رسد حمایت از برنامه‌های ضد پول‌شویی به همان اندازه که در دنیای واقعی اهمیت دارد، در دنیای مجازی نیز اهمیت دارد. در این مقاله سعی در معرفی اجزای تشکیل‌دهنده اکوسیستم متاورس، سرمایه‌گذاری در آن و در نهایت جرائم و تخلفات ابزارهای مالی در متاورس تشریح شده است.

کلمات کلیدی: متاورس، NFT، مالی، جرائم، هویت، رمزارز.

۱ مقدمه

دنیای علم و فناوری به‌سرعت در حال تغییر است و هرساله وسایل ارتباطی جدیدتری با فنّاوری قوی‌تر وارد بازار شده تا راه‌حلی بهتر و کاربردی‌تر برای ایجاد ارتباط بین افراد ارائه کنند و بعلاوه کاربران بتوانند در محیطی کارآمدتر باهم در ارتباط بوده و امور مالی خود را به انجام برسانند.

امروزه و با گسترش شبکه‌های اجتماعی، نیاز افراد به فضاهای آنلاین و مجازی بیشتر از همیشه شده و بنا بر تحقیقات صورت گرفته بیش از چهار میلیارد نفر در سراسر دنیا دارای اینترنت فعال هستند. این بدان معناست که بیش از نیمی از مردم جهان برای ارتباطات و انجام فعالیت‌های اقتصادی نیاز به استفاده از اینترنت دارند. همین موضوع نیاز به محیطی جدید مانند متاورس را دوچندان کرده است. اما منظور از متاورس چیست؟ متاورس از ترکیب دو بخش «متا» و «ورس» تشکیل‌شده است و اگر بخواهیم به مفهوم لغوی

آن اشاره‌کنیم، باید گفت متا در لغت به معنی «فرا» و ورس مشتق شده از واژه یونیورس به معنای «جهان» است، پس می‌توان معنی لغوی متاورس را یک فراجهان دانست که کاربران می‌توانند در آن نقش‌آفرینی داشته و با استفاده از فنّاوری و سخت‌افزارهای واقعیت مجازی در آن محیط با دیگران در تعامل باشند [۹].

پیش‌بینی‌ها نشان می‌دهد متاورس که از آن به‌عنوان پیشرفته‌ترین فضای اینترنتی یاد می‌شود، جانشینی برای فضای اینترنتی فعلی، شبکه‌های اجتماعی و بازی‌های آنلاین باشد. متاورس این امکان را برای افراد فراهم می‌کند تا بدون نیاز به حضور فیزیکی در کنار یکدیگر، باهم معاشرت کنند، به تفریح بپردازند، وارد فضاهای شغلی جدید شوند و نوع جدیدی از تعامل را تجربه نمایند.

البته همچون دیگر فناوری‌های جدید؛ صحبت از متاورس با واکنش‌هایی همراه بوده است و برخی بر این باورند که ایجاد فضای متاورسی غیرممکن است. با این وجود رشد پروژه‌های متاورسی در همین مدت کوتاه، ورود سرمایه‌های هنگفت به این فضا و استفاده از فنّاوری‌هایی مانند واقعیت افزوده و واقعیت مجازی این غیرممکن را ممکن ساخته و شرکت‌های پیشرو در فناوری همچنان در تلاش هستند تا توجه سرمایه‌گذاران و کاربران را به قابلیت‌های متاورس جلب کنند.

در حال حاضر، فضا برای انتقال داده‌های دیجیتال از وب ۲ به وب ۳ آماده‌شده و این دگرگونی در زیرساخت و حرکت به سمت کاربر محوری باعث ایجاد برنامه‌های کاربردی جدید ازجمله امورمالی غیرمتمرکز و احیای ایده‌های تحقق‌نیافته مانند متاورس شده است.

هدف نهایی متاورس ایجاد یک فضای مجازی با شباهت بسیار به دنیای فیزیکی است تا آواتارها بتوانند آزادانه با دیگران در تعامل قرار بگیرند. این تعاملات می‌تواند روی شرایط کاری و ارتباطی شما با افرادی که در فضاهای متاورسی در ارتباط هستید، تأثیرگذار باشد؛ برای مثال متاورس می‌تواند فرصت دورکاری را برای شما فراهم کند تا بتوانید از کشور یا شهر خود با کمپانی‌های بزرگ دنیا وارد همکاری شوید.

این گامی بسیار بزرگ است و باعث تغییرات شگرفی در سبک زندگی خواهد شد؛ اما به همان اندازه هم سؤالات زیادی را در ذهن کاربران و سرمایه‌گذاران ایجاد می‌کند.

در این مقاله سعی بر این شده تا اکوسیستم متاورس تشریح و در ادامه چالش‌ها و جرائم هر بخش توضیح داده شود.

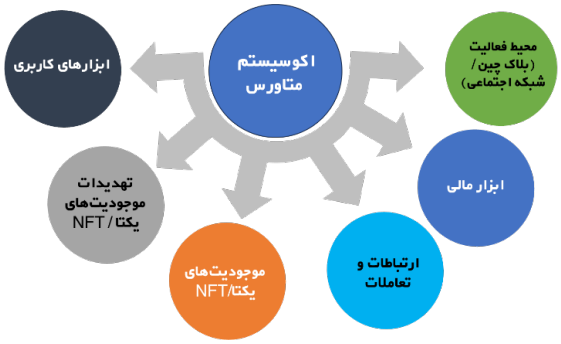
۲ اکوسیستم متاورس

اکوسیستم متاورس در این مقاله به شش بخش تقسیم شده است (شکل ۱).

۱.۲ محیط فعالیت (بلاک‌چین / شبکه اجتماعی)

محیط فعالیت کاربران متاورس به دودسته بر مبنای بلاک‌چین [1] و شبکه اجتماعی یا جهان واقعی تقسیم‌بندی می‌شود.

[1] blockchain



شکل ۱: اکوسیستم متاورس

بلاک‌چین فناوری اصلی ارز دیجیتال است که حیات یک پلتفرم بدون وابستگی به نهاد مرکزی را تضمین می‌کند و می‌توان از آن در حوزه‌های مختلف استفاده کرد. بلاک‌چین اختراعی برجسته و مبتکرانه است؛ زاییده فکر یک فرد یا گروهی از افراد که بانام مستعار ساتوشی ناکاموتو شناخته می‌شوند [۱].

به زبان ساده، بلاک‌چین یک نوع سیستم ثبت اطلاعات و گزارش است. تفاوت آن با سامانه‌های دیگر این است که اطلاعات ذخیره‌شده روی این نوع سیستم، میان همه اعضای یک شبکه به اشتراک گذاشته می‌شود. با استفاده از رمزنگاری و توزیع داده‌ها، امکان هک، حذف و دست‌کاری اطلاعات ثبت‌شده، تقریباً از بین می‌رود [۱].

مفهوم بلاک‌چین اولین بار با پیدایش بیت کوین به‌وجود آمد و پادشاه ارزهای دیجیتال از این راهکار برای ذخیره اطلاعات مربوط به دارایی کاربران بهره برد.

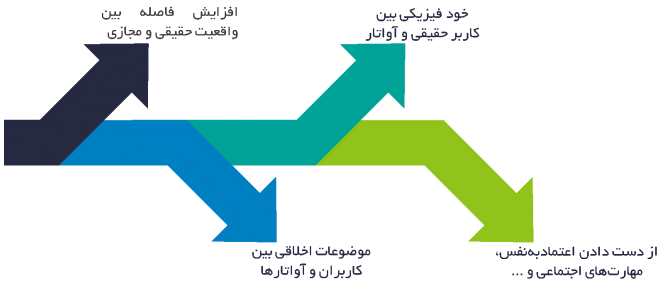
به‌عنوان‌مثال تمامی بازی‌های متاورسی به‌عنوان جهان متاورس بر مبنای بلاک‌چین تعریف می‌شوند که در آن‌ها اجزا بر اساس بلاک‌چین هستند؛ مانند بازی دیسترالند که در آن از رمزارز مانا[۲] (MANA) استفاده می‌شود [۶].

نوع دیگر محیط فعالیت متاورس همان دنیای واقعی یا شبکه‌های اجتماعی ساختگی است که کاربران با استفاده از لباس‌های پوشیدنی در آن محیط فعالیت می‌کنند. این نوع همان هدفی است که در حقیقت شرکت متا (فیس‌بوک سابق) به دنبال ایجاد آن است [۶].

۲.۲ ابزار مالی

ابزارهای مالی همان روش تبادل و تراکنش مالی در دنیای متاورس است. در حال حاضر با توجه به اینکه محیط فعالیت متاورس بیشتر بر مبنای بلاک‌چین است ابزارهای مالی نیز همان رمزارزها و توکن‌ها هستند که بسته به نوع هر بستر یا بازی متاورس تفاوت می‌کنند. این رمزارزها به‌طور کلی در سایت coinmarketcap.com و در بخش metaverse دسته‌بندی شده است [۱].

[2]Mana: Grayscale Decentraland Trust



شکل ۲: ارتباطات در متاورس

۳.۲ ارتباطات و تعاملات

ارتباطات در متاورس به‌نوعی وابستگی به رابطه بین هویت واقعی و مجازی دارد. این رابطه وابستگی و مسئولیت‌پذیری بین کاربر حقیقی و آواتار را نشان می‌دهد. از خطراتی که در این رابطه به وجود می‌آید می‌توان به موارد ذیل اشاره نمود (شکل ۲)؛

- افزایش فاصله بین واقعیت حقیقی و مجازی
- موضوعات اخلاقی بین کاربران و آواتارها
- خود فیزیکی بین کاربر حقیقی و آواتار
- از دست دادن اعتمادبه‌نفس، مهارت‌های اجتماعی و ...

۴.۲ موجودیت‌های یکتا/ NFT

NFT (توکن غیرقابل تعویض)، یک واحد منحصربه‌فرد داده است و از فناوری استفاده می‌کند که به محتوای دیجیتال (از ویدیوها گرفته تا آهنگ‌ها و تصاویر) اجازه می‌دهد تا در بلاک‌چین‌های ارزهای دیجیتال، به‌ویژه اتریوم، ثبت و احراز هویت شوند. پس از ورود محتوا به بلاک‌چین، هر تراکنش از نقل و انتقالات تا فروش، در زنجیره‌ای ثبت می‌شود و در یک دفتر کل، تاریخچه، منشأ و قیمت آن به‌راحتی قابل‌دسترسی است. هدف اصلی NFT، آسان کردن مالکیت و فروش محتوای دیجیتال است. درواقع NFT به وجود آمده تا محتوای دیجیتالی را غیرقابل تکثیر کند. NFT یا توکن غیرمثلی با ارزهای دیجیتال رایجی که آن‌ها را می‌شناسیم متفاوت است. به‌طور مثال شما می‌توانید هرکدام از ارزهای دیجیتال مانند بیت کوین، اتریوم، ریپل یا هر ارز دیجیتال دیگری را در مقابل دیگری معاوضه کنید اما NFTها این‌گونه نیستند.

با توجه به نوظهور بودن توکن‌های غیرمثلی، شناخت دقیقی از عوامل مؤثر بر موفقیت آنها در دسترس نیست. توکن‌های غیرمثلی این امکان را ایجاد می‌کنند که آثار هنری مختلف در قالب آن‌ها عرضه شوند و به‌این‌ترتیب مسئله حراست از مالکیت معنوی روی آثار هنری مختلف تا حد زیادی برآورده می‌شود. همچنین

این روش برای تأمین مالی آثار هنری نیز به‌کار گرفته می‌شود. با استفاده از آثار مسئولیت اجتماعی می‌توان به ایجاد اعتماد و نوع‌دوستی در سرمایه‌گذاران آثار هنری پرداخت [۲].

NFTها کاربرد بسیار زیادی دارند و در صنعت‌های مختلفی می‌توان از آنها استفاده کرد. اما مهم‌ترین استفاده آن‌ها در صنعت گیمینگ و کلکسیون‌ها است [۲].

جک دورسی (بنیان‌گذار توییتر) یکی از معروف‌ترین افرادی است که از بازار ارزهای دیجیتال حمایت می‌کند. آقای دورسی برای اینکه از NFTها حمایت کند، اولین توییت خود را به NFT تبدیل کرد و به فروش گذاشت. طبق مزایده‌ای که انجام شد این تصویر با مبلغ ۳ میلیون دلار به فروش رسید [۲].

وب‌سایت اُپن سی را می‌توانیم به‌عنوان بزرگ‌ترین پلتفرم معاملاتی توکن‌های غیرمثلی معرفی کنیم. یکی از بزرگ‌ترین مزایای این پلتفرم این است که تقریباً همه نوع NFT در این سایت وجود دارد؛ از کارت‌های دیجیتالی تا آیتم‌های بازی‌های بلاک‌چینی در این سایت مورد معامله قرار می‌گیرند. علاوه بر این در این سایت ابزار ویژه‌ای برای سازندگان NFT وجود دارد که با استفاده از آن می‌توانند ان‌اف‌تی خود را به‌وجود آورند [۲].

۵.۲ تهدیدات موجودیت‌های یکتا / NFT

تهدیدات NFT: اگر فایل‌های داده NFT در یک حمله باج‌افزار رمزگذاری شوند، می‌توان مالک را از دسترسی به دارایی مسدود کرد [۲].

کلاه‌برداری مالی: کلاه‌برداران ممکن است فروش آثار هنری تقلبی یا دزدیده‌شده را در متاورس تسهیل کنند [۲].

تهدیدات VR/AR/MR/XR: کلاه‌برداران می‌توانند گالری‌های متاورس جعلی برای نمایش و فروش آثار تقلبی ایجاد کنند [۷].

۶.۲ ابزارهای کاربری

مهم‌ترین راه برای ورود به متاورس استفاده از ابزار سخت‌افزاری است. البته این موضوع تا حدی منجر به ایجاد مشکلاتی نیز خواهد شد [۷]. به‌عنوان مثال؛ اتکای متاورس به فناوری واقعیت مجازی، توسعه و پذیرش گسترده آن را محدود می‌کند و همچنین فقدان گرافیک باکیفیت بالا و عدم پویایی، دو محدودیت مهم به‌شمار می‌روند. برای مثال؛ می‌توان به هزینه هدست اچ‌تی‌سی‌وایو پرو ۲ اشاره کرد که در سال ۲۰۲۱ هزینه‌ای معادل ۷۹۹ دلار آمریکا به همراه کنترلرها داشت که مانعی برای پذیرش گسترده این فناوری است. با این وجود هم‌زمان با گسترش فناوری نرم‌افزاری، سخت‌افزارها هم پیشرفت خواهند کرد و زمانی که به تطابق درستی بین این دو بخش برسیم، می‌توان گفت اوج شکوفایی متاورس را شاهد خواهیم بود [۷].

۱.۶.۲ واقعیت مجازی (VR)

واقعیت مجازی یک تجربه مجازی است که توسط یک دستگاه، به میدان دید یک کاربر اضافه می‌شود. محیط‌های واقعی مجازی به کاربران اجازه می‌دهند تا با همتایان مجازی در تعامل باشند، زندگی واقعی

را تجربه کنند و دانش علمی را بیاموزند. واقعیت مجازی درواقع یک محیط سه‌بعدی تعاملی و باورپذیر هست که رایانه آن را ایجاد می‌کند و می‌توان آن را کشف کرده و احساس کنید که ازنظر فیزیکی و روانی در آنجا حضور دارید [۸].

به‌طور کلی ابزارهای کاربردی برای ایجاد فضای متاورس شامل مواردی مانند شبکه ارتباطی، هوش مصنوعی، بلاک‌چین، IOT و رباتیک، واقعیت افزوده، پروتکل‌های امنیتی و بینایی کامپیوتری است [۸].

۲.۶.۲ تهدیدات ابزارهای کاربری متاورس

- تهدیدات فیزیکی سایبری: حملات مرد میانی بین تجهیزات صنعتی و اپراتورهای راه دور
- حملات IT سنتی: استفاده از اکسپلویت‌های آسیب‌پذیر برای دسترسی به تجهیزات صنعتی
- تهدیدات VR/AR/MR/XR: مجرمان می‌توانند از جفت‌های دیجیتال برای برنامه‌ریزی یک حمله به مرکز صنعتی استفاده کنند [۷].

۳.۶.۲ هویت کاربری (آواتار / ID)

هویت کاربری در متاورس می‌تواند به دو دسته کلی تقسیم‌بندی شود.

در نوع اول؛ کاربر با ایجاد یک آواتار در محیط نقش‌آفرینی کرده که این نوع می‌تواند شامل آواتاری بر اساس NFT و یا با استفاده از ابزارهای واقعیت مجازی باشد [۸].

در نوع دوم؛ کاربر با استفاده از ثبت‌نام در بستر متاورس (مانند بازی‌های متاورس) نقش‌آفرینی می‌کند.

ازجمله چالش‌های هویت کاربری می‌توان به موارد ذیل اشاره کرد؛

- درهم‌تنیدگی هویت فیزیکی افراد و هویت دیجیتال
- تهدید حریم خصوصی کاربران و آواتار
- ظهور نقش‌های جدید، تعدد نهادهای تأمین‌کننده هویت و خصیصه‌های هویتی حریم خصوصی
- جرائم احتمالی علیه آواتار (آزار جنسی، تهمت، تهدید و...)
- پیدایش موضوعاتی مانند اجاره و سرقت هویت

۳ متاورس، فرصت‌ها و سرمایه‌گذاری

متاورس همگام با دنیای مجازی تکامل می‌یابد و درواقع یک فضای سه بعدی مجازی مشترک است که برای ایفای نقش رسانه‌های اجتماعی و اینترنت طراحی شده است [۳]. پیشرفت وب ۳ با ایجاد دسترسی بیشتر برای عموم مردم و واقعی‌تر کردن فضای مجازی، بر بخش فناوری تأثیر می‌گذارد [۳]. دراین بین پروژه‌هایی ایجاد می‌شوند و مؤسسات بزرگ از آن‌ها حمایت می‌کنند تا متاورس را طی زمان به واقعیت تبدیل

کنند. پروژه‌هایی مانند: دیسنترالند، سندباکس، اکسی‌اینفینیتی، انجین و ...؛ اینها پروژه‌هایی هستند که رشد متاورس را توضیح می‌دهند [۳].

۱.۳ چرا باید در متاورس سرمایه‌گذاری کنیم؟

شیکسنگ مائو مدیرعامل و یکی از بنیانگذاران کوبو، مدیر دارایی ارزهای دیجیتال نیز می‌گوید: «متاورس پتانسیل بسیار زیادی برای تغییر سبک زندگی و ارتباطات ما دارد» [۳].

«بهترین روش برای سرمایه‌گذاری رمزارز در متاورس خرید زمین و NFT است. هنرهای گرافیکی، قطعه‌های صوتی یا ویدئویی NFTهای رایجی هستند که به سرمایه‌گذاران اجازه می‌دهند تا یک دارایی مجازی شده را در بلاک‌چین نگه‌دارند» [۳].

سان مورالس مدیرعامل myobu می‌گوید: «نکته‌ای که باید در ابتکارات متاورسی مبتنی بر رمزارزها مدنظر قرار داد این است که می‌توان منابع و دارایی‌های ملموسی را در متاورس به‌دست آورد و آن را با کالاهای دنیای واقعی تعویض کرد» [۴].

جوئل دیتز، از طراحان ArtWallet می‌گوید: «خرید و توسعه زمین و دارایی‌های مجازی را آغاز کنید. در چند پروژه با پتانسیل رشد ۱۰۰ برابری شرکت کنید و سبدهای سرمایه‌گذاری‌تان را متنوع سازید» [۴].

۲.۳ چگونه در متاورس سرمایه گذاری کنیم؟

سرمایه‌گذاری با خرید NFT و یا زمین انجام می‌شود، برای خرید زمین در متاورس باید حداقل حدود سه تا پنج هزار دلار سرمایه داشته باشید، یکی از ساده‌ترین راه‌های خرید زمین این است که یک زمین مناسب با مقدار پول خود خریداری نموده و نگه‌داری شود. پروژه‌های متاورسی روزبه‌روز پیشرفت می‌کنند و بااین اوصاف، ارزش زمین بالا می‌رود. مثلاً یک زمین در شمال غربی دیسنترالند ۹۰۰ دلار ارزش داشته و اکنون ارزش این زمین حداقل ۱۰۰ برابر شده است [۴].

راه دیگر این است که در زمین خریداری شده فعالیت شود. مثلاً بازی طراحی کرده یا فروشگاه و گالری ایجاد شود و سپس آن را با ملک با قیمت بالاتری به فروش برسانند و یا اینکه آن را به یک کسب‌وکار تبدیل کرد [۴].

متاورس هر چقدر به جلو حرکت می‌کند، به نفع کسانی است که زودتر از بقیه در آن فعالیت خود را شروع کرده‌اند [۴].

۴ جرائم و تخلفات ابزارهای مالی در متاورس

مطابق آنچه در قسمت‌های قبل گفته شد، ابزارهای مالی همان رمزارزهای به‌کار گرفته‌شده در فضای متاورس هست. رمزارزهایی مانند APE، MANA، SAND، THETA، AXS ازجمله واحدهای تراکنش در بازی‌های متاورس است.

انواع دسته‌بندی جرائم و تخلفات در حوزه رمزارزها که به‌نوعی به‌عنوان بخشی از اکوسیستم متاورس می‌باشند شامل کلاه‌برداری، تجارت الکترونیکی، علیه امنیت ملی، اخلال در نظام اقتصادی، پول‌شویی، سرقت و جعل هویت است.

۱.۴ کلاه‌برداری

عنوان جرم: خالی‌فروشی. شامل فروش رمزارز بدون انتقال رمزارز موردنظر به کیف پول اشخاص و یا بدون نگه‌داری رمزارز معادل در کیف پول مشخص، درج یا نمایش موجودی غیرواقعی در کیف پول رمزارز اشخاص به شیوه متقلبانه.

عنوان جرم: تقلب در فروش رمزارز. شامل فریفتن اشخاص به داشتن دارائی‌های موهومی به انواع شیوه‌های متقلبانه؛ اقدام به خلق رمزارز با پشتوانه نامشخص یا با کاربردهای ادعایی که در عمل فاقد پشتوانه یا کاربرد مورداشاره بوده و ارزش آن توکن تنها یک ارزش غیرواقعی است.

عنوان جرم: غصب رمزارز اشخاص شامل فروش رمزارزها بدون اعطای اختیار دخل و تصرف در آن به خریدار، یا بدون کسب اجازه کتبی، صریح و انکارناپذیر. گاهی اوقات صرافی‌های رمزارز، رمزارزهای فروخته‌شده به افراد را در کیف پول خود صرافی نمایش می‌دهند اما اجازه انتقال به کیف پول دیگر را نمی‌دهند و برای تبدیل آن به ریال نیز فرد تنها مجاز است رمزارز خود را در صرافی خریداری‌شده به ریال تبدیل کند؛ همچنین ممکن است افراد را مجبور به تبدیل رمزارزها به توکن واسط نمایند. حسب مورد در قالب عنوان مجرمانه خیانت‌درامانت نیز قابل‌شناسایی و دسته‌بندی است.

عنوان جرم: عملیات پانزی با بهره‌گیری از رمزارزها. در کلاه‌برداری به روش پانزی، به افراد وعده دریافت سود بالا در کوتاه‌ترین زمان از طریق سرمایه‌گذاری در بازارهای مالی را می‌دهند که این سودها هیچ منشأ واقعی ندارد بلکه از محل سرمایه کاربران جدید، سود به کاربران قدیمی پرداخت می‌گردد. در این روش برای جذب بیشتر مخاطب بعضاً از روش‌های هرمی استفاده می‌شود. در این روش سرمایه‌گذاری و پرداخت سود توسط رمزارزها صورت می‌پذیرد.

۲.۴ تجارت الکترونیکی

عنوان جرم: هرگونه تبلیغات فریبنده در راستای ترویج و فروش. شامل هرگونه تبلیغات فریبنده در راستای ترویج رمزارزها (داخلی یا خارجی)، یا هرگونه تشویق و ترغیب عمومی به سرمایه‌گذاری در حوزه رمزارزها؛ هرگونه تبلیغات و تشویق مردم جهت سرمایه‌گذاری در سایت‌های پرداخت‌کننده سودهای کلان در کوتاه‌مدت، ارائه اطلاعات غیرواقعی در خصوص سایت‌های فعال در حوزه رمزارزها و سوءاستفاده از عدم آگاهی مردم؛ هرگونه اطلاع‌رسانی که منجر به ترغیب یا تشویق عمومی به خرید یک توکن مشخص یا بازار سازی برای آن گردد. ارائه هرگونه اطلاعات مرتبط با ترویج رمزارزها، ارائه سیگنال‌های مرتبط با بازارهای رمزارز، هرگونه تبلیغات رمزارزهای منتشرشده داخلی فاقد مجوز از سازمان بورس و اوراق بهادار.

عنوان جرم: عدم ارائه یا عدم به‌روزرسانی اطلاعات کارگزاران مبادله درزمینه رمزارزها. شامل هرگونه عدم ارائه یا عدم به‌روزرسانی اطلاعات کارگزاران مبادله درزمینه رمزارزها؛ ازجمله مخفی نگاه‌داشتن اطلاعات هویتی و شناسنامه‌ای شرکت، مخفی نگاه‌داشتن اطلاعات صاحبان کسب‌وکار یا هرگونه استفاده از هویت‌های جعلی در خصوص کسب‌وکار یا گردانندگان آن.

۳.۴ علیه امنیت ملی

عنوان جرم: به‌کارگیری رمزارزها در عملیات مجرمانه و تأمین مالی تروریسم. شامل استفاده از رمزارزها جهت انجام پرداخت‌های مالی مخل امنیت عمومی و برخلاف منافع و مصالح کشور، به‌کارگیری رمزارزها جهت اخذ وجوهات یا تسهیل جریانات مالی مرتبط با کلاه‌برداری‌های رایانه‌ای، باج‌گیری سایبری و سایر اعمال غیرمجاز و مجرمانه در فضای مجازی.

۴.۴ اخلال در نظام اقتصادی

عنوان جرم: خلق و انتشار رمزارز با پشتوانه دارایی‌های تصریح‌شده در مواد ۵ الی ۸ قانون پولی و بانکی کشور. خلق، توزیع و مدیریت رمزارز با پشتوانه طلا، ریال، ارز، اسناد و اوراق بهادار دولتی و جواهرات سلطنتی طبق مفاد قانون پولی و بانکی کشور در انحصار بانک مرکزی بوده و به‌جز این خلاف قانون است.

عنوان جرم: به‌کارگیری رمزارزها در عملیات بازاریابی هرمی و شبکه‌ای. در سیستم هرمی برای فروش کالا یا خدمت، هریک از اعضا شروع به زیرمجموعه گیری می‌کند و بسته به میزان ورود اعضای جدید، اعضای قدیمی‌تر در پوشش تولید کالا و خدمت یا وعده سرمایه‌گذاری در انواع بازارها ازجمله رمزارزها سهیم می‌شوند. در این روش سرمایه اولیه و پرداخت پورسانت ممکن است با رمزارزها یا سایر روش‌های دیگر انجام شود.

عنوان جرم: هرگونه پرداخت به‌وسیله رمزارزها در داخل کشور. شامل استفاده از انواع توکن‌ها و رمزارزها به‌عنوان ابزار پرداخت حضوری یا غیرحضوری یا به‌کارگیری آن‌ها به‌عنوان ابزار وثیقه سپاری در تعامل مالی حضوری یا غیرحضوری.

عنوان جرم: قمار از طریق تبادلات رمزارز (انجام معاملاتی مانند ارز فردایی). انجام معاملات مشابه قمار در حوزه رمزارزها مانند معاملات فردایی (فیوچرز) که توافقنامه‌ای بین دو طرف به‌منظور پیش‌بینی وقوع امری خاص (که در اینجا قیمت رمزارز در آینده است) است که بازنده یا بازندگان ملزم به پرداخت وجه، مال، منفعت، خدمت یا امتیاز مالی به‌صورت مستقیم یا غیرمستقیم به برنده یا برندگان هستند. منظور از برنده شخصی است که پیش‌بینی او درباره واقعه خاص (قیمت رمزارز) محقق شده است.

۵.۴ پول‌شویی

عنوان جرم: به‌کارگیری رمزارزها در پول‌شویی. شامل هرگونه استفاده از رمزارزها با نیت یا هدف مخدوش سازی مسیر ردگیری جریان تراکنش‌ها.

۶.۴ سرقت

عنوان جرم: سرقت داده‌های مرتبط با رمزارز. شامل هرگونه اقدام در راستای سرقت اطلاعات، سرقت کلید خصوصی اشخاص و در اختیار گرفتن رمزارز اشخاص جهت خارج‌سازی دارائی‌های رمزارز اشخاص از کیف پول ایشان و انتقال این دارائی‌ها به کیف پول دیگر.

عنوان جرم: استفاده از کارت یا حساب بانکی اشخاص ثالث در مبادلات رمزارزها. شامل انجام پرداخت‌های بانکی از طریق کارت، حساب بانکی، چک و سایر ابزارهای پرداخت متعلق به شخص ثالث، بدون اطلاع صاحب حساب یا بدون طی تشریفات قانونی مربوطه (اخذ رضایت‌نامه قانونی و یا وکالت‌نامه رسمی از وی).

۷.۴ جعل هویت

عنوان جرم: جعل هویت و سوءاستفاده از مدارک شناسایی اشخاص. شامل جعل هویت، هرگونه دست‌کاری در اسناد هویتی خود شخص یا سایرین، تغییر در چهره جهت ایجاد تشابه با سایرین یا هرگونه دست‌کاری در اسناد هویتی سایر اشخاص باهدف جعل هویت؛ هرگونه وارد نمودن، ایجاد یا تغییر داده‌های قابل استناد نظیر جعل تراکنش‌های رمزارز، جعل اطلاعات و مقدار موجودی کیف پول رمزارز.

۵ نتیجه

اینکه در آینده چه اتفاقاتی رقم خواهد خورد و روند متاورس چطور تغییر خواهد کرد قابل پیش‌بینی نیست؛ چراکه امکانات و درگاه‌هایی به روی ما بازخواهد شد که شاید در حال حاضر هیچ ایده‌هایی از آن‌ها نداشته باشیم؛ اما با توجه به اطلاعاتی که در دست داریم، می‌شود این‌طور برآورد کرد که متاورس گام بعدی دنیای دیجیتال خواهد بود و انتظار می‌رود تمام دارایی‌های واقعی و حقیقی، نوع دیجیتال خودشان را در این فضا داشته باشند. از آواتارها که سمبل شخصیت حقیقی ما کاربرها هستند گرفته تا ماشین، خانه، زمین، مغازه و... همه این‌ها یک نسخه دیجیتال و مجازی خواهند داشت و همین موضوع باعث می‌شود فضای اقتصادی، سبک زندگی، کاری و حتی تفریحی ما شکل و حالات بسیار متفاوتی را در آینده داشته باشد.

تهدیدات در فضای متاورس، خصوصاً علیه هویت‌ها و موجودیت‌ها شامل انواع گوناگونی هستند و جرائم درزمینه ابزارهای مالی و رمزارزها که به‌عنوان واحدهای تراکنش در این محیط شناخته می‌شوند شامل کلاه‌برداری، تجارت الکترونیکی، علیه امنیت ملی، اخلال در نظام اقتصادی، پول‌شویی، سرقت و جعل هویت هست.

با توجه به انواع تهدیدات، تخلفات و جرائم در فضای متاورس (که البته در این مقاله به جرائم مالی این فضا اشاره شد)، وجود قوانین، دستورالعمل و آیین‌نامه‌های اجرایی از سوی دولت‌ها و شرکت‌های پیشرو در این عرصه به‌عنوان بخش ضروری و پیش‌نیاز اصلی برای ورود به متاورس مبرم و اساسی هست.

مراجع

[۱] شاه‌چراغی، محمود، بلاک چین و عملکرد آن در عصر دیجیتال، فصلنامه کهربا، دوره: ۶، شماره: ۲۲، ۱۳۹۷.

[۲] صادقی، هانیه، فراترکیبی بر بررسی تأثیر مسئولیت اجتماعی بر موفقیت تأمین مالی جمعی مبتنی بر توکن‌های غیرمثلی (NFT Tokens) در آثار هنری، هجدهمین اجلاس بین‌المللی مدیریت، ۱۴۰۰.

[۳] حسینی، محمد، نیمه پنهان متاورس، انتشارات آراد کتاب، چاپ اول، ۱۴۰۱، فصل ۷، صفحات ۷۶-۷۷.

[۴] حسینی، محمد، نیمه پنهان متاورس، انتشارات آراد کتاب، چاپ اول، ۱۴۰۱، فصل ۷، صفحات ۸۰-۸۱.

[۵] حسینی، محمد، نیمه پنهان متاورس، انتشارات آراد کتاب، چاپ اول، ۱۴۰۱، صفحه ۱۱۶.

[6] https://coinmarketcap.com/view/metaverse

[7] https://www.trendmicro.com, August 08, 2022.

[8] Numaan Huq, METAVERSE OR METAWORSE?, 2022.

[9] Deloitte 2022, Metaverse report—Future is here, Global XR industry insight, China, 2022.

توسل حق دفاع مشروع در حملات سایبری در حقوق بین‌الملل

علی حیدری، بیژن حیدری

ali.heydari.4001@gmail.com

چکیده

یکی از شیوه‌های نوین تخاصم درصحنه بین‌المللی، حملاتی است که در بستر فضای سایبری صورت می‌گیرد، هرچند این حملات پتانسیل ایجاد تلفات گسترده و خسارات وسیع را دارند اما سرعت بالای تغییرات در این حوزه موجب گردیده است که حقوق بین‌الملل از وضع قواعد جدید متناسب با فضای سایبری عاجز بماند. استفاده از فضای سایبری برای دستیابی سریع و مؤثر به اهداف راهبردی، امروزه به ابزار جدید جنگی و مهم برای همه بازیگران دولتی و غیردولتی تبدیل شده است. شناساییِ قلمرو حقوقیِ آن نیز با موانعی در شرایط مختلف و از جمله حقوق جنگ و حق دفاع مشروع رو به روست که ورود حقوق بین‌الملل به بحث را با چالش مواجه کرده است. در این پژوهش با رویکرد توصیفی و استفاده مطالعات پیشین سعی شده است تا به بررسی ابعد موضوع مطرح شده پرداخته شود.

کلمات کلیدی: جنگ سایبری، حقوق بین‌الملل، حملات سایبری، دفاع مشروع.

۱ مقدمه

در این نوشتار، حملات سایبری بازیگران غیردولتی صرفاً به منظور احراز انتساب آ نها به یک دولت بررسی می‌شود. پژوهش حاضر نتیجه می گیرد که حمله ی سایبری را می توان وفق ماده‌ی ۴(۲) منشور ملل متحد، توسل به زور مسلحانه توصیف نمود. از سوی دیگر، حمله ی سایبری گسترده به زیرساخت‌های اساسی که خسارات مادی یا تلفات انسانی قابل قیاس با حمله‌ی مسلحانه با سلاح‌های متعارف را در پی داشته باشد، حق توسل به دفاع مشروع را به دولت قربانی اعطاء می‌نماید.

هم چنین، درواکنش به حمله ی سایبری که در حد حمله‌ی مسلحانه نباشد، اما حمله‌ی مسلحانه‌ی قریب الوقوعی را با تسلیحات متعارف تدارک ببیند، می‌توان به دفاع مشروع متوسل گردید.

گسترش فزاینده‌ی فن‌آوری اطلاعات و ارتباطات به تحول و دگرگونی جوامع در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی منجر شده است. جوامع، به نحو فزاینده‌ای به رایانه و شبکه‌های رایانه‌ای و خدمات حیاتی متکی به اینترنت وابسته شده‌اند. اهمیت جهانی فضای مجازی، آسیب‌پذیری‌هایی را نیز برای آن در پی داشته است؛ این بدین دلیل است که فن‌آوری و تخصص در زمینه‌ی سایبر، ساده و ارزان به دست

می‌آید؛ این امر به کشورهای ضعیف‌تر و حتی کنشگران غیردولتی امکان می‌دهد که به کشورهای دارای قدرت نظامی متعارف برتر، آسیب‌های قابل توجهی مانند از کار انداختن ژنراتورهای برق، قطع سیستم کنترل و ارتباطات فرماندهی، سرنگون کردن هواپیماها، ذوب راکتورهای هسته‌ای، انفجار خطوط لوله و تخریب تسلیحات را وارد نمایند (حسن بیگی، ۱۳۸۴).

در نتیجه‌ی بروز چنین تهدیداتی است که امنیت در فضای سایبر به دغدغه‌ی عمومی جامعه‌ی بین‌المللی بدل شده است. در این چارچوب، مجمع عمومی سازمان ملل متحد، مجموعه ای از قطعنامه‌ها را در خصوص پیشرفت‌های حاصل شده در خصوص اطلاعات و ارتباطات از راه دور و تأثیر آن بر امنیت بین‌المللی تصویب نموده و تأکید کرده است: «سوء استفاده‌ی جنایتکارانه از فن‌آوری های اطلاعاتی می‌تواند تأثیر شدیدی بر تمامی کشورها داشته باشد» (A/RES/56/121 of 19 December 2001). یکی از جنبه هایی که حقوقدانان بین‌المللی می‌توانند موضوع امنیت سایبری را از آن منظر بررسی نمایند، توسل حق دفاع مشروع در حملات سایبری است؛ حملات سایبری ارتکابی توسط کنشگران غیردولتی، صرفاً به منظور تبیین قابلیت یا عدم قابلیت انتساب به‌یک دولت بررسی می شود. بنابراین، پژوهش حاضر منصرف از جرایم سایبری ارتکابی توسط اشخاص حقیقی یا حقوقی خصوصی است که به لحاظ منافع شخصی بودن مانند سرقت پول از حساب‌های بانکی و علیه محرمانه داده‌ها و سیستم‌های رایانه‌ای صورت می‌گیرند. در ضمن «تروریسم سایبری» که عبارت است از تخریب یا اخلال گسترده‌ی داده‌ها، اطلاعات یا سامانه‌های رایانه‌ای یا ارتباطی از طریق فضای سایبر با انگیزه‌های سیاسی، مذهبی، ایدئولوژیکی و نژادی (پاکزاد، ۱۳۸۸) با این تحقیق ارتباط نمی‌یابد.

۲ مفهوم دفاع مشروع

«دفاع مشروع» امروزه استثنائی مهم بر اصل منع توسل به زور محسوب می‌شود. حق دفاع مشروع در «حملات مسلحانه» به‌عنوان یک اصل حقوق بین‌الملل عرفی است که در منشور به‌عنوان یک «حق ذاتی» به آن اشاره شده است. مفهوم عینی دفاع مشروع و اهمیت آن در چارچوب تحولات حقوق بین‌الملل در طول قرن گذشته به نحو قابل ملاحظه‌ای تغییر کرده است. در واقع با گسترش سازماندهی حقوق بین‌الملل در طی دهه‌های گذشته و بویژه فرایندی که با تأسیس جامعه ملل آغاز شده است مفهوم دفاع مشروع اهمیت قابل ملاحظه‌ای یافته است.

۳ مفهوم سایبری

واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح «سایبرنتیک» توسط ریاضیدانی به نام نوربرت وینر Norbert Wiener در کتابی با عنوان «سایبرنتیک، کنترل و ارتباط در حیوان و ماشین» در سال ۱۹۴۸ به‌کار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی (و کامپیوترها) است.

سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای

کامپیوتر و اطلاعات است. در طی توسعه اینترنت واژه های ترکیبی بسیاری از این کلمه سایبر به‌وجود آمده است. از محیط سایبر (Cyberspace) نیز تعاریف گوناگونی به‌عمل آمده است که می‌توان در مجموع محیط سایبر را چنین تعریف کرد. محیط مجازی و غیرملموس موجود در فضای شبکه‌های بین‌المللی که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ‌ها ، ملت‌ها، کشورها و به‌طور کلی هرآنچه در کره خاکی به‌صورت ملموس و فیزیکی وجود دارد در یک فضای مجازی به‌شکل دیجیتالی وجود دارد و قابل استفاده و دسترس استفاده‌کنندگان و کاربران است و از طریق رایانه، اجزای آن و شبکه‌های بین‌المللی به‌هم مرتبط هستند.

۴ قانون‌گذاری در فضای سایبر

شیوه قانون‌گذاری در فضای سایبر، مبتنی بر دو نوع نگرش متفاوت به حاکمیت در فضای سایبر است. نگرش نخست، مبتنی بر انحصار دولت‌ها در عرصه قانون‌گذاری فضای سایبر است و نگرش دوم که ملهم از دکترین میراث مشترک بشریت است، مخالف ورود انحصاری دولت‌ها به این عرصه است. هر یک از این دو رویکرد، موجد روش‌های قانون‌گذاری مختلفی در فضای سایبر است. روش‌های قانون‌گذاری ملی، بین‌المللی و خودانتظامی در زمره روش‌های قانون‌گذاری در فضای سایبر به شمار می‌آیند.

اگرچه توسل به هر یک از روش‌های قانونگذاری با اشکالاتی در عرصه اجرا روبه‌روست، در این میان می‌توان رویکردی بینابین و مختلط را برگزید تا ضمن رفع نواقص دیگر روش‌ها، زمینه را برای نیل به تفاهم میان کشورها و گروه‌های فعال در زمینه فضای سایبر هموار سازد. نگرش دولت جمهوری اسلامی ایران، اساساً مبتنی بر شیوه قانون‌گذاری ملی است. با این حال، عملکرد ایران در سطح بین‌المللی و به‌ویژه در اتحادیه بین‌المللی مخابرات، حاکی از پذیرش روش مختلط در قانون‌گذاری در فضای سایبر است.

۱.۴ صلاحیت کیفری مراجع قضایی در فضای سایبر

مسألهٔ چگونگی تعیین مرجع قضایی صالح جهت رسیدگی به جرائم ارتکابی در فضای مذکور است. چون بر اساس قواعد سنتی مهم‌ترین ضابطهٔ تعیین صلاحیت مراجع قضایی کیفری، مکان وقوع جرم می‌باشد و در فضای جدید سایبر، که یک فضایی مجازی و فارغ از مکان می‌باشد، چنین ضابطه‌ای قابل اجرا نبوده و یا مستلزم تعدیل ویژه می‌باشد. در همین راستا برخی سعی کرده‌اند همان قواعد سنتی ناظر بر صلاحیت کیفری مراجع قضایی را با نگرشی جدید در این فضا اجرا کنند و برخی دیگر با طرح تئوری‌های نو در خصوص صلاحیت، از قبیل «فضای سایبر به‌عنوان یک فضای آزاد بین‌المللی» و یا پیش‌بینی دادگاهی ویژه به نام «دادگاه دیجیتالی یا سایبری» و یا صلاحیت «دادگاه ذی‌ارتباط منطقی با جرم» را مطرح کرده‌اند. کشور ایران در قانون مجازات جرائم رایانه‌ای در ماده ۲۸ تئوری اول یعنی اجرای قواعد سنتی با نگرشی جدید را اتخاذ کرده است. در این مقاله سعی شده است هر یک از تئوری‌های مطرح شده در این زمینه مورد نقد و بررسی قرار گیرد و در نهایت یک معیار تلفیقی ارائه گردد، با این توضیح که تا جایی که قواعد سنتی قابل اجرا باشند همان قواعد اجرا می‌شوند و در غیر آن صورت تئوری صلاحیت دادگاه ذی‌ارتباط منطقی با جرم

به‌عنوان ضابطه نهایی پذیرفته شود.

۲.۴ اعمال صلاحیت کیفری در مورد جرائم ارتکابی در فضای سایبر

تشخیص صلاحیت محاکم کیفری در فضای واقعی عمدتاً مبتنی بر مکان و مرز می‌باشد اما فضای سایبر فاقد مکان و حصری است. حال سؤال اینجاست که آیا این فضا دارای رژیم خاص حقوقی است؟ آیا قواعد سنتی حاکم بر انواع صلاحیت‌ها با توجه به ویژگی‌های فضای سایبر قابل اعمال است؟ می‌توان گفت تأکید کشورها بر حاکمیت واصل سرزمینی سبب عدم ایجاد رژیم خاص حقوقی برای صلاحیت کیفری در فضای سایبر شده است. همچنین در بین انواع صلاحیت اصل سرزمینی بیشترین چالش را با این فضا دارد. صلاحیت‌های حمایتی وتابعیتی نیز چالش‌هایی با این امر دارند هرچند که صلاحیت جهانی به‌دلیل عدم اتکاء به مکان و مرز کاربردی‌تر بنظر می‌رسد.

۵ بهره‌گیری از حقوق معاهدات و عرف‌های بین‌المللی

در حا حاضر تعداد اندکی معاهده‌ی بین‌المللی وجود دارند که می‌توانند تشکیل دهنده‌ی یک عرف بین‌المللی باشند که نهایتاً در تنظیم جنگ سایبری تا حدودی به کار رود. برای مثال، معاهده‌ی «کنوانسیون بین‌المللی مخابرات» و ماده‌ی ۳۵ آن، هر گونه مداخله‌ی زیان‌بار با استفاده از ارتباطات از راه دور را ممنوع می‌کند.

ماده‌ی ۳۷ همان نیز به گونه‌ای ممکن است بر جنگ‌های سایبری اثرگذار باشد. همچنین ماده‌ی ۱۹ بند ۲ و ماده‌ی ۲۰ این کنوانسیون نیز مستعد بهره‌گیری در این خصوص است (Schaap, 2009: 21).

یک سند حقوقی بین‌المللیِ دیگر که قابلیت ارتباط گرفتن با موضوع را دارد، موافقت‌نامه‌ی اجتناب از فعالیت‌های خطرناک نظامی است که در سال ۱۹۴۹ بین ایالات متحده آمریکا و شوروی به امضا رسیده بود. این موافقت‌نامه هر گونه مداخله‌ی زیان‌بار در «سیستم‌های فرماندهی و کنترلی دشمن» را ممنوع کرده بود. در اواخر قرن بیستم نیز با افزایش توجه رسانه‌ها و محافل دانشگاهی به مفهوم نوظهور جنگ سایبری، در جامعه‌ی بین‌المللی تلاش‌هایی برای مذاکراتی برای انعقاد معاهده‌هایی در این زمینه صورت گرفت. به‌طور نمونه، روسیه در اکتبر ۱۹۹۴ متولی تصویب قطعنامه‌ای در کمیته‌ی اول شورای امنیت سازمان ملل شد که به‌عنوان تلاشی آشکار برای جلب نظر ملل متحد به این موضوع شناخته می‌شود. این قطعنامه شامل فراخوانی برای دولت‌ها بود که از نظرهای آنها در مورد ایجاد نظام‌های حقوقی بین‌المللی به‌منظور تهدید، گسترش، ساخت و استفاده از سلاح‌های اطلاعاتی خاص حمایت کند. این تلاش با استقبال اندکی در جامعه‌ی بین‌المللی مواجه شد و هرگز برای رأی‌گیری عمومی وارد مجمع عمومی ملل متحد نشد (Hoisington, 2009).

اینک شاید با گذشت دو دهه از طرح اولیه‌ی آن و گسترش تهدیدات و حملاتی که برخی از آنها اشاره شد، جلب نظر جامعه‌ی بین‌المللی به دشواری گذشته نباشد، اما احتمالاً پس از آنکه حمله‌ی سایبری به حد مخاصمه‌ی مسلحانه رسید، یک نظام امنیتی بین‌المللی که شامل حقوق بشردوستانه بین‌المللی و حقوق بشر می‌شود، به جریان می‌افتد.

توسل به مفهوم دفاع مشروع نیز در خصوص این حملات مورد تردید واقع شده و امکان اعمال این حق

در این فضا به استناد ماده ۵۱ منشور ملل متحد و یا حقوق بین‌الملل عرفی از مهم‌ترین پرسش‌هایی است که بی‌پاسخ مانده است. به نظر می‌رسد در صورتی که حملات سایبری به زیرساخت‌های حیاتی یک کشور نفوذ کرده و پتانسیل ایجاد تخریب و اضمحلال در حد یک حمله مسلحانه را داشته باشند، مسلحانه فرض شده و دولت قربانی از حق دفاع مشروع برخوردار خواهد بود. برای مثال در خصوص حمله کرم رایانه‌ای استاکس‌نت در سال ۲۰۱۰ به تأسیسات هسته ای ایران، صرف نظر از مسئله انتساب آن به‌عنوان یک امر موضوعی، حق دفاع مشروع قابل اثبات است (غلامعلی قاسمی، سعید نامدار،۱۳۹۷).

۶ توسل به دفاع مشروع در موارد نقض اصل منع تهدید یا استفاده از زور

مبانی حقوقی دفاع مشروع به عنوان یک قاعده در حقوق بین‌الملل که خود استثنایی بر قاعده اصل منع تهدید و یا استفاده از زور می‌باشد، در ماده ۵۱ منشور ملل متحد آمده است. دفاع مشروع در طرح مسئولیت بین‌المللی دولت‌ها ۲۰۰۱ به‌عنوان یکی از معاذیر رافع وصف متخلفانه بین‌المللی ذکر شده است و از شرایط اساسی آن احراز تجاوز مسلحانه و رعایت شرط تناسب و ضرورت در اعمال حق دفاع مشروع است. از موارد دیگر در رعایت آن محدود و تحت کنترل بودن آن می‌باشد که باید به شورای امنیت در این باره گزارش داد و به‌محض ورود شورای امنیت به قایه دفاع مشروع منتفی می‌شود (احمدرضا توحیدی، ۱۳۹۷).

در استناد به دفاع مشروع در مقابل حمالت سایبری سه رویکرد وجود دارد:

الف. رویکرد ابزارمحور: در این رویکرد استفاده از تسلیحات نظامی متعارف برای استناد به دفاع مشروع اهمیت دارد. در این رویکرد در صورتی یک حمله سایبری واجد شرایط استناد به ماده ۵۱ منشور است که از تسلیحات نظامی استفاده شود، مثال: بمباران سرورهای رایانه‌ای یا کابل‌های اینترنتی.

ب. رویکرد هدف‌محور: براساس این رویکرد در صورت وقوع یک حمله سایبری واحد به یک سامانه حیاتی کشور، می‌توان پاسخ نظامی متعارف به این حمله داد.

ج. رویکرد تأثیرمحور: رویکرد تأثیرمحور به‌واسطه شدت تأثیرات یک حمله سایبری، آن را یک حمله مسلحانه تلقی می‌کند. رویکرد تأثیرمحور به‌دلیل مواضع میانه خود از مقبولیت بیشتری برخوردار است.

حتی برخی از کشورها از جمله روسیه و آمریکا برای خود حق دفاع مشروع در مواجهه با حملات سایبری قائل شده‌اند. مقامات روس اعلام کرده‌اند که حتی حق توسل به سلاح اتمی در مواجهه با حملات سایبری را دارند (K. Joanna, 2009).

این قبیل موضع‌گیری از جانب کشورهای قدرتمند و عضو دائم شورای امنیت و موضع‌گیری‌های مشابه از سوی کشورهای دیگر به نوعی بیانگر آینده خطرناک حملات سایبری و لزوم شناسائی آن توسط جامعه بین‌المللی را برای جهانیان گوشزد می‌کند.

۷ ضرورت انجام دفاع مشروع

پذیرش عمومی اصل ضرورت به سال ۱۸۴۳ برمی‌گردد. قواعد حقوقی حاکم بر جنگ (Jus ad bellum) نظیر ممنوعیت توسل به زور بند (۴) ماده (۲) منشور را می‌توان در مورد جنگ‌های سایبری نیز قابل تسری دانست و حملات سایبری را به‌مثابه نقض اصل منع توسل به زور توصیف کرد. در مورد قواعد در جنگ (Jus in Bello) نیز تقریباً اکثر قواعد حقوق بین‌الملل بشردوستانه نظیر لزوم رعایت «اصل تفکیک میان نظامیان و غیرنظامیان» قابل اجرا است. برای مثال در موردی که حملات سایبری با ایجاد اختلال رایانه‌ای در بیمارستان‌ها یا مراکز درمانی، حیات غیرنظامیان را در معرض تهدید قرار می‌دهد و یا در جایی که حملات سایبری عملکرد تاسیساتی را مختل می‌سازد که مستقیم یا غیرمستقیم جان و مال غیرنظامیان را در معرض آسیب قرار می‌دهد، اصل مذکور را که در مواد (۵۴) پروتکل اول ۱۹۷۷ الحاقی به کنوانسیون‌های ژنو ۱۹۴۹ و نیز ماده (۱۴) پروتکل دوم الحاقی نیز منعکس شده است، می‌توان قابل اعمال دانست.

همچون حملات مسلحانه فیزیکی آنچنان که دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه (نیکارگوئه علیه آمریکا)، ۱۹۸۶ میلادی بر معیار آستانه و شدت درگیری ها برای تلقی آن به‌عنوان حمله مسلحانه تأکید کرد، در حملات سایبری نیز باید معیار شدت و گستردگی این حملات برای تلقی آن به عنوان حمله مسلحانه و نقض اصل قاعده منع توسل به زور مطمح نظر قرار گیرد.

۱.۷ بیانیه ستاد کل نیروهای مسلح

بیانیه ستاد کل نیروهای مسلح شامل چهار ماده، دستاورد مهم و اقدام مؤثری در تبیین سیاست‌های کشور نسبت به تهدیدات و حملات فضای سایبری محسوب می‌شود. در ماده (۱) تحت عنوان کلیات، راجع به حقوق بین‌الملل قابل اعمال بر فضای سایبری بر لزوم توزیع عادلانه منافع و امتیازات یک فضای صلح‌آمیز سایبری که متضمن «دسترسی» و «حاکمیت منصفانه» برای تمام دولت‌ها باشد، تأکید شده است.

«اصل مسئولیت مشترک اما متفاوت دولت‌ها» (Common But Differentiated Responsibilities) از دیگر اصول مهم حقوق بین‌الملل است که در بیانیه مزبور بدان استناد شده است. همچنین در این بیانیه اصل برابری حاکمیت دولت‌ها و ممنوعیت توسل به زور و عمل تجاوزکارانه در فضای سایبری نیز قابل اعمال توصیف شده است.

در ماده (۲) این بیانیه ضمن تسری اصل حاکمیت سرزمینی و صلاحیت دولت بر تمامی اجزای فضای سایبری، تأکید شده است که «هرگونه استفاده عامدانه از زور سایبری با پیامدهای فیزیکی یا غیر فیزیکی که تهدیدی برای امنیت ملی بوده یا منجر به بی‌ثباتی آن به واسطه بی‌ثباتی سیاسی، اقتصادی، اجتماعی و فرهنگی شود، ناقض حاکمیت دولت است». همچنین بیان شده است که «عملیات بهره‌برداری سایبری در مواقعی که مستلزم نفوذ غیرمجاز به زیرساخت‌های سایبری (دولتی یا خصوصی) تحت کنترل دولت دیگری باشد، می‌تواند نقض حاکمیت دولتِ هدف تلقی شود».

۸ واکنش علیه حملات سایبری

با این فرض که کشور قربانی بتواند مبدأ حمله‌ی سایبری را شناسایی کند و آن را به کشوری انتساب نماید، چندین گزینه را بدین شرح در دسترس خواهد داشت:

توسل به شورای امنیت سازمان ملل متحد. کشور قربانی بر اساس ماده‌ی ۳۵ (۱) منشور ملل متحد می‌تواند وضعیت را به شورای امنیت ارجاع نماید؛ ممکن است شورای مذکور روش‌های مناسب را بر اساس ماده‌ی ۳۶ (۱) منشور جهت حل و فصل اختلاف توصیه نماید؛ در صورتی که شورا وضعیت را تهدیدی علیه صلح، نقض صلح یا اقدام تجاوزکارانه تلقی کند، می‌تواند اختیارات خود را بر مبنای فصل هفتم منشور اعمال کند. هر چند در نظر طراحان منشور ملل متحد چنانچه شورای امنیت سازمان ملل متحد، یک حمله‌ی سایبری را تهدیدی علیه صلح تلقی کند (Osterdahl, 1998)، می‌تواند به‌موجب ماده‌ی ۳۹ منشور ملل متحد توصیه‌هایی را ارائه نموده و برای جلوگیری از وخیم‌تر شدن بحران و به‌موجب ماده‌ی ۴۰ این منشور اقداماتی را پیشنهاد نماید و سرانجام به استناد مواد ۴۱ و ۴۲ منشور ملل متحد در خصوص اقدامات مبتنی بر عدم توسل به زور و یا توسل به زور اتخاذ تصمیم کند. شورای امنیت سازمان ملل متحد همچنین می‌تواند محاصره‌ی سایبری را بر کشور مسؤول حمله‌ی سایبری و به‌منظور ممانعت از استمرار یا تکرار حمله، تحمیل نماید.

در این راستا، مطابق با حقوق بین‌الملل یک دولت می‌بایست میان حمله و منبع آن ارتباط برقرار کند؛ زیرا قوانینی که بر پاسخ مشروع به یک تهاجم تصریح می‌کنند (پاسخ به تهاجم را مجاز می‌شمارند)، بر اساس دولتی بودن یا دولتی نبودن منشأ تهاجم متفاوت است؛ بنابراین اِشکالی که اینجا وجود دارد این است که مواد یاد شده تنها ناظر به دولت‌هاست پس برای منشأ غیردولتی نمی‌توان از این مواد بهره جست؛ بنابراین واقعیت این است که ممنوعیت موضوع بند ۴ ماده ۲ منشور در زمینه توسل به‌زور فقط در مورد دولت‌ها قابل‌اعمال و استناد است، نه درباره اشخاص. درصورتی‌که اقداماتی که در مقابله با این حملات صورت می‌گیرد در چارچوب موازین دفاع مشروع و استثناءهای اصل منع توسل به زور نباشد، خود نوعی نقض حقوق بین‌الملل به شمار می‌رود. از سوی دیگر، مطابق همین موازین، دفاع مشروع تنها زمانی میسر است که اقدامات در جهت دفاع از حملات دولت متجاوز صورت گرفته و حملات به‌طور قطعی به آن منتسب باشد نه به اشخاص خصوصی یا هر نهاد دیگر که احیاناً دست به حملات سایبری زده باشد. بدیهی است احراز دفاع مشروع و یا اقدام مقابله به‌مثل یا هر استراتژی حقوقی دیگر در این زمینه منوط به تحلیل و تبیین صحیح حملات سایبری به‌مثابه نقض اصول توسل به‌زور و شناسایی اصول حاکم بر این حملات در چارچوب حقوق جنگ خواهد بود؛ در غیر این صورت هرگونه اقدام تلافی‌جویانه خود می‌تواند موجبی برای طرح مسئولیت بین‌المللی دولت مرتکب باشد. به‌هر روی حملات سایبری اگر مصداقی از تجاوز یا توسل به‌زور محسوب نشوند، می‌تواند به‌عنوان مداخله در امور داخلی دولت، یک تخلف بین‌المللی تلقی شود. در صورت انتساب این اقدامات به دولت، طرح مسئولیت بین‌المللی دولت امکان‌پذیر خواهد بود. درصورتی‌که این حملات توسط افراد خصوصی که در استخدام دولت یا تحت کنترل دولت باشند به دولت منتسب می‌شود. اعمال «نظریه تقصیر» در حملات

سایبری موجب می‌شود تا با شناسایی «مقصر» حمله سایبری، «مرتکب» حملـه سـایبری نیز شناسایی شود. پس در این صورت امکان جبران خسارت به روش‌های مختلـف اعم از توقف عمل متخلفانه، پرداخت غرامت و جلب رضایت وجـود خواهـد داشت.

رجوع به دادگاه بین‌المللی. کشور مسؤول حمله‌ی سایبری را می‌توان جهت جبران غرامت ناشی از نقض ماده‌ی ۲(۴) منشور ملل متحد و اصل عدم مداخله، به یک دادگاه بین‌المللی از جمله دیوان بین‌المللی دادگستری، احضار نمود. با این وجود باید توجه داشت که تعیین میزان خسارات ناشی از یک حمله‌ی سایبری، امری دشوار است؛ زیرا مؤسسات مالی ممکن است در تهیه‌ی اطلاعات دقیق و تعیین میزان خسارات مردد باشند؛ همچنین دیوان بین‌المللی دادگستری مانند سایر دادگاه‌های بین‌المللی، فاقد صلاحیت اجباری است؛ بنابراین، هر دو طرف اختلاف باید در خصوص ارجاع قضیه به دیوان توافق نمایند.

وفق ماده‌ی ۹۶ منشور ملل متحد، گزینه‌ی دیگر می‌تواند درخواست نظریه‌ی مشورتی از دیوان بین‌المللی دادگستری در خصوص مشروعیت یا عدم مشروعیت حملات سایبری باشد. چنین نظریاتی اختیاری و غیرالزام‌آورند؛ هرچند در شکل‌گیری یک قاعده‌ی عرفی بین‌المللی مؤثر می‌باشند (Conforti, 2005).

۹ مقابله به مثل و اقدام متقابل

کشور قربانی یک حمله‌ی سایبری می‌تواند به مقابله به مثل و اقدامات متقابل غیر نظامی علیه حمله‌کننده متوسل شود. بر اساس ماده‌ی ۴۹(۱) طرح مسئولیت بین‌المللی دولت، دولت صدمه‌دیده می‌تواند علیه دولت مسئول تخلف بین‌المللی، برای وادار ساختن دولت مذکور به ایفای تعهدات خود، به اقدامات متقابل مبادرت ورزد (حلمی،۱۳۸۷). حملات سایبری و تبلیغات سایبری با هدف ایجاد شورش و منازعه‌ی داخلی در کشور هدف، امری غیرقانونی بوده و با اصول ممنوعیت توسل به زور و ممنوعیت مداخله در امور داخلی سایر کشورها مغایر است؛ این‌گونه مداخلات کشور صدمه دیده را قادر می‌سازد اقدامات متقابل متناسب و سازگاری با حدود و شرایط مذکور در مواد ۵۰ تا ۵۲ طرح مسئولیت بین‌المللی دولت اتخاذ نماید.

پرسشی که در این راستا مطرح می‌شود، این است که آیا کشور قربانی یک حمله‌ی سایبری می‌تواند به اقدام متقابل مبتنی بر توسل به زور علیه حمله‌کننده مبادرت ورزد؟

پاسخ مثبت به این پرسش در صورتی است که در ماده‌ی ۵۱ منشور یا حقوق بین‌الملل عرفی، توسل به دفاع مشروع در مقابل حمله‌ی سایبری امری مجاز باشد. در نتیجه‌ی ماده‌ی ۵۰(۱) طرح مسئولیت بین‌المللی دولت ممنوع باشد، کشور قربانی حمله‌ی سایبری نمی‌تواند واکنش نشان دهد؛ مگر آنکه حمله‌ی سایبری شدید بوده و آثار گسترده‌ای داشته باشد؛ در این صورت به استناد ماده‌ی ۵۱ منشور ملل متحد، کشور مذکور محق به واکنش می‌باشد. وضعیتی که مدنظر کمیسیون حقوق بین‌الملل از تصویب ماده‌ی ۵۰ طرح مسئولیت بین‌المللی دولت بوده، ناظر بر کشوری است که در برابر نقض پیشین مثلاً یک معاهده‌ی بازرگانی توسط کشور دیگر، به زور مسلحانه متوسل گردد بر اساس ماده ۵۰(۱) طرح مذکور، چنین اقدام متقابلی که تناسبی با اقدام اولیه ندارد، منع شده است.

۱.۹ توسل به زور مسلحانه به استناد دفاع مشروع

پرسش این است که حمله‌ی سایبری از کدام ویژگی‌ها، گستردگی و پیامدها باید برخوردار باشد تا بتوان علیه آن به زور مسلحانه متوسل شد؟ پاسخ این پرسش در ادامه خواهد آمد.

شرایط تلقی حمله‌ی سایبری معادل حمله‌ی مسلحانه: ماده‌ی ۵۱ منشور ملل متحد مقرر می‌کند: در صورت وقوع حمله ی مسلحانه علیه یک عضو ملل متحد تا زمانی که شورای امنیت اقدامات لازم برای حفظ صلح و امنیت بین‌المللی را به عمل آورد، هیچ یک از مقررات این منشور به حق ذاتی دفاع از خود اعم از فردی یا دسته‌جمعی لطمه‌ای نخواهد رسانید؛ کشور قربانی توسل به زور سایبری در صورت تلقی چنین حمله‌ای به‌عنوان یک حمله‌ی مسلحانه، می‌تواند به دفاع مشروع متوسل شود.

پرسش مهم این است که آیا یک حمله‌ی سایبری به شبکه‌ی رایانه‌ای یک زیرساخت غیرنظامی می‌تواند در صورت دارا بودن معیار مقیاس و تحقق نتیجه، به‌نحو بالقوه یک حمله‌ی مسلحانه تلقی شود؟

در صورتی که به زیرساخت‌های مهم حمله شود و چنین حمله‌ای با تلفات و خسارات گسترده همراه باشد، پاسخ مثبت است؛ اما در خصوص اینکه زیرساخت‌های مهم کدامند، توافقی وجود ندارد. مجمع عمومی سازمان ملل متحد اعلام نموده است که هر کشور باید زیرساخت‌های مهم اطلاعاتی را خود تعیین نماید (A/RES/58/199 of 23 December2003).

۲.۹ امنیت سایبری؛ ظرفیت‌های حقوق بین‌الملل

از نمونه‌های جدید و مهم تهدیدهای سایبری، می‌توان به حمله جاسوسی Solarwinds در سال ۲۰۲۰ اشاره کرد، که سازمان‌ها و شرکت‌های آمریکایی و ایمیل مقامات وزارت امنیت آمریکا مورد حملات گسترده قرار گرفتند. دامنه این حمله‌ها که ادعا می‌شد توسط هکرهای روسی صورت گرفته، آنچنان گسترده بود که مؤسسه ملی بهداشت، پنتاگون، وزارت انرژی و همچنین مشتریان کمیسیون بورس اوراق بهادار نیز در فهرست آسیب‌دیدگان این حمله قرار گرفتند. تهدیداتی نیز که در سایه همه‌گیری کووید-۱۹ پیش آمد، به‌ویژه در نشست‌های غیررسمی شورای امنیت (Arria Formula) مورد بحث قرار گرفت و بر ثبات سایبری، پیشگیری از درگیری و ظرفیت‌سازی تأکید شد. از آنجا که تهدیدهای امنیت سایبری هر روزه، رواج، پیچیدگی و شدت بیشتری می یابند، دولت‌ها و جامعه فنی و صنعتی بر تقویت امنیت سایبری تمرکز کرده‌اند. درواقع، امنیت و ثبات فضای سایبری، سنگ بنای بحث در مورد فضای سایبری، حاکمیت اینترنت و آزادی اینترنت قرار گرفته است.

نگرانی جامعه بین‌المللی در این زمینه، موجب شد از سالهای ۱۹۹۸ مجمع عمومی ملل متحد آغاز به تصویب قطعنامه‌های سالانه نماید و تأکید کند که فناوری اطلاعات بالقوه می‌تواند برای مقاصدی مغایر حفظ ثبات و امنیت بین‌المللی به کار گرفته شود.

مجمع عمومی در قطعنامه ۳۲/۵۸ از دبیر کل درخواست کرد تا گروهی متشکل از کارشناسان دولتی را برای پیشبرد رفتار مسئولانه دولت‌ها در فضای سایبری در چارچوب امنیت بین‌المللی تشکیل دهد. این کار گروه که متشکل از ۲۵ عضو بود، از زمان آغاز به کار در سال ۲۰۰۴ تاکنون ۶ کارگروه تشکیل داده

است و آخرین کارگروه، کار خود را در ماه مه ۲۰۲۱ با تصویب یک گزارش به اتفاق آراء به پایان رسانید. در دوره‌های پیشین، مهم‌ترین دستاورد گروه کارشناسان دولتی، پذیرش کاربرد حقوق بین‌الملل در فضای سایبری (۲۰۱۳) و معرفی هنجارهای غیرالزام آور داوطلبانه رفتار مسئولانه دولت در سال ۲۰۱۵ بوده است. مذاکرات دور ۲۰۱۶-۲۰۱۷ این کارگروه به علت اختلاف نظر کارشناسان در مورد مسائل مربوط به کاربرد حقوق بین‌الملل به‌ویژه حقوق بشردوستانه، اقدامات متقابل و دفاع مشروع سایبری با شکست مواجه شد و نتیجه‌ای در پی نداشت.

به دنبال افزایش تنش‌ها میان قدرت‌های سایبری و شکست گروه کارشناسان دولتی در دور پیشین، مجمع عمومی در سال ۲۰۱۸ قطعنامه‌ای با حمایت روسیه مبنی بر ایجاد کارگروه بازبررسی تحولات در زمینه ارتباطات و اطلاعات در چارچوب امنیت بین‌المللی (OEWG) به تصویب رساند. تأسیس این کارگروه به انشعاب تلاش‌های سازمان ملل در این زمینه منجر شد و کارگروه باز به موازات گروه کارشناسان دولتی موظف شد موضوعات اساسی را که گروه کارشناسان در مورد آنها به اجماع رسیده‌اند، به بحث گذارد. نخستین گزارش این کارگروه به اتفاق آراء کشورهای شرکت‌کننده در مارس ۲۰۲۱ تصویب شد، که به‌دلیل مشارکت مستقیم دولت‌ها در تصویب آن می‌تواند از جایگاه مهم‌تری نسبت به سایر گزارش‌ها و اقدامات در این زمینه برخوردار باشد.

این گزارش، فراوانی، پیچیدگی و تنوع رویدادهای خرابکارانه فناوری اطلاعات و ارتباطات و همین‌طور افزایش احتمال استفاده از ابزارهای سایبری در مخاصمات آینده توسط تروریست‌ها و گروه‌های تبهکار و آثار بالقوه ویرانگر آنها را از جمله افزایش تعداد حملات سایبری خصمانه که خدمات عمومی ضروری مثل امکانات پزشکی، خدمات مالی، انرژی، آب، حمل و نقل و بهداشت را به مخاطره می‌اندازند، شناسایی کرده است. موضوع دومی که در این گزارش بدان پرداخته شده، هنجارها و اصول است و بر ارتباط و محدودیت‌های هنجارهای غیرالزام‌آور داوطلبانه برای صلح، امنیت و ثبات بین‌المللی تأکیده شده است. همچنین بر وظایف دولت‌ها برای جلوگیری از گسترش ابزارهای مخرب و بر لزوم گزارش‌دهی آسیب‌پذیری‌ها تأکید می‌کند. در این گزارش مشارکت فعال و مستمر دولت‌ها در گفتگوهای سازمانی منظم تحت نظارت سازمان ملل نیز مورد تأکید قرار گرفته است.

۱۰ الزامات حقوقی دفاع مشروع علیه حمله‌ی سایبری

به هنگام توسل به دفاع مشروع علیه یک حمله‌ی سایبری که در حد حمله‌ی مسلحانه باشد باید الزامات «ضرورت»، «تناسب» و «فوریت» رعایت شود (Din stein, 2005).

ضرورت بدین معنی است که توسل به زور آخرین گزینه و راهکار است؛ لذا باید سایر راهکارها ناکارآمد بوده یا احتمالاً ناکارا و بی‌فایده باشند. به‌عنوان یک الزام و شرط حداقلی، ضرورت بر این دلالت دارد که کشوری که درصدد دفاع مشروع است، باید دریابد که حمله‌ی سایبری یک تصادف نبوده و موضوع را نمی‌توان با توسل به روش‌های کمتر قهرآمیز حل و فصل نمود؛ روش‌هایی چون جلوگیری از دسترسی نفوذگران سایبری به شبکه‌ها و وب‌سایت‌های هدف حمله از طریق توسل به دفاع سایبری. در خصوص الزام تناسب باید گفت که

در عمل، واکنش یکسانی به حمله‌ی سایبری امکان‌پذیر نمی‌باشد. چرا که گاهی کشور قربانی فاقد فناوری توسل به حمله‌ی سایبری بوده و یا متجاوز فاقد یک شبکه‌ی به حد کافی توسعه‌یافته برای حمله به آن است (Greenberg, 1998).

سرانجام اینکه، الزام فوریت بیانگر آن است که هدف غایی دفاع مشروع تنبیه مهاجم نمی‌باشد، بلکه هدف، دفع حمله‌ی مسلحانه است. چنین الزامی به‌ویژه در خصوص حملات سایبری باید به نحو انعطاف‌پذیری به کار رود؛ چرا که برای مثال، در فرض استفاده‌ی متجاوز از «بمب های هوشمند یا زمانی» خسارات واقعی مدت‌ها پس از حمله‌ی سایبری ایجاد خواهد شد؛ امری که واکنش در قالب دفاع مشروع را با تأخیر مواجه می‌سازد.

۱۱ عملیات سایبری و حمله مسلحانه در معنای ماده ۵۱ منشور سازمان ملل متحد

تهدیدهای سایبری که شاید بتوان گفت برای اولین بار در سال ۱۸۳۴ با هک سیستم تلگراف فرانسه و ربودن اطلاعات مالی بانکی آغاز شد به چنان قدرت انهدام و ویران‌گری رسیده است که امروزه دولت‌ها از امکان تلقی برخی عملیات سایبری به‌عنوان حمله مسلحانه در مفهوم ماده ۵۱ منشور ملل متحد و توسل به دفاع مشروع فردی یا حتی جمعی در مواجه با آن، سخن می‌گویند.

در مواجهه با این تهدیدها، رویکرد اصلی حقوق بین‌الملل آن است که هر قاعده در دنیای واقعی قابل سرایت و اعمال است بر فضای مجازی؛ (برای نمونه نک به بند ۶۹ آخرین گزارش گروه کارشناسان دولتی در مورد رفتار مسؤولانه در فضای مجازی، بند ۷ آخرین گزارش گروه کاری نامحدود و قطعنامه شورای حقوق بشر در مورد اینترنت) ـ گویی که فضای مجازی همان آرایه ادبی است به کنایه از دنیای واقعی ما. از این منظر، حمله مسلحانه قلمداد کردن عملیات سایبری ممکن بوده و در نتیجه علاوه بر موضع بسیاری از دولت‌ها، بسیاری از صاحب‌نظران حقوقی از جمله کارشناسان مورد مشورت در دستورالعمل تالین ۲ نیز بر این نظر هستند که «دولت قربانی عملیات سایبری که به سطح حمله مسلحانه رسیده باشد، می‌تواند به حق دفاع مشروع ذاتی خود متوسل شود» (تأکید اضافه شده است، قاعده ۷۱). این کارشناسان، عملیات سایبری را هنگامی حمله مسلحانه قلمداد می کنند که «گستره و تأثیر» آن مشابه آستانه‌ای باشد که برای تلقی توسل به زور به حمله مسلحانه در دنیای واقعی اعمال می‌شود و در نتیجه بر این نظر هستند که چنانچه عملیات سایبری منجر به «صدمات جدی یا مرگ تعدادی یا ایراد خسارت یا نابودی اموال» شود، یعنی آثار فیزیکی همانند یک حمله مسلحانه به بار آورد، می‌تواند به‌عنوان حمله مسلحانه در مفهوم ماده ۵۱ منشور تلقی گردد (بند ۸، قاعده ۷۱).

این کارشناسان دو مبنای عمده برای چنین نتیجه‌گیری عنوان می‌کنند: نخست، نظر دیوان بین‌المللی دادگستری در مورد قابل اعمال بودن ممنوعیت توسل به زور و همچنین ماده ۵۱ منشور بر هر نوع «سلاح» (بند ۳۹ نظریه مشورتی دیوان در مورد سلاح های هسته‌ای)؛ و دوم وجود اجماع بر آنکه حمله‌های غیرکینتیک (یا غیرجنبشی) به مانند شیمیایی یا بیولوژیک در صورت ایراد آثاری مشابه با حمله‌های کینتیک می‌تواند در

گستره مفهوم حمله مسلحانه مندرج در منشور قرار گیرد (بند ۴ قاعده ۷۱).

با وجود مشابهت عملکرد عملیات سایبری با یک حمله شیمیایی از لحاظ غیرکینتیک بودن، در این واقعیت تردیدی نیست که در مورد اول ما با یک برنامه کامپیوتری مواجه هستیم که جز در فضای رایانه‌ای وجود ندارد و جز به کمک رایانه اثر نخواهد کرد و در مورد دوم با یک عنصر شیمیایی موجود در عالم واقع. به دیگر سخن، تأثیر یک عملیات سایبری به خودی خود و مستقیم نیست بلکه به دلیل تأثیری است که بر عملکرد کامپیوتر و شبکه‌ها و افزاره‌های متصل به آن گذاشته و در نتیجه عملکرد نادرست سیستم‌های کامپیوتری، ممکن است خسارتی به اموال یا لطمه‌ای به افراد وارد شود. دقیقاً به دلیل همین تفکیک است که اخیرا، اشمیت و بیلر در مقاله‌ای در مورد ابزار یا روش جنگی بودن عملیات سایبری، می‌نویسند از آنجا که در هیچ سلاح دیگری این مرحله میانی وجود ندارد که از خود هدف خواسته شود که زیان مورد نظر را پدید آورد، عملیات سایبری که متشکل است از مجموعه کدهایی که دستور اقدامات زیان‌آور را به یک سیستم رایانه‌ای می‌دهد، نمی‌تواند در مفهوم «سلاح» یا «ابزار» جنگی قرار گیرد بلکه توصیف درست از آن، در ذیل «روش جنگی» است. با توجه به اینکه اشمیت خود بانی و موتور اصلی دستورالعمل‌های تالین است، بعید نیست در دستورالعمل تالین ۳ که شروع آن کلید خورده است، تغییراتی در تقسیم‌بندی عملیات سایبری به سلاح و روش جنگی صورت گیرد (قاعده ۱۰۳ دستورالعمل تالین ۲ در حال حاضر ابزارهای سایبری را سلاح سایبری و سیستم‌های متصل به آن و روش‌های سایبری را تاکتیک، تکنیک و آیین‌های سایبری هدایت مخاصمات می‌خواند). با آنکه مقاله اشاره شده در بالا در مقام بیان تبیین یک قاعده از هدایت مخاصمات در حقوق بشردوستانه است (و خود تأکید می‌کند که چنین تفکیکی تأثیری در اجرای قواعد حقوق بشردوستانه ندارد)، چنین روشنگری نمی‌تواند بدون تأثیر در حوزه های دیگر حقوق و به‌خصوص حقوق توسل به زور باشد. برای نمونه، اگر عملیات سایبری در هر شکل و ابعاد به مانند توسل به حیله که صرفاً یک روش جنگی است، به‌طور طبیعی نمی‌تواند در مفهوم «سلاح» قرار گیرد و در نتیجه، از نظر موضوعی از دامنه شمول نظریه مشورتی دیوان در مورد سلاح‌های هسته‌ای در مورد قابل اعمال بودن ماده ۲ و ۵۱ منشور بر هر «سلاحی» خارج می‌شود.

در زمان تدوین دستورالعمل تالین ۲، این بحث مطرح شد که آیا استفاده از «سلاح» برای تحقق حمله مسلحانه ضروری است یا خیر. پیش از ادامه این بحث، اشاره به این مطلب ضروری است که در دستورالعمل تالین ۲، کارشناسان بر تفاوت میان «تجاوز» و «حمله مسلحانه» اذعان داشته و هر «تجاوزی» را لزوماً مساوی با «حمله مسلحانه» نمی‌دانند (بند ۲ قاعده ۷۱)، که خود تأییدی است بر تفکیک میان «تجاوز مسلحانه» یا همان حمله مسلحانه با سایر اشکال «تجاوز». با این حال، در بحث ضرورت استفاده از سلاح، نظر اکثر کارشناسان بر این بود که لازم نیست حمله مسلحانه با استفاده از سلاح باشد ـ امری که با تعریف تجاوز مسلحانه می‌تواند در مغایرت باشد – اما این نظر را نیز رد نکردند که واژه «مسلحانه» بودن صرفاً بر استفاده از سلاح اطلاق می‌شود و در نتیجه جز عملیات سایبری که با استفاده از سلاح سایبری در مفهوم قاعده ۱۰۳ انجام گیرد، سایر عملیات‌های سایبری صرف نظر از گستره و آثار نمی‌تواند به‌عنوان حمله مسلحانه در مفهوم ماده ۵۱ منشور در نظر گرفته شود.» (بند ۵ قاعده ۷۱). با این توصیف، اگر طبقه‌بندی اشمیت در مورد روش جنگی بودن عملیات سایبری پذیرفته شود، این دو دیدگاه قطعاً غیر قابل جمع خواهند شد، یعنی یا بایستی

قائل به تعمیم حمله مسلحانه به عملیات سایبری به صرف آثار بود و یا با توجه به اینکه عملیات سایبری صرفاً مجموعه‌ای از دستورهای کامپیوتری است و در نتیجه هیچ اقدام مسلحانه‌ای در عالم واقع صورت نگرفته است، در صورت وجود سایر شرایط آن را صرفاً مشمول مداخله، توسل به زور و یا حتی تجاوز دانست و نه حمله مسلحانه.

چنانچه قایل به نظر اول شویم، یعنی تنها آثار را به عنوان معیار حمله مسلحانه بودن عملیات سایبری در نظر بگیریم، آیا این امر منجر نمی‌شود که بتوان سایر روش‌هایی را نیز که منجر به مرگ و آسیب گسترده می‌شوند، برای نمونه تحریم‌های اقتصادی یک‌جانبه، در مفهوم حمله مسلحانه ماده ۵۱ قرار گیرد؟ مقایسه عملیات سایبری با تحریم‌ها از این جهت جالب توجه می‌نماید که آثار تحریم، به‌خصوص خسارات و لطمات معمولاً فوری نبوده، بلکه در طولانی‌مدت رخ دهد. این تأثیر مشابه همان اتفاقی بود که در مورد ویروس استاکس‌نت روی داد؛ با وجود اینکه کدهای دستوری مختلف مدت‌های مدیدی بود که در سیستم‌های رایانه‌ای وارد شده بودند (گفته می‌شود حدود چهار سال)، اما امکان تلقی آن به‌عنوان «حمله مسلحانه» تنها زمانی در نظر گرفته شد که خسارات گسترده‌تر وارد شده بود (ذکر این مطالب ضروری است که تاکنون نه استاکس‌نت و نه هیچ عملیات سایبری دیگر به‌عنوان حمله مسلحانه مورد شناسایی دولت‌ها قرار نگرفته و حتی در مورد استاکس نت، کارشناسان تالین در مورد حمله مسلحانه قلمداد کردن آن تردید داشتند، با وجود آنکه همه موافق بودند که این عملیات توسل به زور بوده است. (بند ۱۰، قاعده ۷۲)). حال، چرا بایستی تفاوتی بین کدهای دستوری زیان‌بار و وضع قوانین تحریمی زیان‌بار قائل شد زمانی که ـ همان‌طور که همه تجربه کرده‌ایم ـ هر دو موجب مرگ و آسیب می‌شوند؟ در این خصوص، توجه به این مسأله مهم است که با وجود اینکه از موارد تجاوز مندرج در اساسنامه دیوان بین‌المللی کیفری، توسل به روش «محاصره بنادر و سواحل توسط نیروهای مسلح دولت دیگر» (بند ج ماده ۸ مکرر اساسنامه دیوان بین‌المللی کیفری) است که در معنای سنتی، جنگی است اقتصادی برای ممانعت از ورود کالا و افراد به قلمروی کشور دشمن (تفسیر جنایت تجاوز، ص. ۴۴۳) اما آنچه این روش را تبدیل به تجاوز می‌کند، حضور نیروهای مسلح دولت محاصره‌کننده است که می‌توانند عملاً مانع ورود و خروج کالا و خدمات شوند (همان، ص. ۴۴۴) و نه صرف تحریم.

رویه دیوان بین‌المللی دادگستری در تبیین تفاوت میان توسل به زور و حمله مسلحانه به صرف اشاره به گستره و آثار نبایستی توجه را از این مطلب دور کند که در هر سه پرونده فعالیت‌های نظامی و شبه نظامی در نیکاراگوئه، سکوهای نفتی و فعالیت های مسلحانه در کنگو، تردید یا حتی بحثی در مسلحانه بودن اقدامات انجام شده در مفهوم عادی و کلاسیک و واقعی آن نبود؛ بلکه محل تردید، تعیین آستانه یا مصادیق حمله مسلحانه در توجیه اقدامات نظامی متقابل در قالب دفاع مشروع بود. از این دیدگاه، صرف در نظر گرفتن معیار گستره و آثار بدون بستر آن، که همان عملیات نظامی مشروحه در هر پرونده‌ای بود، به‌مثابه حکایت نادان خواندن فیل در شعر مولاناست (دکتر کتایون حسین نژاد، ۱۴۰۱).

با وجود آنکه عملیات سایبری می‌تواند آثار بسیار مخربی داشته باشد، اما، همگام با صاحب‌نظرانی که ماده ۵۱ منشور سازمان ملل متحد را استثنایی نه بر منع توسل به زور بلکه بر اقدامات جمعی سازمان ملل متحد ذیل فصل هفتم منشور و تحت لوای شورای امنیت و محدود به موارد تجاوز مسلحانه‌ای می‌دانند که اقتضای

اقدام فوری پیش از اتخاذ تدابیر ضروری توسط شورای امنیت تامین صلح و امنیت را دارد. به دلیل ماهیت مجازی، چنین عملیاتی نمی‌تواند در مفهوم حمله مسلحانه قرار گیرد. این ایده، منصرف از این استدلال است که حتی اگر عملیات سایبری را حمله مسلحانه بدانیم، متناسب‌ترین دفاع در برابر آن به احتمال قوی مقابله مجازی با آن و نه استفاده از بمب و موشک است.

۱۲ تأثیر و شدت حملات سایبری

حملات سایبری می‌تواند از بسیاری جهات بر سازمان‌ها تأثیر بگذارد، از اختلالات جزئی در عملیات گرفته تا خسارات عمده مالی. صرف نظر از نوع حمله سایبری، هر نتیجه‌ای نوعی هزینه دارد، چه پولی و چه غیر پولی. پیامدهای حملات سایبری ممکن است هفته‌ها و یا ماه‌ها بعد بر روی کسب‌وکارها تأثیر بگذارد. در ادامه پنج منطقه‌ای که ممکن است آسیب ببیند آورده شده است:

- خسارات مالی
- از دست دادن بهره‌وری
- خسارت به اعتبار
- مشکلات مداوم تجاری
- بدهی‌های قانونی

حملات باج‌افزار به‌عنوان یک نگرانی بزرگ شیوع بیشتری پیدا کرده است. در پایان سال ۲۰۱۶ هر ۴۰ ثانیه یک تجارت قربانی حمله باج‌افزار می شد. بر اساس گزارشی از Cybersecurity Ventures انتظار می‌رود این میزان تا امسال هر ۱۱ ثانیه افزایش یابد. این حمله سایبری زمانی اتفاق می‌افتد که از نرم‌افزار مخربی برای محدود کردن دسترسی به سیستم رایانه‌ای یا داده‌ها استفاده شود، تا زمانی که قربانی، باج خواسته شده توسط مجرم را پرداخت کند.

از زمانی که افراد از سیستم‌های تجاری آسیب‌پذیر بهره‌مند می‌شوند، جرائم سایبری افزایش یافته است. غالباً مهاجمان به دنبال باج گرفتن هستند: ۵۳ درصد از حملات سایبری منجر به خسارت ۵۰۰،۰۰۰ دلاری یا بیشتر شده است.

اهداف حملات سایبری: ایجاد اختلال در یک سرور، به‌کار گرفتن کامپیوتر افراد به‌عنوان سپر، دسترسی به اطلاعات یک سیستم کامپیوتری، ورود به اتصالات اینترنتی که پهنای باند زیادی دارند، مطالعه و زیر نظر گرفتن یک سازمان به‌صورت غیر مجاز، دسترسی و سرقت اطلاعاتی که در یک کامپیوتر نگهداری می‌شود.

۱۳ دفاع مشروع علیه حمله‌ی سایبری از منظر حقوق بین‌الملل عرفی

همان‌گونه که آورده شد، به‌موجب ماده‌ی ۵۱ منشور ملل متحد، می‌توان به دفاع مشروع علیه حمله‌ی سایبری متوسل شد. پرسش این است که آیا قاعده‌ی عرفی در این خصوص وجود دارد؟ در قضیه‌ی نیکاراگوئه، دیوان بین‌المللی دادگستری دریافت که هویت کاملاً مجزایی میان قواعد عرفی بین‌المللی توسل به زور و مقررات ناظر بر آن در منشور ملل متحد وجود ندارد و حقوق بین‌الملل عرفی صرف نظر از حقوق بین‌الملل معاهدات به وجود و کارکرد خود ادامه می‌دهد؛ حتی اگر هر دو نظام حقوقی محتوای یکسانی داشته باشند (Nicaragua case, 1986).

ایالات متحده آمریکا، در خصوص حق دفاع مشروع در تقابل با حملات سایبری، مواضعی را اتخاذ نموده است. بر اساس ارزیابی وزارت دفاع این کشور، کشور حامی حملات سایبری، حق توسل به دفاع مشروع را برای طرف مقابل ایجاد می‌کند.از منظر این وزارتخانه ، هرگاه یک حمله‌ی شبکه‌ای رایانه‌ای هماهنگ، سیستم کنترل ترافیک هوایی یک کشور و یا سیستم‌های بانکداری و مالی آن را مختل کند، دریچه‌ی چندین سد را باز کند و در نتیجه سیل جاری شود و هر یک از این اقدامات تلفات گسترده غیرنظامیان و یا خسارات مادی را در پی داشته باشد، کشور اخیر، قربانی و هدف یک حمله‌ی مسلحانه یا عملی برابر با یک حمله‌ی مسلحانه واقع شده است (www.au.af.mil).

رویه‌ی سازمان‌های بین‌المللی مربوطه، شکل دیگری از رویه‌ی کشورها است که در ارزیابی وجود یک قاعده‌ی حقوق بین‌الملل عرفی باید مورد توجه قرار گیرد (انجمن حقوق بین‌الملل، ۱۳۸۴).

حقوق بین‌الملل عرفی نیز با توجه به وجود نسبی رویه‌ی کشورها و اعتقاد حقوقی، به‌ویژه در خصوص حق دفاع مشروع علیه حملات سایبری، می‌تواند نقشی را در این زمینه ایفاء نماید. این فرایند ادامه دارد و می‌تواند به شکل‌گیری یک قاعده‌ی عرفی در سال‌های پیش رو منجر گردد. ضمن آنکه همکاری‌های بین‌المللی در سطوح منطقه‌ای و جهانی می‌تواند در مقابله با حملات سایبری که پدیده‌ای بدون مرز است، نقش مؤثری ایفاء نماید. در این راستا ضرورت انعقاد معاهده‌های خاص در مورد ممنوعیت حملات سایبری بیش از پیش احساس می‌شود.

۱۴ آزادی اطلاعات در فضای سایبر از منظر حقوق بین‌الملل

در فرهنگ سیاسی و فلسفی کمتر واژه‌ای به اندازه «آزادی» به بازی گرفته شده است. در حالی که عده‌ای آزادی را به مفهوم رهایی از هر گونه قید و بند دانسته‌اند، جمعی دیگر آن را اطاعت از عقل و اقدام به قانون معنی کرده‌اند. گویی رمز این همه اختلاف و ابهام در خود واژه آزادی نیز نهفته باشد. امروزه آزادی بیان به‌صورت گسترده یکی از حقوق بشر تلقی می‌شود؛ بدین معنی که انسان‌ها «به‌خاطر انسان بودنشان» حق آزادی بیان دارند. در کنار پذیرش عمومی مفهوم آزادی بیان، از طرف دیگر توافقی عمومی نیز وجود دارد که باید برای آزادی بیان حد و مرز مشخص کرد؛ دیگر فضای سایبر یک فضای تک‌بعدی وب‌سایتی نیست . امروز

مخاطب بدون اینکه احساس کند در میان چندین وجه از اشکال سایبر است. می‌توان فضای سایبر را به‌مثابه دریاچه‌ای در نظر گرفت که ابعاد گوناگون آن مانند جزایر کوچک و بزرگی هستند که شناگران در این فضا هر از چند گاهی به یکی از این جزایر سر می‌زنند. امروزه دیگر فعالیت در یک عرصه از فضای سایبر نمی‌تواند یک فعالیت اثرگذار و جامع باشد، بلکه بسیاری از مراکز مهم و تأثیرگذار در تمام ابعاد این فضا با محتواهای مختلف در موضوعات مشترک فعال هستند.

۱.۱۴ مزیت‌ها و محدودیت‌های فضای سایبر برای آزادی بیان

پیش از وارد شدن به بحث‌های خاصی که فضای سایبر در مورد اصل آزادی بیان به‌وجود آورده لازم است مفهوم آن در حدی که مورد توجه اسناد بین‌المللی حقوق بشری بوده، تبیین شود. بر این پایه، اعلامیه جهانی حقوق بشر (۱۹۴۸) در ماده ۱۹ خود مقرر می‌دارد: «هرکس حق آزادی عقیده و بیان دارد و این حق مستلزم آن است که از داشتن عقیده بیم نداشته باشد و در دریافت و انتشار اطلاعات و افکار، به تمام وسایل ممکن بدون ملاحظات آزاد باشد بی‌گمان این ماده همانند دیگر مفاد این سند به شکل کلی تنظیم شده و استیفاء این حقوق ایجاب می‌کرد که این مفاهیم دقیق‌تر و شفاف‌تر تعریف شده و حدود و ثغور آنها مشخص شود. از این رو در سال ۱۹۷۶ میثاق بین‌المللی حقوق مدنی و سیاسی به‌تصویب دولت‌های عضو سازمان ملل رسید. در این سند دو ماده ۱۸ و ۱۹ به تبیین این موضوع پرداخته‌اند. ماده ۱۸ حق آزادی تفکر آگاهی و دین را به رسمیت می‌شناسد که آزادی عقیده موضوع ماده ۱۹ را نیز دربر می‌گیرد. تأکید اصلی این ماده، محترم شمردن آزادی تفکر درباره همه موضوع‌های مربوط به ایمان شخصی و تعهد به دین یا اعتقاد خاص است و آن‌گونه که در بند ۲ ماده ۴ میثاق آمده، حتی در شرایط خاص و اضطراری هم نباید آن را خوار شمرد و تحقیر کرد. البته این ماده میان آزادی تفکر آگاهی و دین یا عقیده و آزادی ابراز آنها تفکیک قائل شده است. گروه نخست تحت حمایت مطلق هستند تا اندازه‌ای که طبق ماده ۱۷ و بند ۲ ماده ۱۸ هیچ‌کس را نمی‌توان مجبور کرد تا افکار خود را آشکار کند یا به دین یا عقیده خاصی بگرود. ولی، بر گروه دوم محدودیت‌هایی اعمال شده که در جای خود به آنها اشاره خواهد شد.

ماده ۱۹ با عنوان آزادی عقیده حق داشتن اعتقاد بدون مداخله را با هیچ استثناء یا محدودیتی به رسمیت می‌شناسد (بند ۱). در اینجا نیز میان اصل این حق و آزادی ابراز آن تفکیک صورت گرفته و در بند ۲ میثاق آمده حتی در شرایط خاص و اضطراری هم نباید آن را خوار شمرد و تحقیر کرد. البته این ماده میان آزادی، تفکر، آگاهی و دین یا عقیده و آزادی ابراز آنها تفکیک قائل شده است.

۱۵ نتیجه‌گیری

با پیشرفت فناوری، فضای سایبری به‌عنوان فضای پنجم در حقوق بین‌الملل دیر زمانی نیست پا به عرصه ظهور گذاشته است. مثل اکثر پیشرفت‌هایی که فناوری به همراه داشته است در این باره هم از این فضا برای اعمال خرابکارانه استفاده شده است. ماهیت غیرملموس فضای سایبری و تهدیداتی که این فضا برای امنیت وحاکمیت دولت‌ها دارد و ویژگی‌هایی که حملات سایبری دارد، تدوین و تطبیق قوانین بین‌المللی بر

این نوع فعالیت‌های سایبری را ایجاب می‌کند. با توجه به عناصری که برای یک جنگ می‌توان برشمرد، با نگاهی به مقررات بین‌المللی، از جمله منشور ملل متحد، نظریات تفسیری دیوان بین‌المللی دادگستری در قضایای ترافعی یا مشورتی، کنوانسیون‌های چهارگانه ژنو ۱۱۸۱، پروتکل‌های الحاقی ۱۱۷۷ آن و رویه دولت‌ها، می‌توان ابزارهای به‌کار رفته در حملات سایبری را با نگاه غایت‌محور به عنوان ابزار جنگی شناسائی کرد و این نوع حملات را تحت عنوان «زور» که در منشور ملل متحد آمده است، قلمداد نمود. علاوه بر این، با به‌کار بردن معیارهای شناخت حملات سایبری می‌توان این نوع حملات را به‌عنوان ناقض اصول منع تهدید و عدم توسل به زور و اصل عدم مداخله در امور داخلی کشوها بر شمرد. با در نظرگرفتن ملاحظات ذکرشده، کشورها در هنگام مواجهه با حملات سایبری با رعایت مقررات و موازین بین‌المللی حق توسل به دفاع مشروع و اقدامات متقابل را دارا می‌باشند. با توجه به اهمیت این اصول برای جامعه بین‌المللی که به‌عنوان قواعد آمره بین‌المللی نیز شناسایی شده‌اند، ماهیت حقوقی حملات سایبری باید توسط نهادهای ذیربط همچون دیوان بین‌المللی دادگستری با ارجاع دعوای ترافعی به دیوان یا درخواست نظریه مشورتی، همچنین توسط شورای امنیت سازمان ملل متحد که طبق فصل هفتم منشور ملل متحد مسئولیت اصلی حفظ صلح و امنیت بین‌المللی را به دوش می‌کشد و به‌عنوان مرجع اصلی احراز وقوع تجاوز طبق قطعنامه تعریف تجاوز باید به این عرصه ورود پیدا کنند.

نکته حائز اهمیت دیگر در مورد مسئولیت دولتها در قبال فعالیت‌های سایبری است. در هنجار ۱۳(ج) این گزارش مقرر شده است که دولت‌ها نباید آگاهانه اجازه دهند که با استفاده از فناوری اطلاعات و ارتباطات از قلمروشان برای اعمال مغایر حقوق بین‌الملل استفاده شود.

این هنجار که به مفهوم مراقبت مقتضی (Due Diligence) معروف است، اخیراً در حوزه سایبری به‌عنوان راهکاری امیدوارکننده برای پاسخگویی دولت‌ها در قبال عملیات سایبری که از قلمرو آنها سرچشمه می‌گیرند یا از قلمروی آنها عبور می‌کند، بسیار مورد توجه قرار گرفته است.

با وجود تلاش‌ها و اقدامات برشمرده شده توسط کشورهای عضو سازمان ملل و حقوقدانان بین‌المللی در نهایت، دست‌یابی به راه حل اصلی در تنظیم مقررات سایبری دشوار به نظر می‌رسد. از سویی، دولت‌های غربی و ذی‌نفعان عرصه سایبری، بر این نظرند که حقوق بین‌الملل موجود برای تنظیم رفتار دولت‌ها در فضای سایبر کافی است و تنها باید به چگونگی عملیاتی کردن این قواعد پرداخت. اما در مقابل، برخی کشورها مانند ایران، روسیه و کوبا معتقدند در حقوق موجود شکاف‌ها و ناکارآمدی‌هایی وجود دارد که نیازمند تنظیم قواعد جدید در این زمینه از طریق تدوین یک معاهده جدید و یا تحول حقوق بین‌الملل عرفی است.

حتی در رویکرد معتقدان به ضرورت قواعد جدید نیز همسویی وجود ندارد. برخی دولت‌ها بر معاهده‌ای متمرکز هستند که از دولت‌ها در برابر مردم محافظت می‌کند و برخی دیگر به‌دنبال معاهده‌ای هستند که از مردم در برابر دولت‌ها محافظت کند.

مراجع

[۱] توحیدی، محمدرضا، «ارزیابی ماهیت حقوقی حملات سایبری با نگاهی به منشور سازمان ملل متحد»، ۱۳۹۷.

[۲] اسمعیل‌زاده ملاباشی، پرستو، عبدالهی، محسن، زمانی، سیدقاسم، «حملات سایبری و اصول حقوق بین‌الملل بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)»، فصلنامه مطالعات حقوق عمومی، دوره ۸۷، شماره ۲، صفحه ۵۸۲، تابستان ۱۳۹۶.

[۳] آهنی امینه، محمد، «حقوق بین‌الملل مدرن و جنگ سایبری در فضای مجازی»، مؤسسه انتشاراتی جهان جام جم، ۱۳۹۷، صفحات ۱۰۶-۱۱۰.

[۴] پاکزاد، بتول، «ماهیت تروریسم سایبری» مجله‌ی تحقیقات حقوقی دانشگاه شهید بهشتی، ویژه‌نامه‌ی شماره‌ی ۴، بهار ۱۳۹۰.

[۵] پاکزاد، بتول، تروریسم سایبری، رساله‌ی دکتری حقوق کیفری و جرم‌شناسی، دانشکده‌ی حقوق دانشگاه شهید بهشتی، ۱۳۸۸.

[6] Abraham M. Denmark, James Mulvenon. (2010). Contested Commons: The Future of American Power in a Multipolar World, Center for New American Security (CNAS).

[7] Hess, Charlotte. (1996). “Untangling the Web: The Internet as a Commons.” Workshop in Political Theory and Policy Analysis”, Indiana University.

[8] Schmitt, Michael N. (2013). Tallinn Manual on the International Law: Applicable to Cyber Warfare, Cambridge University Press.

[9] Robertson Jr., H.B., “Self-Defense Against Computer NetworkAttack Under International Law”, in: Schmitt/O’Donnell (eds).

[10] Computer Network Attack and International Law, 2001. Roscini, M., Threats of Armed Force and Contemporary International.

[11] Schmitt, M. (2017). Computer network attack and the use of force in international law: thoughts on a normative framework. In The Use of Force in International Law (pp. 379-431). Routledge.

[12] Shackelford, S. J. (2009). From nuclear war to net war: analogizing cyber attacks in international law. Berkeley J. Int’l Law, 27, 192.

اعمال حاکمیت بر قلمرو سایبری ملی با اتکا به حقوق بین‌الملل

سید حسین علوی[۱]، محمدرضا حسینی[۲]، مهراب رامک[۳]

[۱] دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
h.alavi@aut.ac.ir
[۲] دانشیار گروه مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
rezahsn88@gmail.com
[۳] دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
m.ramak@aut.ac.ir

چکیده

در ابتدای شکل‌گیری فضای سایبر، برخی نظریه‌پردازان بر این باور بودند، توسعه فضای سایبری و برقراری تعاملات اقتصادی، سیاسی و فرهنگی در سطح جهانی، با تعابیری از قبیل مرززدایی، سرزمین‌زدایی، قلمروزدایی و حاکمیت‌زدایی همراه خواهد بود اما هم اکنون به‌طور گسترده‌ای پذیرفته شده است که فضای سایبری یک منطقه عاری از قانون نیست که در آن هر کس بتواند با رفتار بدون ضابطه و بدون در نظر گرفتن قوانین، مقررات و قواعد پذیرفته شده بین‌المللی، هر گونه فعالیت خصمانه‌ای انجام دهد. مسئله اصلی این پژوهش این است که آیا اصول و قواعد حقوق بین‌الملل حال حاضر، با قاطعیت و شفافیت از اقدامات خصمانه سایبری که حاکمیت کشورها بر قلمرو سایبری را نقض می‌کنند، جلوگیری می کند و این اصول و قواعد قابل اتکا در صیانت از حاکمیت کشورها بر قلمرو سایبری ملی هستند؟ این نوشتار با مرور و بررسی اسناد، اصول و قواعد حقوق بین‌الملل مرتبط با حاکمیت سایبری ملی که با استفاده از روش تحلیل محتوای کیفی و ابزار نرم‌افزار مکس‌کیودا انجام پذیرفته است نتیجه می‌گیرد، اصول و قواعد حقوق بین‌الملل حال حاضر از کارایی و توانایی لازم در صیانت از حاکمیت سایبری ملی کشورها برخوردار نیست و عموماً اقدامات ناقض حاکمیت سایبری ملی با شدت متوسط و کم (اعم از: توسل به زور، مداخله غیرمجاز و ...) فاقد پیگرد قانونی هستند. از این رو این قواعد و اصول در مقابل اقدامات مخرب و ناقض حاکمیت سایبری ملی از بازدارندگی لازم برخوردار نیستند.

کلمات کلیدی: قلمرو سایبری، حاکمیت ملی سایبری، اصول و قواعد حقوق بین‌الملل.

۱ مقدمه

در ابتدای شکل‌گیری فضای سایبر، برخی نظریه‌پردازان بر این باور بودند، توسعه فضای سایبری و برقراری تعاملات اقتصادی، سیاسی و فرهنگی در سطح جهانی، با تعابیری از قبیل مرززدایی، سرزمین‌زدایی، قلمروزدایی، و دولت‌زدایی همراه خواهد بود و توسعه فناوری اطلاعات و ارتباطات که به ارتباط انسان‌ها

در اقصی نقاط کره زمین و در فضای مجازی منجر شده است به‌منزله نابودی قلمرو، مرز، حکومت و دولت خواهد بود. لیکن پس از آن مشخص شد چون فضای سایبری از هر حیث بر فضای واقعی تکیه دارد و از سوی دیگر از ماهیت ابزاری برخوردار است که به‌وسیله انسان در فضای واقعی و در راستای تأمین نیازهایش بکارگرفته و مدیریت می‌شود، تصور نابودی و زدایش این مفاهیم ممکن نیست. بر پایه این استدلال مفاهیم حاکمیت، قلمرو و مرز، ابدی و انکارناپذیر بوده و با تحولات فناورانه از قبیل توسعه فضای سایبری و فناوری‌های اطلاعاتی و ارتباطی و تجلی‌های دیجیتالی آن از بین نمی‌رود. با این تفاوت که قلمرو و مرز در فضای سایبری از ماهیت مجازی و دیجتالی برخوردار بوده و محدوده آن با شاخص‌های متفاوتی نسبت به فضای واقعی تعیین می‌گردد.

از این رو بکارگیری فضای سایبر در شئونات مختلف زیست بشری موجب گردیده است اعمال حاکمیت در فضای سایبر کشورها یکی از ابعاد جدید حاکمیت ملی و امری ضروری به شمار آید. یکی از شیوه‌های مؤثر در اعمال حاکمیت سایبری ملی، اتکا به حقوق بین‌الملل در این زمینه است و تسلط و توانایی در ارایه مستندات و دلایل حقوقی در پیگیری حقوقی و قضایی اقدامات و فعالیت‌های ناقض حاکمیت ملی در فضای سایبری در مجامع بین‌المللی، بخشی از قدرت ملی به حساب می‌آید.

به علاوه، از آنجا که فضای سایبری در امتداد فضای واقعی است، دولت‌ها می‌توانند بر مردم و اشیاء موجود در قلمرو خود اعمال قدرت کنند و فعالیت‌های آنها را تنظیم کنند. یعنی اینکه افراد، تجهیزات و داده‌های موجود در قلمرو سایبری هر کشور تابع حکمرانی آن کشور بوده و تمام کشورها حق دارند از قلمرو خود در برابر هر گونه تجاوز محافظت نمایند. از سوی دیگر اعمال نشدن حاکمیت سایبری ملی، منجر به تضعیف نظام حاکم خواهد شد و رفتار قانون‌مند کنشگران ملی و بین‌المللی در یک فضای قانونی را به همراه نخواهد داشت.

امروزه زیرساخت‌های حیاتی کشور به‌عنوان مؤلفه حائز اهمیت حاکمیت ملی، یا بخشی از فضای سایبر کشور محسوب می شوند یا حداقل در این فضا پایش، کنترل، مدیریت و مورد بهره‌برداری قرار می‌گیرند. استفاده از سخت‌افزارها، میان‌افزارها، نرم‌افزارها و پروتکل‌های غیربومی در محیط شبکه‌ای زیرساخت‌های حیاتی، در صورتی که چگونگی اعمال حاکمیت بر قلمرو سایبری ملی مشخص نگردد و تضمین‌های لازم در ممانعت از هر گونه نقض حاکمیت ملی در این فضا با استناد به اصول و قواعد حقوق بین‌الملل احصاء نگردد، می‌تواند عواقب گاه جبران‌ناپذیری در مقابل اقدامات ناقض حاکمیت اعم حملات سایبری خارجی و ... برای امنیت ملی کشور به همراه داشته باشد.

واضح است در صورت مشخص نشدن چگونگی اعمال حاکمیت بر قلمرو سایبری ملی در پرتو حقوق بین‌الملل و عدم آگاهی و آشنایی متولیان و کنشگران کشور به اصول، قواعد و راهکارهای حقوقی، پیگیری قانونی و حقوقی در صورت تعرض به قلمرو فضای سایبری کشور و نقض حاکمیت ملی در این عرصه، امکان‌پذیر نخواهد بود.

همچنین در صورت مشخص نشدن چگونگی اعمال حاکمیت بر قلمرو سایبری ملی در پرتو حقوق بین‌الملل؛ امکان سیاست‌گذاری، هماهنگی و اجرا بین بخش های مختلف کشور، در اعمال حاکمیت سایبری ملی فراهم نخواهد شد.

دغدغه و مسئله این تحقیق، اکتشاف چگونگی اعمال حاکمیت بر قلمرو سایبری ملی با اتکا به حقوق بین‌الملل می‌باشد و گروه محققین، با مرور و بررسی اصول و قواعد حقوق بین‌الملل حال حاضر به دنبال پاسخ به این سؤال هستند که آیا اصول و قواعد حقوق بین‌الملل با قاطعیت و شفافیت از اقدامات خصمانه سایبری که حاکمیت کشورها بر قلمرو سایبری را نقض می‌کنند، جلوگیری می‌کند و این اصول و قواعد قابل اتکا در صیانت از حاکمیت کشورها بر قلمرو سایبری ملی هستند؟

۲ مبانی نظری تحقیق

۱.۲ پیشینه تحقیق

با بررسی‌های انجام شده در منابع مختلف، موارد زیر به عنوان پیشینه تحقیق به‌دست آمده است:

مصطفی فضائلی و موسی کرمی (۱۳۹۹) در مقاله‌ای با عنوان «تحول تاریخی حقوق بین‌الملل توسل به زور تا شکل‌گیری نظام ملل متحد؛ بیم‌ها و امیدها» که در فصلنامه علمی مطالعات دفاع مقدس دانشگاه عالی دفاع ملی به چاپ رسیده است، کوشیده‌اند تا از رهگذر تاریخی به تحلیل چگونگی تنظیم حقوقی توسل به زور تا شکل‌گیری نظام ملل متحد، کاستی‌ها و چالش‌های آن بپردازند و بر این نکته تأکید نموده‌اند، طی دهه‌های گذشته جامعه بین‌الملل شاهد گذار از اصل توسل به زور برای حل و فصل اختلافات، به اصل ممنوعیت بکارگیری زور به‌سان قاعده‌ای بنیادین در روابط میان دولت‌ها بوده است. به باور نگارندگان این پژوهش، این روند تکاملی را باید از نشانه‌های نهادینه شدن تدریجی حقوق بین‌الملل توسل به زور در روابط میان دولت‌ها قلمداد کرد و بر همین پایه می‌توان از کارآمدی نسبی این شاخه حقوقی در کاهش بکارگیری زور در این بستر سخن راند. در نتیجه طی سال‌های گذشته، روابط بین‌الملل از افسارگسیختگی بی‌حد و حصر دولت‌ها در بکارگیری زور تا محدود شدن آن به مواردی انگشت‌شمار و معین را تجربه کرده و شاهد بوده است (مصطفی فضائلی و موسی کرمی،۱۳۹۹)؛ (Fazaeli, Mustafa & Karami, Musa, 2020).

در پژوهشی دیگر احسان کیانخواه (۱۳۹۸)، طی مقاله‌ای با عنوان «چالش‌های راهبردی حکمرانی با گسترش فضای سایبر» که درفصلنامه علمی امنیت ملی دانشگاه عالی دفاع ملی به چاپ رسیده است، به اکتشاف چالش‌های حکمرانی با گسترش فضای سایبر پرداخته است. این پژوهش نتیجه می‌گیرد، به خدمت گرفتن هر پدیده نیازمند فهم دقیق آن است و توجه به مصالح و مفاسد آن دارد. درجه پیچیدگی فهم پدیده‌ها بر اساس کارایی و وسعت آثار آن متفاوت است. فضای سایبر در کنار تحولات مطلوب و پرشتاب آن، دارای مفاسدی است که موجب چالش‌های کلیدی برای حکمرانی کشور شده است. در پایان نیز چالش‌های راهبردی حکمرانی با گسترش فضای سایبر را احصا نموده است. این پژوهش تأکید می‌نماید عدم توجه به چالش‌های راهبردی حکمرانی با گسترش فضای سایبر، منجر به وابستگی کشور به بیگانگان و سلطه کفار بر نظام اسلامی خواهد شد. (احسان کیانخواه، ۱۳۹۸)؛ (Kiankhah. 2020).

در مقاله‌ای دیگر، امید جعفرنیا و محمدرضا کریمی قهرودی (۱۳۹۹)، در پژوهشی با عنوان «اهمیت و الزامات حاکمیت فضای سایبری» که در چهارمین کنفرانس ملی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک ایران به چاپ رسیده است، به بررسی اهمیت و الزامات حاکمیت فضای سایبری پرداخته‌اند. این

پژوهش تصریح می کند، حاکمیت فضای مجازی به بخش مهمی از حاکمیت فضای واقعی ملی تبدیل خواهد شد. این پژوهش، ضمن بررسی برخی اختلافات به‌وجود آمده در نبود حاکمیت فضای مجازی، لزوم وجود حاکمیت فضای سایبری و فواید آن در حاکمیت ملی، کنترل و همکاری در امور مربوط به ایجاد عدالت بین‌المللی در این فضا را اثبات می‌نماید. بر این اساس حضور قوی در تعاملات بین‌المللی فضای مجازی جهت تبیین ملاحظات و الزامات کشور در ساختارهای مدیریت و کنترل جهانی این فضا به عنوان خروجی این تحقیق احصاء شده است (امید جعفرنیا و محمد رضا کریمی قهرودی، ۱۳۹۹)؛ (Jafarnia, Omid and Karimi Ghahroudy, Mohammad Reza, 2019).

علی‌رغم انجام پژوهش‌های متعدد در زمینه حقوق بین‌الملل، حاکمیت ملی و حاکمیت سایبری که در منابع داخلی و خارجی ارایه گردیده است، و با توجه به شرایط خاص کشور ما که همواره دشمنان در پی نقض حاکمیت سایبری ملی و وارد نمودن آسیب به منافع و سرمایه‌های ملی کشور هستند، بررسی چگونگی اعمال حاکمیت سایبری ملی با اتکا به حقوق بین‌الملل که مد نظر این پژوهش است، تاکنون انجام نشده است و با توجه به خلأ دانشی موجود در این زمینه، انجام این پژوهش ضروری به نظر می‌رسد.

۲.۲ مفهوم‌شناسی تحقیق

۱.۲.۲ قلمروی سایبری

قلمرو عبارت است از فضای جغرافیایی مشخص، اعم از واقعی و مجازی که منعکس‌کننده عرصه حاکمیت و فرمان‌روایی یک بازیگر سیاسی به ویژه حکومت یا حوزه کنترل و نفوذ یک کارکرد و فعالیت سیاسی، اجتماعی، فرهنگی و ... آن می‌باشد. همان‌طور که در فضای واقعی حیات و فعالیت انسان‌ها، قلمروها و عرصه‌های مختلف برای اعمال حاکمیت وجود دارد، در فضای سایبری نیز عرصه‌های حاکمیتی و قلمروهای فعالیت، با فضا و چارچوب مشخص وجود دارد. با این تفاوت که این قلمروها از ماهیت مجازی و دیجیتالی برخوردارند (حافظ نیا، ۱۳۹۰)؛ (Hafeznia Mohammad Reza, 2011).

۲.۲.۲ حاکمیت ملی سایبری

حاکمیت فضای سایبری یک کشور مبتنی بر سامانه‌های اطلاعاتی و ارتباطی تحت اختیار آن کشور می‌باشد. مرزهای حاکمیت فضای سایبری یک کشور از مجموعه تجهیزات شبکه‌ای آن کشور که به طور مستقیم به تجهیزات شبکه‌ای کشورهای دیگر متصل هستند تشکیل می‌شود. حاکمیت فضای سایبری به منظور حفاظت از عملیات‌های مختلفی که کاربران سایبر روی داده‌ها انجام می‌دهند اعمال می‌گردد.

تعریف سازمان ملل متحد از حاکمیت ملی سایبری عبارت است از: «حاکمیت ملی، هنجارها و اصول بین‌المللی که از حاکمیت نشئت می‌گیرند، در مورد فعالیت‌های کشورها در ارتباط با فناوری اطلاعات و ارتباطات و اختیار آنها بر زیرساخت‌های اطلاعاتی و ارتباطی موجود در قلمرو سرزمینی نیز صادق می‌باشد. بر این اساس اگرچه در تعریف مذکور به طور مستقیم به واژه «فضای سایبری» اشاره نشده است ولی این تعریف نشان می‌دهد حاکمیت ملی در دو سطح اعمال می‌گردد: سطح فنی و سطح اجتماعی. در سطح فنی حاکمیت ملی در مورد زیرساخت‌های اطلاعاتی و ارتباطی، که در سطح «سایبر» قرار دارند و اینترنت و

انواع مختلف شبکه‌های مخابراتی و سامانه‌های ارتباطی، شبکه‌های رادیویی و تلویزیونی، سامانه‌های رایانه‌ای و پردازشگرها و کنترل‌کننده‌های موجود در تجهیزات صنعتی کلیدی را در بر می‌گیرند، اعمال می‌شود. در سطح اجتماعی، حاکمیت ملی در مورد فعالیت‌های مرتبط با فناوری اطلاعات و ارتباطات که در سطح «فضا» قرار دارند و فعالیت‌های مختلف که سکوی نظام فناوری اطلاعات و ارتباطات را در بر می‌گیرند، اعمال می‌گردد.» (کریمی قهرودی، ۱۳۹۹)؛ (Karimi Ghahroudi Mohammad Reza, 2020).

از این رو اقدامات و عملیات‌های سایبری که از اعمال امتیازات حاکمیتی دولت ممانعت به عمل می‌آورند و موجب نقض اقتدار حاکمیتی دولت در فضای سایبری می‌شوند، ناقض حاکمیت سرزمینی کشورها بوده و در حقوق بین‌الملل ممنوع می‌باشند.

۳.۲.۲ اصول و قواعد حقوق بین‌الملل مرتبط با حاکمیت ملی سایبری

اصل خودداری از تهدید و توسل به زور. بند ۴ ماده ۲ منشور ملل متحد مقرر می‌دارد، کلیه اعضای ملل متحد در روابط بین‌الملل خویش از تهدید و بکارگیری زور علیه یکپارچگی سرزمینی یا استقلال سیاسی کشور دیگر به هر شیوه‌ای که با اهداف ملل متحد ناسازگار باشد خودداری خواهند ورزید و امروزه این ممنوعیت قاعده‌ای از حقوق بین‌الملل عرفی به حساب می‌آید. یعنی اگر چه بند ۴ ماده ۲ منشور ملل متحد در بیان صریح خود انحصاراً بر اعضای ملل متحد اعمال می‌شود، ولی ممنوعیت توسل به زور از رهگذر حقوق بین‌الملل عرفی به کشورهای غیر عضو نیز تسری می‌یابد (Leigh, M. 1985).

دیوان بین‌المللی دادگستری نیز با استناد به ماده ۲ بند ۴ منشور ملل متحد، ممنوعیت هر گونه بکارگیری زور توسط دولت‌ها (فارغ از تسلیحات مورد استفاده) به‌منظور نقض یا خدشه‌دار نمودن حاکمیت سرزمینی کشور دیگر را اعلام نموده است. لزومی ندارد عملی که «بکارگیری زور» به‌شمار می‌آید، ضرورتاً توسط نیروهای مسلح یک کشور انجام شده باشد یا صرف اینکه یک رایانه (و نه یک اسلحه یا سامانه تسلیحاتی) در انجام عملیات به‌کار رود، تأثیری در «به‌کارگیری زور» قلمداد شدن یا نشدن عملیات ندارد. هر گونه توسل به زور که توسط عوامل دولتی انجام شود یا وفق حقوق مسئولیت دولت، قابل انتساب به یک دولت باشد ذیل این اصل حقوق بین‌الملل قرار می‌گیرد. واضح است اقدامات بازیگران غیردولتی از جمله افراد، گروه‌های سازمان‌یافته و سازمان‌های تروریستی قابل تسری به این ممنوعیت نخواهد بود مگر اینکه قابل انتساب به دولت باشند (Falk, R. 1997).

اصل ممنوعیت مداخله غیرمجاز در امور داخلی دیگر کشورها. ممنوعیت مداخله غیرمجاز در امور داخلی دیگر کشورها، یک اصل اساسی حقوق بین‌الملل است که در منشور ملل متحد صراحتاً به آن اشاره نشده است ولی طی سالیان گذشته از حقوق عرفی برخوردار شده است. بر اساس بیانیه مجمع عمومی سال ۱۹۶۵ میلادی در مورد غیرقابل قبول بودن مداخله در امور داخلی دولت‌ها و حفاظت از استقلال و حاکمیت آنها، که مجدداً در بیانیه مجمع عمومی سال ۱۹۷۰ میلادی در مورد روابط دوستانه و همکاری میان دولت‌ها نیز تکرار شد: «هیچ دولتی حق مداخله مستقیم یا غیر مستقیم در امور داخلی و خارجی دولت‌های دیگر را ندارد». در نتیجه، مداخله مسلحانه و سایر اشکال مداخله و یا حتی تلاش برای تهدید علیه شخصیت

دولت و عناصر سیاسی، اقتصادی و فرهنگی آن محکوم است. همچنین دیوان بین‌المللی دادگستری در پرونده نیکاراگوئه، ممنوعیت مداخله را «حق هر دولت مستقل برای انجام امور [خارجی یا داخلی] خود بدون دخالت خارجی» تعریف کرده است (Leigh, M. 1985).

برای تعریف محتوا و معنای اصل عدم مداخله در حقوق بین‌الملل، باید معنای نقطه مقابل آن، یعنی مداخله را توضیح دهیم. بر اساس تعریف اوپنهایم، مداخله عبارت است از «هر گونه مداخله یا اقدام توأم با اجبار و زور که دولت را از کنترل بر موضوع مورد نظر محروم می‌کند». از تعریف فوق معلوم می‌شود که برای انتصاب مداخله، باید دو شرط برآورده گردد: اول باید بر امور و موضوعاتی که در حاکمیت یک دولت قرار دارند تأثیر بگذارد و ثانیاً باید اجباری باشد (Oppenheim, L. 1921).

۴.۲.۲ اسناد حقوق بین‌الملل مرتبط با حاکمیت ملی سایبری

منشور ملل متحد. با استناد به متن منشور ملل متحد، اعلامیه اصول حقوق بین‌الملل درباره روابط دوستانه و همکاری میان دولت‌ها، اعلامیه ارتقاء اثربخشی اصل خودداری از تهدید یا توسل به زور در روابط بین‌الملل و آراء دیوان بین‌المللی دادگستری، حاکمیت بر قلمرو ملی و سرزمینی یکی از اصول اساسی منشور ملل متحد است که از تساوی حاکمیتی کشورها، عدم توسل به زور علیه تمامیت ارضی و ممنوعیت اقداماتی که با مقاصد منشور در تضاد هستند نتیجه می‌شود. منشور ملل متحد در فصل اول، پس از برشمردن مقاصد ملل متحد در ماده یک؛ برای نیل به مقاصد یاد شده، در ماده دوم به اصل تساوی حاکمیت تمامی اعضا تأکید می‌نماید. مهم‌تر از آن در بند ۴ ماده ۲ مقرر می‌دارد «تمامی اعضا در روابط بین‌الملل خود از تهدید به زور یا استفاده از آن علیه تمامیت ارضی و استقلال سیاسی کشورهای دیگر، از هر روشی که با مقاصد منشور ملل متحد در تضاد باشد، خودداری خواهند نمود» (منشور ملل متحد، ۱۹۴۵).

کتابچه راهنمای تالین ۲. یکی از مهم‌ترین تلاش‌ها برای تحقیق روی قواعد بین‌المللی حاکم بر اقدامات سایبری، توسط گروه کارشناسان بین‌المللی به دعوت مرکز تعالی دفاع سایبری ناتو تحت عنوان راهنمای تالین یک و دو انجام پذیرفته است. راهنمای تالین یک با عنوان«دستورالعمل حقوق بین‌الملل قابل اعمال در نبرد سایبری» توسط متخصصین و صاحب‌نظران حقوقی و فنی در قالب ۹۵ قاعده اساسی در سال ۲۰۱۳ میلادی توسط انتشارات دانشگاه کمبریج به چاپ رسیده است. نسخه تکمیلی راهنمای تالین یک، تحت عنوان راهنمای تالین دو که به حقوق بین‌الملل قابل اعمال بر عملیات‌های سایبری می‌پردازد، در قالب ۱۵۴ قاعده کلی حقوق بین‌الملل حاکم بر اقدامات سایبری در سال ۲۰۱۷ تدوین و به چاپ رسیده است.

در این زمینه قواعد تالین دو که مرتبط با احترام به حاکمیت سرزمینی کشورها و ممنوعیت نقض حاکمیت ملی در فضای سایبر، احترام به حقوق بشر، منع مداخله در امور داخلی کشورها، ممنوعیت تهدید و توسل به زور می‌باشند و همه این قواعد به حاکمیت بر قلمرو سایبری کشورها و ممانعت از هرگونه تجاوز و دست اندازی به قلمرو و مرزهای سایبر ملی تاکید دارند، اشاره می‌گردد.

صلاحیت سرزمینی و حاکمیت بر قلمرو از اصول بنیادین حقوق بین‌الملل به شمار می روند. قواعد ۱ تا ۱۳ راهنمای تالین دو، تصدیق می‌نمایند صلاحیت سرزمینی و فراسرزمینی و نیز حاکمیت دولت‌ها بر قلمرو،

می‌بایست در فضای سایبری نیز اعمال گردد. اگر چه اصل صلاحیت سرزمینی در دل اصل حاکمیت نهفته است، گروه کارشناسان بین‌المللی تالین این اصول را در قالب قواعد تفکیک شده تدوین نموده‌اند. از میان قواعد مبتنی بر صلاحیت سرزمینی و حاکمیت دولت‌ها در فضای سایبری، قاعده شماره ۴ که به ممنوعیت نقض حاکمیت دولتی کشورها در این فضا اشاره دارد، از اهمیت بیشتری برخوردار است. قواعد تالین دو مقرر می‌نمایند، یک دولت، با لحاظ محدودیت‌های مقرر در حقوق بین‌الملل، از صلاحیت سرزمینی و فراسرزمینی بر فعالیت‌های سایبری مرتبط با خود برخوردار است.

قواعد ۳۴ تا ۳۸ راهنمای تالین دو، از نظام بین‌الملل حقوق بشر در فعالیت‌های سایبری، تعهد دولت‌ها به احترام و حمایت از حقوق بشر و موارد استثناء قابل قبول در تخطی از حقوق بشر، سخن می‌گوید. کارشناسان تدوین تالین دو بر این باورند، اعلامیه جهانی حقوق بشر، به عنوان بازتاب‌دهنده هنجارهای عرفی اصلی حقوق بشر مورد تأیید همگان است.

به واسطه پیوند روزافزون جامعه جهانی و وابستگی رو به رشد دولت‌ها به بهره‌گیری از زیرساخت‌های سایبری، این عرصه فرصت‌هایی را برای مداخله سایر دولت‌ها در امور داخلی کشورها قرار داده است. بر این اساس قواعد ۶۶ و ۶۷ راهنمای تالین دو، به مبانی حقوق بین‌الملل منع مداخله جبرآمیز دولت‌ها و ملل متحد (به استثناء آنچه ذیل فصل هفتم منشور ملل متحد قرار می‌گیرد) در امور داخلی کشورها در فضای سایبری و با استفاده از ابزارهای سایبری اختصاص یافته است. اصل برابری حاکمیتی و احترام به حاکمیت دولت‌ها ایجاب می‌نماید، دولت‌ها از اقدامات و اموری که در حیطه حاکمیت دولت دیگر هستند و مداخله در آنها، حاکمیت دولت سرزمینی را خدشه‌دار می‌نماید از طریق ابزارهای سایبری اجتناب نمایند (Schmitt, M. N. 2017. Tallinn manual 2.).

۳ روش‌شناسی تحقیق

۱.۳ نوع تحقیق

نظر به اینکه انجام این پژوهش به بررسی چگونگی اعمال حاکمیت بر قلمرو سایبری ملی با اتکا به حقوق بین‌الملل منجر می‌شود و نتایج حاصل از این پژوهش شناخت بهتر و افزایش توان اتخاذ مناسب‌ترین تصمیمات توسط متولیان امر در کشور را به همراه خواهد داشت، جنبه کاربردی دارد. همچنین با توجه به اینکه توسعه پژوهش‌های گذشته و گسترش دانش در این حوزه را به دنبال دارد، توسعه‌ای به حساب می‌آید. بنابراین تحقیق حاضر با توجه به هدف، از نوع توسعه‌ای-کاربردی می‌باشد.

۲.۳ روش تحقیق

روش تحقیق مورد استفاده، با رویکرد کیفی از نوع تحلیل محتوا و ابزار مورد استفاده نرم‌افزار مکس‌کیودا[1] می‌باشد. در این پژوهش اسناد حقوق بین‌الملل مرتبط با حاکمیت سایبری ملی و سرزمینی اعم از منشور ملل متحد، منشور حقوق بشر، اعلامیه حقوق بین‌الملل درباره روابط دوستانه و همکاری میان دولت‌ها، اعلامیه

[1] MAXQDA 10

ارتقاء اثربخشی اصل خودداری از تهدید یا توسل به زور در روابط بین‌الملل، آراء دیوان بین‌المللی دادگستری، گزارش‌های گروه کارشناسان دولتی سازمان ملل متحد در زمینه توسعه فناوری اطلاعات و ارتباطات (GGE) و کتابچه راهنمای تالین دو (به‌عنوان یکی از مهم‌ترین تلاش‌ها برای تحقیق روی قواعد بین‌المللی حاکم بر اقدامات سایبری که توسط گروه متخصصین بین‌المللی به دعوت مرکز تعالی دفاع سایبری ناتو انجام پذیرفته است)؛ با استفاده از نرم‌افزار مکس‌کیودا در قالب روش تحلیل محتوای استنباطی از نوع قراردادی یا عرفی مورد بررسی قرار گرفت.

در این زمینه قواعدی که به موضوع حاکمیت سایبری ملی کشورها تأکید دارد اعم از قواعد احترام به حقوق بشر بین‌المللی، احترام به حاکمیت سرزمینی کشورها، ممنوعیت نقض حاکمیت ملی، ممنوعیت تهدید یا توسل به زور و منع مداخله غیرمجاز در امور داخلی کشورها؛ با استفاده از نرم‌افزار مکس‌کیودا تحلیل محتوا و کدگذاری گردید که منجر به احصاء ۸۱ کد یا واحد معنایی در زمینه حاکمیت بر قلمرو سایبری ملی و سرزمینی گردید. در ادامه پس از چند بار مرور کدها، کدها یا واحدهای معنایی نزدیک به هم با یکدیگر ترکیب گردید تا واحدهای معنایی منسجم و ساختاریافته‌تری ایجاد گردد. در مرحله بعد پس از مرور چندباره واحدهای معنایی، واحدهای معنایی که با یکدیگر مرتبط و یک مقوله خاصی را تداعی می‌نمایند، دسته‌بندی گردید تا زیرطبقات مورد بحث تولید گردند. در این مرحله نیز واحدهای معنایی و زیرطبقات به‌صورت رفت و برگشتی چند بار مرور شد تا از صحت فرآیند دست‌یابی به زیرطبقات اطمینان حاصل شود.

پس از بررسی واحدهای معنایی و زیرطبقات مرتبط با حاکمیت بر قلمرو سایبری ملی در اسناد حقوق بین‌الملل، مشخص گردید، علی‌رغم وجود اصول و قواعدی که احترام به حاکمیت کشورها بر قلمرو سرزمینی، پایبندی به حقوق بشر (مردمان) ساکن در قلمرو سرزمینی سایر دولت‌ها، احترام به صلاحیت دولت‌ها در کنترل و مدیریت منابع و زیرساخت‌ها در قلمرو سرزمینی، ممنوعیت تهدید و توسل به زور علیه دولت دیگر و ممنوعیت مداخله در امور داخلی دیگر کشورها را از اصول اساسی در حقوق بین‌الملل به شمار می‌آورند؛ در اسناد مزبور، واحدهای معنایی و زیرطبقاتی وجود دارند که نه‌تنها صیانت از حاکمیت ملی و سرزمینی را تضمین نمی‌نمایند بلکه امکان نقض حاکمیت سایبری ملی و سرزمینی را فراهم می‌نمایند و پیگرد حقوقی اقدامات و عملیات‌های سایبری با استناد به اصول و قواعد حقوق بین‌الملل میسر نیست. از این رو می‌توان نتیجه گرفت، اسناد حال‌حاضر حقوق بین‌الملل، حاکمیت سایبری ملی کشورها را تضمین نمی‌نمایند و موارد نقض متعدد غیرقابل پیگیری در حقوق بین‌الملل وجود دارد.

جدول ۱، واحدهای معنایی و زیرطبقات موارد نقض حاکمیت سایبری ملی در حقوق بین‌الملل، که با استفاده از نرم‌افزار مکس‌کیودا احصاء شده است و این واحدهای معنایی و زیرطبقات، نمایان‌گر طبقه اصلی حاصل از تحلیل محتوای کیفی که «ناتوانی حقوق‌بین‌الملل در صیانت از حاکمیت سایبری ملی کشورها» می‌باشد را نشان می‌دهد.

جدول ۱: کدهای هدایت‌کننده، زیرطبقات و طبقه اصلی

طبقه اصلی	زیرطبقات	کدهای هدایت کننده
ناتوانی حقوق بین الملل در صیانت از حاکمیت سایبری ملی کشورها	ابهام و عدم قطعیت اسناد حقوق بین‌الملل در تعیین اقدامات و عملیات‌های سایبری غیرمجاز که حاکمیت سایبری ملی دیگر کشورها را نقض می نمایند.	• علی‌رغم وجود نظام حقوق بین‌الملل عرفی و معاهداتی، فهرست قطعی و نهایی از حقوق بین‌الملل لازم الاجرا برای دولت‌ها وجود ندارد. • تعریف دقیقی از اقدامات ناقض حاکمیت ملی (اعم از: توسل به زور، مداخله غیرمجاز و ...) در اسناد حقوق بین‌الملل وجود ندارد. • تهدید و توسل به زور، صرفاً به اقدامات مسلحانه یک دولت علیه حاکمیت، تمامیت ارضی یا استقلال سیاسی دولت دیگر اطلاق می‌گردد. • تفسیر کشورها از اقدامات ناقض حاکمیت ملی در اسناد حقوق بین‌الملل متفاوت است. • تعیین سطح آستانه اقدامات و عملیات‌های سایبری ناقض حاکمیت سرزمینی به سادگی امکان‌پذیر نیست. • تفسیر کشورها از همترازی اقدامات و عملیات‌های فضای سایبری با اقدامات و عملیات‌های فضای واقعی متفاوت است.
	اقدامات و عملیات‌های سایبری مخرب و ناقض حاکمیت سرزمینی، صرفاً در مواردی که قابل انتساب به یک دولت دیگر باشند از پیگرد حقوقی برخوردار است.	• هر دولت صرفاً مسئول اقدامات اشخاص و نهادهایی است که به نوعی نماینده دولت محسوب می‌گردند. • صرفا اقدامات و عملیات‌هایی که قابل انتساب به یک دولت باشند، امکان پیگیری حقوقی دارد. یعنی اقدامات توسط عوامل دولتی یا عوامل غیردولتی که تحت حمایت، کنترل و مدیریت یک دولت هستند انجام گرفته باشد و یا یک دولت عملیات مزبور را به عنوان عملیات خود تصدیق نموده و بپذیرد. • انتساب اقدامات و عملیات‌های سایبری به دولت متخاصم با پیچیدگی و عدم قطعیت‌های فنی و حقوقی همراه است. • تنبیه دولت متخاصم حتی در صورت قطعیت اقدامات متخلفانه سایبری (اعم از توسل به زور، مداخله غیرمجاز و ...) که حاکمیت سرزمینی کشور دیگر را نقض نموده است، با توجه به عدم امکان انتساب به دولت، عملاً امکان‌پذیر نیست. • عملیات‌ها و اقداماتی که به سطح توسل به زور و اجبار از سوی یک دولت نرسند، ممنوعیت حقوق بین‌الملل را نقض نمی‌نمایند.اقدامات و عملیات‌های سایبری که توسط کنشگران غیردولتی اعم از افراد، گروه‌های سازمان‌یافته، سازمان‌های تروریستی و ... انجام می‌پذیرد و قابل انتساب به دولت نباشد، قواعد حقوق بین‌الملل را شامل نمی شود.
	اقدامات و عملیات‌های سایبری مخرب و ناقض حاکمیت سرزمینی، صرفاً در مواردی که علیه یک دولت انجام شده باشند از پیگرد حقوقی برخوردار هستند.	• اقدامات دولت متخاصم که نهادها، شرکت ها، اقوام و ... را هدف قرار می دهند، اگر چه تا اندازه‌ای حاکمیت دولت سرزمینی را نقض می‌نمایند، قابل پیگیری از طریق مجاری حقوق بین‌الملل نیستند. • عملیات‌ها و اقداماتی که به سطح توسل به زور و اجبار علیه دولت دیگر نرسند، ممنوعیت حقوق بین‌الملل را نقض نمی‌نمایند. • حقوق بین‌الملل عرفی و معاهداتی، موارد استثناء قابل قبول در تخطی دولت‌ها از تعهدات بین‌المللی در برابر سایر دولت‌ها قائل شده است.
	عدم تمایل کشورهای پیشرفته و صاحب فناوری به تدوین نظامات حقوقی روشن و متقن برای فضای سایبری در جهت ممانعت و مقابله با فعالیت‌های مخرب و ناقض حاکمیت ملی و سرزمینی کشورها	• عدم اهتمام کشورهای پیشرفته در تصویب قوانین و هنجارهای بین المللی دقیق در منع استفاده خصمانه از فضای سایبری. • استفاده از شرایط بدون مرزی، ابهام و پیچیدگی فضای سایبری توسط کشورهای پیشرفته در جهت استفاده از این فضا برای دست یابی مقاصد و منافع خصمانه. • بهره گیری از فضای سایبری به عنوان عرصه ای کم هزینه و آسان در جهت استعمار نوین. • به نظر نمی رسد در آینده نزدیک اجماع و توافق بین المللی در تدوین اصول، قواعد و هنجارهای اختصاصی فضای سایبری که تضمین کننده حاکمیت سایبری ملی کشورها باشد، انجام پذیرد.
	ناتوانی جامعه بین‌الملل در تدوین نظامات حقوقی شفاف فضای سایبری	• عدم توافق کشورها در تدوین اصول و هنجارهای اختصاصی فضای سایبری. • نگرش متفاوت کشورها نسبت به مدل حکمرانی فضای سایبری، دست یابی به نظام واحد حقوقی در این زمینه را دور از ذهن نموده است. • با توجه به اینکه مقیاس و آثار اقدامات و عملیات‌های ناقض حاکمیت سایبری ملی ممکن است در کوتاه‌مدت امکان‌پذیر نباشد، تدوین نظام حقوقی متناسب برای آنها نیز میسر نیست.

۴ تجزیه و تحلیل یافته‌ها

از تحلیل محتوای کیفی اسناد حقوق بشر یافت می‌شود، احترام به حاکمیت کشورها بر قلمرو سرزمینی یک اصل اساسی در حقوق بین‌الملل به شمار می‌رود و از آن قواعد و هنجارهای بازدارنده‌ای از حقوق بین‌الملل ناشی می‌شود که مورد پذیرش همگان است. مهم‌ترین این قواعد، پایبندی به حقوق بشر (مردمان) ساکن در قلمرو سرزمینی سایر دولت‌ها، احترام به صلاحیت دولت‌ها در کنترل و مدیریت منابع و زیرساخت‌ها در قلمرو سرزمینی، ممنوعیت تهدید و توسل به زور علیه دولت دیگر و ممنوعیت مداخله در امور داخلی دیگر کشورها می‌باشد.

اما همچنین از تحلیل محتوای اسناد حقوق بین‌الملل مرتبط با حاکمیت سایبری ملی و سرزمینی کشورها می توان به این نتیجه رسید، قوانین و هنجارهای فعلی بین‌المللی، اقدامات زیر سطح آستانه این قواعد را نهی نمی‌کند و دولت‌ها را ملزم نمی‌کند از هرگونه فعالیتی که حاکمیت دولت سرزمینی را خدشه‌دار می‌کند خودداری نمایند. به خصوص اینکه تعیین سطح آستانه اقدامات ناقض حاکمیت سرزمینی کشورها در فضای مجازی و همتراز شمردن اقدامات و عملیات‌های سایبری با اقدامات و عملیات‌های ناقض حاکمیت سرزمینی در فضای واقعی، به دلیل عدم شفافیت و قطعیت اسناد حقوق بین‌الملل در این زمینه، دوچندان مشکل است. به علاوه، با توجه به خصوصیات و ویژگی‌های فضای سایبری، انتساب اقدامات ناقض حاکمیت سرزمینی به دولت متخاصم، در قریب به اتفاق موارد امکان‌پذیر نیست. شواهد این امر را می‌توان در این واقعیت مشاهده کرد که دولت‌ها عملیات‌های نفوذ، جاسوسی و جمع‌آوری اطلاعات حیاتی و حتی تخریب منابع، زیرساخت‌ها و سامانه‌های موجود در قلمرو سرزمینی دیگر کشورها را از طریق فضای سایبری آن کشورها انجام می‌دهند و پیگرد قانونی از طریق حقوق بین‌الملل متصور نیست.

در کنار این موضوعات، بی‌علاقگی یا ناتوانی کشورها در تدوین نظامات حقوقی شفاف و متقن برای فضای سایبری در جهت ممانعت و مقابله با فعالیت‌های مخرب و ناقض حاکمیت ملی و سرزمینی کشورها در فضای سایبری (با توجه به ویژگی‌های منحصر به فرد این فضا)، منجر به پیدایش ابهامات و روزنه‌هایی برای نقض حاکمیت کشورها و عدم امکان تعیین زمان دقیق نقض حاکمیت و به تبع آن عدم پیگیرد بین‌المللی در این زمینه شده است.

با عنایت به مراتب یاد شده می توان استنباط کرد، رویکردی که در اسناد حال‌حاضر بین‌المللی فضای سایبر مورد تاکید قرار گرفته است، بر تاثیرات فیزیکی اقدامات سایبری بر علیه قلمرو سرزمینی کشورها تاکید دارد و جنبه مهم دیگر، یعنی احترام به صلاحیت دولت‌ها در کنترل دسترسی، مدیریت و بهره‌برداری از زیرساخت‌ها و سامانه‌های سایبری مستقر در قلمرو ملی کشورها را به هنگام نقض اصول امنیت سایبری ملی مورد توجه قرار نمی‌دهد. از این رو اقداماتی که منجر به آسیب فیزیکی یا از دست رفتن عملکردهای اساسی نشوند که نیازمند تعمیر یا جایگزینی زیرساخت‌ها و سامانه‌ها باشد، نقض حاکمیت ملی سایبری تلقی نمی‌گردند. همچنین اگر نقض تمامیت سرزمینی یک کشور در حوزه سایبری، صرفا به تجلی آثار فیزیکی حملات یا از دست دادن عملکرد قابل توجه سامانه‌ها بستگی داشته باشد، دولت‌های هدف در برابر عملیات سایبری که در مراحل مقدماتی خود قرار دارند و یا در حال انجام هستند ولی تاکنون منجر به آسیب و خسارت

سطح بالا نشده اند، هیچ گونه راه‌حل قانونی در دفاع از خود نخواهند داشت. امروزه عملیات‌های سایبری پیچیده و گسترده علیه زیرساخت‌های یک کشور، به چندین مرحله مقدماتی اعم از شناسایی هدف، انتخاب بردار حمله مناسب، دور زدن امنیت زیرساخت‌ها و سامانه‌های سایبری کشور هدف و در نهایت انجام فعالیت مورد نظر نیاز دارد (در برخی مدل‌های تحلیلی، مراحل مقدماتی انجام عملیات سایبری تا ۷ مرحله عنوان شده است). رویکرد فعلی نقض حاکمیت ملی سایبری در صورت عدم ظهور آثار فیزیکی، تمامی این مراحل را که منجر به نقض اصول امنیت سایبری ملی کشور هدف می‌شوند، نقض حاکمیت بر قلمرو سایبری کشور هدف نمی‌داند و اقدام متقابل و الزام به توقف تحت قواعد و هنجارهای بین‌المللی را به همراه ندارد.

در این شرایط و در مورد عملیات‌های سایبری متوسط و کم‌شدت که منجر به خسارت فیزیکی عمده نشوند، مصداق توسل به زور به حساب نیایند یا مداخله آشکار در امور داخلی کشور هدف نباشند عدم قطعیت قانونی وجود دارد.

۵ نتیجه‌گیری

با بررسی و تحلیل محتوای کیفی اسناد حقوق بین‌الملل که با استفاده از نرم‌افزار مکس‌کیودا انجام شد و با استناد به واحدهای معنایی، زیرطبقه‌ها و طبقه اصلی احصا شده، نتیجه می‌شود، اصول و قواعد حقوق بین‌الملل از کارایی و توانایی لازم در صیانت از حاکمیت سایبری ملی کشورها برخوردار نیست و عموماً اقدامات ناقض حاکمیت سایبری ملی با شدت متوسط و کم (اعم از: توسل به زور، مداخله غیرمجاز و ...) فاقد پیگرد قانونی هستند. از این رو این قواعد و اصول در مقابل اقدامات مخرب و ناقض حاکمیت سایبری ملی از بازدارندگی لازم برخوردار نیستند.

همچنین با توجه به اینکه هنوز هیچ گونه قواعد و هنجار اختصاصی برای اقدامات زیرآستانه استفاده از زور و مداخله آشکار در فضای سایبر سایر کشورها توسعه نیافته است، تعیین دقیق مرز بین اقدامات مجاز و غیر مجاز سایبری با استناد به قوانین، مقررات و هنجارهای بین‌المللی امکان‌پذیر نیست و در بسیاری از موارد دولت‌ها آزاد هستند در این زمینه مطابق تفسیر و میل خود عمل کنند.

از این رو با توجه به یافته این پژوهش لزوم مواجهه فعالانه با موضوع فضای سایبر کشور در جهت صیانت از حاکمیت سایبری ملی، بیش از پیش ضروری به نظر می‌رسد و نیازمند شناسایی و اتخاذ راهکارهایی با هدف تقویت و ارتقاء حاکمیت بر قلمرو سایبری ملی بدون اتکا به اصول و قواعد حقوق بین‌الملل هستیم. از نظر نگارندگان این نوشتار دو راهکار قلمروگذاری و مرزبانی مؤثر و کارآمد از فضای سایبری کشور در عرصه ملی و دیپلماسی، همکاری و هماهنگی با کشورهای همسو و حضور مؤثر در مجامع بین‌المللی با هدف تبیین مواضع تقویت کننده حاکمیت سایبری در عرصه بین‌المللی می‌تواند راهگشا باشد.

مراجع

[1] Fazaeli, Mustafa & Karami, Musa. (2020). The historical evolution of the international law of the use of force until the formation of the United Nations system; Insurance and hopes. Scientific Quarterly of Sacred Defense Studies, 6 (1), 31-60. (In Persian).

[2] Kiankhah. (2020). Research Article: Strategic Governance Challenges with the Expansion of Cyberspace DOR: 20.1001. 1.33292538. 1398.9. 34.5. 5. National Quarterly Journal of National Security, 9 (34), 153-174 (In Persian).

[3] Jafarnia, Omid and Karimi Ghahroudy, Mohammad Reza, 2019, The importance and requirements of cyberspace governance, 4th National Conference on Computer Science and Technology of Electrical Engineering, Iran, Tehran (In Persian).

[4] Hafeznia Mohammad Reza, 2011, Political Geography of Cyberspace, Samat Publications (In Persian).

[5] Karimi Ghahroudi Mohammad Reza, 2020, The Rule of Cyberspace, Publications of the Defense Industries Educational and Research Institute (In Persian).

[6] Leigh, M. (1985). Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America). 1984 ICJ Reports 392. American Journal of International Law, 442-446.

[7] Falk, R. (1997). Nuclear Weapons Advisory Opinion and the New Jurisprudence of Global Civil Society. Transnat'l L. & Contemp. Probs, 7, 333.

[8] Oppenheim, L. (1921). The future of international law (Vol. 43). Clarendon Press.

[9] United States. President (1945-1953: Truman). (1945). The Charter of the United Nations with the Statute of the International Court of Justice Annexed Thereto: Address by the President of the United States Delivered Before the Senate on July 2, 1945 Presenting the Charter of the United Nations, with the Statute of the International Court of Justice Annexed Thereto: and a Message from the President of the United States Transmitting a Certified Copy of the Charter of the United Nations, with the Statute of the International Court of Justice Annexed Thereto ... US Government Printing Office.

[10] Keller, H. (2009). Friendly Relations Declaration (1970). Max Planck Encyclopedia of Public International Law.

[11] Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

[12] 2013, 2015 & 2017 UN GGE – Reports of the group of governmental experts on developments in the field of information and telecommunications.

[13] Iman Mohammad Taghi and Noshadi Mahmoud Reza, 2011, Qualitative content analysis, research, third year, second issue (In Persian).

پیشنهاد ریشه‌شناسی جدید برای مفهوم سایبر با استفاده از روش زبان‌شناسی تاریخی

محمد شمس‌الدینی [۱]، کاظم فولادی قلعه [۲]

[۱] پژوهشگر آینده‌پژوهی، پژوهشکده حضرت ولیعصر (عج)، دانشگاه جامع امام حسین (ع)
shams.m@chmail.ir
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
kfouladi@ut.ac.ir

چکیده

یکی از روش‌های فهم دقیق معانی الفاظ، ریشه‌شناسی آنهاست. در ریشه‌شناسی مفهوم سایبرنتیکز، هیچ پژوهشگری تا کنون، ریشه‌ی آن را به مفهومی غیر از کوبرنتس (kybernetes) در زبان یونانی نبرده است؛ اما تقریباً همه‌ی این پژوهشگران، پیش از آن را بررسی نکرده‌اند و به نظر می‌رسد که با مطالعه‌ی پیش از یونان، معانی مهم‌تری از این مفهوم، روشن می‌شود. در این پژوهش، برای رسیدن به معنای دقیق‌تری از مفهوم سایبرنتیکز و به‌طور خاص مفهوم سایبر، با استفاده از روش زبان‌شناسی تاریخی و به‌طور مشخص، ریشه‌شناسی و عبارت‌شناسی، سعی شده است تا ریشه‌های پیش‌تری از این مفهوم را در نزد متفکرانی که این مفهوم را استفاده کرده‌اند، کاوش کنیم. در نتیجه با ریشه‌شناسی مفهوم سایبر و مفاهیم نزدیک به آن مانند جبر، زمینه‌های جدیدی از ریشه و معنای تاریخی سایبر پیشنهاد شده است. نهایتاً با دسته‌بندی شواهد و طرح ۶ محور مفهومی به‌عنوان شاهد برای هم‌ریشگی دو مفهوم سایبر و جبر، مدعی شده‌ایم که سایبر، برگرفته از مفهوم جبر است و به‌لحاظ کارکردی نیز، اراده‌ای که در پس جهان سایبر قرار گرفته است، همان اراده‌ای است که در بنیاد معنایی مفهوم جبر نشسته است.

کلمات کلیدی: ریشه‌شناسی، سایبر، جبر، زبان‌شناسی تاریخی.

۱ مقدمه

ریشه‌شناسی، یکی از روش‌های فهم دقیق معانی مفاهیم و واژگان است که می‌توان آن را جزئی از دانش زبان‌شناسی تاریخی دانست.

مفهوم «سایبرنتیک [۱]» که در حال حاضر به‌عنوان نام یک علم به‌کار برده می‌شود و پیشوند «سایبر» که

[1] Cybernetics

از آن اخذ شده است، در دنیای امروز کاربرد فراوانی پیدا کرده است و به‌همین دلیل از جنبه‌ی معرفتی فهم معنای دقیق و ظرفیت مفهومی آن اهمیت دارد.

در ریشه‌شناسی این مفهوم، پژوهشگران به خاستگاه یونانی این واژه رسیده‌اند و هیچ پژوهشگری تا کنون، ریشه‌ی آن را به مفهومی غیر از کوبرنتس (kybernetes) در زبان یونانی نبرده است؛ این در حالی است که مشاهده می‌شود تقریباً همه‌ی این پژوهشگران، پیش از این مفهوم یونانی را بررسی نکرده‌اند و به نظر می‌رسد که با مطالعه‌ی پیش از یونان، معانی مهم‌تری از این مفهوم، روشن می‌شود.

در این پژوهش، برای رسیدن به معنای دقیق‌تری از مفهوم سایبرنتیکز و به‌طور خاص مفهوم «سایبر»، با استفاده از روش زبان‌شناسی تاریخی و به‌طور مشخص، ریشه‌شناسی (اتیمولوژی) و عبارت‌شناسی (ترمینولوژی)، سعی می‌کنیم ریشه‌های قدیمی‌تری از این مفهوم را در نزد متفکرانی که آن را استفاده کرده‌اند، کاوش کنیم. در نتیجه با ریشه‌شناسی مفهوم سایبر و مفاهیم نزدیک به آن مانند «جبر»، زمینه‌های جدیدی از ریشه و معنای تاریخی سایبر را پیشنهاد می‌کنیم. نهایتاً با دسته‌بندی شواهد و طرح شش محور مفهومی به‌عنوان شاهد برای هم‌ریشگی دو مفهوم «سایبر» و «جبر»، ادعا می‌کنیم که سایبر، برگرفته از مفهوم جبر است و به‌لحاظ کارکردی نیز، اراده‌ای که در پس جهان سایبر قرار گرفته است، همان اراده‌ای است که در بنیاد معنایی مفهوم جبر نشسته است.

این مقاله در چهار قسمت سازمان‌دهی شده است. پس از مقدمه، در قسمت دوم به بیان روش پژوهش می‌پردازیم و در قسمت سوم یافته‌های پژوهش معرفی می‌شوند. در نهایت در قسمت چهارم به نتیجه‌گیری از بحث پرداخته خواهد شد.

۲ روش پژوهش

در این پژوهش، از روش‌های زبان‌شناسی تاریخی و به‌طور خاص ریشه‌شناسی، به‌عنوان یکی از فنون زبان‌شناسی تاریخی (Durkin, 2006) و عبارت‌شناسی (ترمینولوژی) به‌معنای استفاده‌ی واژه نزد متفکر در معنایی خاص، برای درک مفهوم «سایبرنتیکز» استفاده شده است. زبان‌شناسی تاریخی، شامل مطالعه‌ی زبان در طول زمان است، چه از افق پس‌نگرانه‌ی اکنون به زمان‌های پیشین و مراحل نامستند (به‌عنوان زیرشاخه‌ای از بازسازی)، و چه از افق پیش‌نگرانه‌ی مراحل پیشین و پیش‌تر به اکنون (حوزه‌ی تغییر زبان) (McMahon, 2001).

۳ یافته‌های پژوهش

۱.۳ ریشه‌شناسی سایبر

عبارت «سایبر»، عموماً به‌عنوان مخفف «سایبرنتیکز[۲]»، شناخته می‌شود. سایبرنتیکز، مرکب از دو بخش cybernetes و ics– است. پسوند ics–، بیان‌گر این است که این مفهوم، نام یک رشته‌ی دانشی و یا دانش

[2] Cybernetics

است. cybernetes ریشه در مفهوم یونانی kybernetes به معنای «کشتی‌بان»، «ناخدا» و «سکّان‌دار[۳]» است که به‌صورت استعاری، به‌معنای حاکم و رهبر، استفاده می‌شود (T. F. Hoad, 1996). این نکته گفتنی است که سابقاً، جهت‌دهی کشتی، با سیستم مکانیکی مانند سکّان، انجام نمی‌شده است بلکه کوبرنتس، در واقع هنر هماهنگ کردن پاروزنان برای حرکت و مدیریت سرعت کشتی بوده است. ریشه‌ی این مفهوم نیز kybernan به معنای «پیش بردن»، «کنترل کردن»، «جهت دادن» و «قیادت» کشتی[۴] است که به‌صورت استعاری، به عنوان فرمان‌روایی، رهبری و حاکمیت جامعه و افراد، استفاده می‌شود (Klein, 2003). گفته می‌شود که مفهوم govern به معنای حاکمیت[۵] و جهت‌دهی و کارگردانی[۶]، از ریشه‌ی لاتین gubernare است که صورت متبدل ریشه‌ی یونانی کوبرنتس در زبان لاتین و سپس انگلیسی است (T. F. Hoad, 1996). این مفهوم در ریشه‌ی یونانی کوبرنائو یا کیورنائو[۷]، به معنای «سر برای، رأس برای»[۸] (Beekes & van Beek, 2010) و به‌صورت استعاری، به‌معنای فرمانداری[۹] و حاکمیت[۱۰] و نیز هدایت و راه‌نمایی[۱۱] (Liddell & Scott, 1996) آمده است. روشن است که به لحاظ ریشه‌شناسی، هر دو مفهوم Cybernetics و Govern، نه فقط به یک ریشه باز می‌گردند، بلکه به‌لحاظ معنایی نیز کاربرد مشترک جدی دارند.

۲.۳ ریشه‌شناسی جبر

جبر را به‌معنای زورمند و قوی گفته‌اند و در ریشه‌ی واژه‌ی Gabriel معتقدند که بخش آغازین آن از واژه‌ی عربی «جبر» به معنای مرد جوان قوی و جبار به معنای زورگو گرفته شده است و ریشه‌ی آن در زبان آکدی به gapru به‌معنای قوی، و در اتیوپیایی به gabara به معنای «او عمل کرد» و در عبری به gibbor به معنای «قوی، نیرومند و زورمند» می‌رسد (Klein, 2003). در زبان عبری، واژه‌ی «gevar - גבר» به معنای «قوی، مرد» آمده است (Brown & Robinson, 1975). در آرامی نیز، دلالت بر معانی قاهر مطلق، عظیم، صورت فلکی اریون (در عربی جبار) و شاه برای این مفهوم ذکر شده است (Koehler & Baumgartner, 2000). در قدیمی‌ترین لغت‌نامه‌های زبان عربی، جبر به معنای «تَجْبُر إنسانا على ما لا يريد و تُكْرِهه» یعنی «واداشتن انسان به کاری که نمی‌خواهد و اکراه دارد»، گفته شده است (الفراهيدي، ۱۳۹۱). در لغت‌نامه‌ها، جبر را مقابل کسر (به معنای شکستن) و به‌معنای بستن، گفته‌اند که به‌طور خاص، به معنای بستن استخوان‌های شکسته به هم، گفته شده است (صاحب‌بن‌عباد، ۱۳۹۱) و پیداست که جا انداختن و بستن استخوان شکسته، در دوران گذشته، علاوه بر دانش خاص، نیاز به زور و توان زیادی برای حرکت دادن و در محل خود قرار دادن استخوان‌ها داشته است.

---

[3] Steersman
[4] Steer
[5] Rule
[6] Direct
[7] κυβερναώ
[8] Head for
[9] to govern
[10] rule
[11] Guide

علاوه بر این، جبر در واژه‌ی جبرئیل به‌معنای مرد، جبار به معنای مَلِک (شاه) گفته شده است و علاوه بر این، برای بیان معنای نجار به دلیل اینکه چوب‌ها را وامی‌دارد که کنار هم قرار بگیرند و چیزی ساخته شود، از عبارت «یَجْبُر» استفاده شده است. به‌صورت کلی، در مدخل «جبر» در لغت‌نامه‌های متعدد زبان عربی مانند «تاج العروس من جواهر القاموس»، «لسان‌العرب» و «مجمع البحرین» موجود در نرم‌افزار کامپیوتری جامع‌الأحادیث، دلالت معنایی جبر در ابواب مختلف بر معانی رایجی همچون قهر، سلطه، تکبر، تعظم، مَلِک (شاه)، مرد، شجاعت، قوت و حکومت و عدم اختیار گفته شده است (جامع‌الأحادیث ۵.۳، ۱۳۹۱). لذا سه معنای مشخص «واداشتن به کاری خلاف اراده»، «حاکمیت، فرمانروایی و اعمال نیرو و قدرت» و «کنار هم گذاشتن و هماهنگ کردن اجزایی در کنار هم به یک هدف خاص»، به‌صورت غالب در ریشه‌ی جبر وجود دارد و علاوه بر این، یک معنای «مردی و مذکریت» نیز در آن نهفته است.

یکی از مفاهیم نزدیک به مفهوم جبر، «جبرن» است که به لحاظ شکلی نیز شبیه کوبرن است. جبرن در لغت‌نامه‌ها، ریشه‌ی مفهوم جبرین (با تفاوت‌های لفظی اعرابی) گفته شده است که صورت متغیر واژه‌ی جبریل و جبرئیل خوانده شده است و در برخی منابع، به شهری کهن در منطقه‌ی الخلیل به نام بیت‌جبرین نسبت داده شده که هم نسبتی با جبرئیل دارد و هم آن عبارت «قوماً جبارین» قرآن کریم، به آن بازگشت داده شده است. در تلمود این نام به‌صورت بت‌گوبرین (بت‌جوبرین) آمده است و آنجا را خانه و جایگاه جبرئیل نیز گفته‌اند (سعیدی، ۱۳۹۹). طبق آنچه در سوره‌ی مائده، آیات ۲۰ تا ۲۵ آمده است، هنگامی که حضرت موسی، قومش را از مصر به أرض موعود می‌کوچاند، آنها به او می‌گویند، در این سرزمین، «قوم جبارین» ساکنند و تا آنها خارج نشوند، ما داخل نمی‌شویم. این سرزمین موعود، شرق دریای مدیترانه است و سرزمین کهن یونان، شمال دریای مدیترانه. یونان امروز نیز، شمال غربی دریای مدیترانه است. یونان کهن و باستان، در واقع، بخشی از آسیای صغیر در غرب ترکیه‌ی امروزی (فلات آناتولی)، نزدیک به سرزمین‌های اقوام کاریایی و لیدیایی بوده است که امروزه، شمال دریای مدیترانه است و به‌لحاظ تاریخی، جغرافیای پیرامون دریای مدیترانه، یک جغرافیای راهبردی و پیوسته بوده است که نزدیکی همه‌ی اینها به دریا، استفاده از مفاهیم یکسان را برای مفاهیم نزدیک به هم، توجیه می‌کند.

از منظر حروف نیز می‌توان به هم‌ریشگی این واژه‌ها پرداخت. حرف C در چنین کلماتی، معادل حرف کاپا «κ» در یونانی و برابر حرف «ج» در زبان‌های عربی و فارسی است. این تغییر حرف را در زبان ترکی استانبولی که ریشه در زبان ترکی عثمانی و زبان‌های نیای آن در فلات آناتولی دارد نیز می‌توان دید. امروزه حرف c در زبان ترکی استانبولی که برساخت حرف «ج» در ترکی عثمانی است، به صورت حرف «C» انگلیسی و لاتین نوشته می‌شود اما در تلفظ، ج خوانده می‌شود (مانند cebir که در تلفظ، جبیر خوانده می‌شود). کلمات دیگری نیز وجود دارد که این تغییر در آنها دیده می‌شود؛ به‌طور مثال، مانند مکعب (هم‌ریشه با کعبه) که در فارسی به جعبه، در لاتین به cubus، در یونانی به κύβος (کیوُس یا کیبُس) و در انگلیسی به cube تبدیل شده است.

۳.۳ عبارت‌شناسی

در گفتگوی یکم سقراط با آلکی‌ویادس (Lamb, 1950)، آنجایی که در مورد حاکمیت گفتگو می‌کنند، به‌طور کلی بحث بر سر این است که حاکم بر افراد در حالی حکومت می‌کند که آنها، افراد دیگر را «خرومنون – χρωμένων» می‌کنند. این تعبیر خرومنون را مترجمان به استفاده، ترجمه کرده‌اند یعنی حاکم در حالی بر انسان‌های شهر حکومت می‌کند که آنها انسان‌ها را استفاده می‌کنند. سقراط برای فهم معنای خرومنون، دو مثال می‌زند تا ببیند منظور آلکی‌ویادس چیست: رهبر گروه کر (ارکستر) و کشتیبان یا سکان‌دار کشتی (κυβερνητικὴ) که این هر دو (نوازندگان و قایقرانان)، یک دسته از افراد دیگر را (نوازندگان، رقاص‌ها را و قایقرانان، پاروزنان را) در جهت خاصی و برای انجام کنش خاصی، به‌کار گرفته و هماهنگ می‌کنند؛ و می‌گوید که آیا منظور تو، حکومت بر این افرادی است که هر کدام، یک مجموعه افراد دیگر را به‌کار می‌گیرند (خرومنون می‌کنند)؟ این هر دو نمونه، حاکمیت سلسله‌مراتبی هستند. آلکی‌ویادس رد می‌کند و معنای دیگری درمی‌اندازد. او با طرح دو مفهوم «کینونونتون –κοινωνούντων» و «سیموَلونتون – συμβαλλόντων»، مفهوم ارتباط، اشتراک، مشارکت و جامعه‌ی مسطح را پیش می‌کشد و روشن می‌کند که منظورش، نوعی از روابط اجتماعی است که همه‌ی افراد جامعه، در تعامل با یکدیگر هستند.

سقراط می‌گوید، قبول؛ پس تکنیک حاکمیت و تخنه‌ی آرخین بر همین ملوانان همکار و مرتبط چیست؟ آلکی‌ویادس می‌گوید کوبرنتیک. سقراط می‌پرسد دانش حاکمیت و اپیستمه‌ی آرخین بر آن تعاملات نوازندگان چیست؟ پاسخ می‌شنود که خورودیداسکالیا. سقراط می‌گوید: خب پس نام اپیستمه‌ی ارتباطات همشهریان را چه می‌گذاری و پاسخ می‌شنود: «اِوولیَن –εὐβουλίαν» که به‌معنای مشاوره‌ی خیرخواهانه است و عموماً به شورای خوب/ خیر ترجمه شده است. به نظر می‌رسد که آلکی‌ویادس به دنبال نوعی از حاکمیت غیرسلسله‌مراتبی بر شبکه‌ای از انسان‌های مرتبط است و منظورش از تعبیر «بولیا– βουλία» که در دو صورت «اَوُلیا – ἀβουλία» (شورای شر/ بد) و «اِوولیا – εὐβουλία» (شورای خیر/خوب)، که به شورا ترجمه شده و معنای پارلمان نیز در آن نهفته است، یک حکومت مشورتی است. در این گفتگو، کوبرنتیک، تخنه‌ی آرخه‌ی بر پاروزنان است یعنی آن فن و هنر و تکنیکی که سکان‌دار برای آرخه، اریکه و عرشه‌داری و حاکمیت و اعمال قدرت بر دسته‌ی پاروزنان در جهت هماهنگ کردن آنها استفاده می‌کند، کوبرنتیک نامیده می‌شود. و همین اپیستمه‌ی آرخه‌ی بر خوانندگان گروه کر، خورودیداسکالیک نامیده شده است. دقت به تفاوت استفاده از عبارات تخنه و تکنیک برای کشتی‌بانی و اپیستمه برای رهبری گروه هم‌خوانی و هم‌نوازی، راه‌گشا خواهد بود. سقراط، به آلکی‌ویادس می‌فهماند که در همان شورای خوب هم تکنیک و هنر حاکمیت بر شبکه‌ی ارتباطات انسان‌هایی که همدیگر را استفاده می‌کنند و حکومت بر مردم شهر در حالی که مشغول کار و زندگی و اشتغالات یکدیگر هستند، کوبرنتیک است.

مفهوم سایبرنتیک در دوران جدید، برای نخستین بار توسط آندره ماری آمپر[۱۲]، فیزیک‌دان و ریاضی‌دان فرانسوی، در سال ۱۸۳۴ میلادی در کتابی با عنوان فلسفه‌ی علم[۱۳]، این مفهوم را در صورت cybernetique،

[12] André-Marie Ampère
[13] Essai sur la philosophie des sciences, ou, Exposition analytique d’une classification naturelle de toutes les connaissances humaines

به‌عنوان «حکومت سیاسی مردم[۱۴]» (Stanley-Jones & Stanley-Jones, 1960) و «دانش حکومت مدنی[۱۵]» استفاده کرده و گفت: «علم حکومت در آینده، باید سایبرنتیک نامیده شود» (Tsien, 1954). مبتنی بر همین زمینه‌ی تاریخی این مفهوم، نوربرت ویه‌نر[۱۶] در سال ۱۹۴۸ میلادی، صورت cybernetics این مفهوم را برای عنوان کتاب خود، برگزید. قصد ویه‌نر از این کار، طرح دانش جدیدی به نام سایبرنتیکز با محوریت مطالعه‌ی تطبیقی غالباً ریاضی «کنترل و ارتباط در حیوان و ماشین»[۱۷] و تبیین مکانیسم حاکمیت و حکومت در دستگاه‌های مکانیکی بود (Wiener, 1948). در مورد مفهوم کنترل که ویه‌نر، آن را از جنس ارتباطات فهم می‌کند، گفتنی است که از ترکیب دو ریشه‌ی contra به معنای ضد[۱۸] و مخالف[۱۹]، و rotulus به‌معنای گشتن و گرداندن[۲۰]، به‌دست آمده است (T. F. Hoad, 1996) و با توجه به این ریشه‌شناسی، کنترل یعنی بازگرداندن؛ یعنی نظارت مستمر و مدام بر یک محرک و بازگرداندن آن به مسیر، به محض انحراف از راه؛ یعنی شیء یا شخص را بر خلاف راهی که می‌خواهد برود، به جهتی دیگر جهت دادن (خلاف میلش).[۲۱]

کمی بعدتر و در سال ۱۹۶۰ میلادی، دو پژوهش‌گر حوزه‌ی پزشکی و فیزیولوژی به نام دی. استنلی‌جونز و ای. استنلی‌جونز در کتابی به نام «کیبرنتیکزِ سیستم‌های طبیعی: مطالعه‌ای بر الگوهای کنترل»، با تأکید بر تفاوت املایی منظور خود از این مفهوم با مفهوم مدّ نظر ویه‌نر و استفاده‌ی از حرف k به جای حرف c در آغاز این واژه و با بیان اینکه سایبرنتیکز، در منظر ویه‌نر، به‌تبع مطالعات ماری آمپر، به‌عنوان دانش جدید حکومت ماشین‌ها به‌کار رفته است، نوشتند: «ما Kybernetics را مبتنی بر زمینه‌ی ریشه‌شناسانه‌ی آن، ظاهراً شبیه اما متفاوت از دانش هویتی حکومت در ساختارهای زنده، عرضه می‌کنیم» (Stanley-Jones & Stanley-Jones, 1960). به‌نظر می‌رسد که در نگاه استنلی‌جونز، رویکرد کیبرنتیک به مسائل مشخصی در زیست‌شناسی، کاملاً غیرریاضی است و بر همین مبنا، مفاهیم حوزه‌ی سایبرنتیک مانند تئوری اطلاعات، کانال‌های ارتباط، آنتروپی و برخی مفاهیم دیگر، حذف شده و مفاهیمی مانند بازخورد مثبت و منفی، نوسان، پایداری و ... موضوعیت می‌یابند.

نوربرت وینر، ریاضیدان یهودی آمریکایی، کتابی دارد به نام «استفاده‌ی انسانی از انسان‌ها: سایبرنتیک و جامعه» که در آن، گویا با نظر به مکالمه‌ی آلکی‌ویادس و ارسطو، مفهوم سایبرنتیک را بیشتر از کتاب پیشینش، شرح کرده است. اینجا برای عبارت‌شناسی دقیق مفهوم سایبر، بخشی از متن نوشته‌ی وینر، مستقیماً نقل قول خواهد شد. او در بیان تاریخ سایبرنتیک، با تأکید بر اینکه پس از جنگ جهانی دوم، نظریه‌ی پیام‌ها، دامنه‌ی بسیار گسترده‌ای از دانش‌ها و عرصه‌های علمی مانند مطالعه زبان، مطالعه پیام‌ها به عنوان ابزار کنترل ماشین‌آلات و جامعه، توسعه‌ی ماشین‌های محاسباتی و سایر خودکارها، تأثیرات جدی بر روانشناسی و مطالعه‌ی سیستم عصبی و حتی نظریاتی در روش علمی را در بر می‌گرفت، می‌گوید (Wiener, 1989): «تا

[14] Political Government of People
[15] Science of Civil Government
[16] Norbert Wiener
[17] Control and Communication in the Animal and the Machine
[18] Counter
[19] Opposite
[20] Roll

[۲۱] در ادبیات دینی، مرتبط به این معنا، مفهوم هدایت و إهداء (در نسبت با صراط مستقیم) طرح می‌شود.

همین اواخر، هیچ عنوانی برای همه‌ی این مجموعه‌ی ایده‌ها وجود نداشت، و من برای اینکه کل این عرصه را با یک اصطلاح فراگیر بشناسانم، یک عنوان ابداع کردم: سایبرنتیکز[۲۲] که از واژه‌ی یونانی کوبرنتس[۲۳] یا «کشتی‌بان[۲۴]» مشتق شده است، یعنی همان واژه‌ی یونانی که در نهایت «فرمان‌دار[۲۵]» را نیز از آن گرفته‌ایم. اتفاقاً بعداً متوجه شدم که این عبارت، قبلاً توسط آمپر برای ارجاع به «علم سیاسی[۲۶]» و نیز توسط یک دانشمند لهستانی، در زمینه دیگری، هر دو در اوایل قرن نوزدهم، استفاده شده است. ... من در ارائه تعریف سایبرنتیک در کتاب قبلی، ارتباطات و کنترل را با هم طبقه‌بندی کردم. چرا این کار را کردم؟ وقتی من با شخص دیگری ارتباط برقرار می‌کنم، پیامی را به او می‌رسانم، و وقتی با من ارتباط برقرار می‌کند، پیامی مرتبط را برمی‌گرداند که حاوی اطلاعاتی است که اساساً برای او قابل دسترسی است و نه برای من. از سوی دیگر، وقتی من اقدامات شخص دیگری را کنترل می‌کنم، پیامی را به او می‌رسانم (ارتباط می‌دهم)، و اگرچه این پیام در حال امری است، تکنیک ارتباط با یک پیام واقعی، تفاوتی ندارد. علاوه بر این، اگر قرار است کنترل من مؤثر باشد، باید به هر نحو، از پیامی که نشان‌دهنده‌ی فهمیده‌شدن و اطاعت دستور است، مطلع بشوم. تز این کتاب این است که جامعه را تنها با مطالعه‌ی پیام‌ها و تجهیزات ارتباطاتی متعلق به آن، توسعه آینده‌ی این پیام‌ها و امکانات ارتباطاتی، پیام‌های بین انسان و ماشین‌ها، بین ماشین‌ها و انسان و بین ماشین و ماشین که مقدر شده است تا نقشی فزاینده ایفا کنند، می‌توان شناخت. وقتی من به یک ماشین، دستور می‌دهم، وضعیت ذاتاً با وقتی که به یک شخص انسانی دستور می‌دهم، تفاوتی نمی‌کند ... بنابراین تئوری کنترل در مهندسی، چه انسان یا حیوان یا مکانیکی، بخشی از نظریه‌ی پیام‌ها است. طبیعتاً تفاوت‌های جزئی در پیام‌ها و مشکلات کنترل، نه تنها در ارتباط بین یک ارگانیسم زنده و یک ماشین، بلکه در ارتباط بین هر طبقه‌ی محدودتری از موجودات نیز وجود دارد. هدف سایبرنتیکز، توسعه‌ی زبان و تکنیک‌هایی است که ما را به‌صورت کلی برای هجمه به مسئله‌ی کنترل و ارتباطات، توانمند می‌کنند؛ بلکه مخزن مناسبی از ایده‌ها و تکنیک‌ها را برای طبقه‌بندی نمودهای خاص آن‌ها تحت مفاهیم خاص پیدا کنیم. فرمان‌هایی که ما از طریق آنها، کنترل خود را بر محیط خود اعمال می‌کنیم، نوعی از اطلاعات هستند که به آن ابلاغ کرده و می‌رسانیم».

۴ نتیجه‌گیری

مسیر ریشه‌شناسی مفهوم سایبرنتیکز تا یونان، مسیر واحد و مقبولی است که کسی در آن تردید نکرده است. اما نکته‌ی مهم در این است که این مفهوم، پیش از آن چه سیری داشته است. در این پژوهش، تلاش شد تا با استفاده از روش زبان‌شناسی تاریخی، شواهدی برای امتداد ریشه‌شناسی این واژه به مفهوم جبر در زبان‌های پیشین، ارائه شود. پس با کنار هم قرار دادن محورهای مفهومی زیر در ریشه‌شناسی و عبارت‌شناسی، که پیش

[22] Cybernetics
[23] kubernetes
[24] steersman
[25] Governor
[26] Political Science

از این تشریح شدند، هم‌ریشگی دو مفهوم سایبر و جبر، طرح می‌شود:

۱. آشکار بودن معنای حاکمیت، حکمرانی و اعمال قدرت و اراده در سایبر و کوبرنتس و هم‌ریشگی آن با مفهوم Govern

۲. آشکار بودن معنای حاکمیت، حکمرانی و اعمال قدرت و زور در مفهوم جبر و شکل‌گیری مفاهیمی همچون جبار و اجبار

۳. آشکار بودن معنای هماهنگ‌سازی اجزاء و اعضا در سایبر به عنوان کنش مشخص کشتی‌بان در هماهنگ‌کردن پاروزنان

۴. آشکار بودن معنای هماهنگ‌سازی اجزاء و اعضا در جبر به عنوان کنش مشخص شکسته‌بندی و نجاری در هماهنگ کردن استخوان‌ها یا قطعات چوب

۵. وجود نمونه‌های دیگری از تبدیل حرف «ج» به «کاپا» در یونانی و سپس «C» در لاتین و ترکی

۶. نزدیکی جغرافیایی سرزمین‌های فلسطین، فلات آناتولی (ترکیه امروزی)، یونان باستان (دولت‌شهر یونان) به عنوان سرزمین‌های نیای زبانی زبان یونانی

با استناد به این شواهد، مدعای این پژوهش آن است که جبر و سایبر هم‌ریشه هستند و بنابراین ترجمه مناسب و شفاف فضای سایبر، فضای جبر است. این ترجمه، بدان معناست که اراده‌ی معطوف به سایبر، اراده‌ی معطوف به جبر است اما نه با کارکرد اجبار و اکراه بیرونی و فیزیکی بلکه جبر درونی. از آنجایی که سایبرنتیک، تکنیک کنترل از طریق ارتباطات است؛ و ارتباط، واجد دو سطح اتصالات و سطح اطلاعات است، پس اگر شبکه‌ای وجود داشته باشد که همه‌ی انسان‌ها به آن متصل باشند، آنگاه از طریق مدیریت انتشار اطلاعات در آن اتصالات، می‌توان آنها را از درون، کنترل و جهت‌دهی کرد به‌نحوی که آنها احساس آزادی و اعمال اراده داشته باشند؛ این ایده‌ی بنیادین دانش سایبرنتیک است. جان دانش سایبرنتیک، ارتباطات و به دنبال آن، کنترل است، یعنی نحوه‌ی انتقال فرمان و أمر از فرمان‌ده به فرمان‌بر؛ یعنی چگونگی انتقال فرمان از سکان (سکان‌دار، کشتی‌بان) به کشتی. این فرایند در سیستم مکانیکی، مکانیسم نام دارد و در سیستم‌های الکتریکی باید آن را الکتریسم نام داد. جبران (نزدیک به کوبرن)، از باب فُعلان و به معنای اوج جبر است. جبر به معنای واداشتن دیگران به انجام کارهایی یا بازداشتن آنها از انجام کارهایی است که من می‌خواهم. جبر می‌تواند در دو صورت اطاعت (انجام خودخواسته‌ی کار) و اکراه (انجام ناخودخواسته‌ی کار) محقق شود. از این منظر، جهان سایبر، جهان فاعلیت نیست، جهان آمریت است.

انسان می‌خواهد از سوژگی فاعلیت به سوژگی آمریت برسد. از عاملیت آفاقی به عاملیت أنفسی. می‌خواهد با تصرف در درون انسان، او را به کار وادارد که این تصرف، این یک تصرف زنانه است؛ در تشریح آن باید گفت، وقتی کسی به شما می‌گوید آن لیوان را بده و شما لیوان را به او می‌دهید، سوژه‌ی فاعل، شما هستید اما سوژه‌ی آمر، آن شخص است. انسان مدرن، در طرح و درانداختن جهان سایبر، می‌خواهد مقام خودش را

از سوژه‌ی فاعل در جهان، به سوژه‌ی آمر، ارتقا دهد. می‌خواهد از این پس، امر کند نه فعل؛ و بقیه فعل را انجام دهند. امر کردنش هم امر آفاقی نیست، امر أنفسی است. جهان سایبر، جهان امارت أنفسی است و نه أمارت آفاقی که از طریق درون انسان، به او امر می‌کند، صورتی از اجبار اطاعی و خودخواسته. اجبار در فهم بشر، همواره با اکراه همراه بوده است اما در صورت نوین جبر که در جهان سایبر آشکار شده است، انسان تن به اجبار همراه با اطاعت (به معنای خودخواسته و در مقابل اکراه) داده است؛ گویی نفس انسان به او بگوید فلان کار را بکن. صاحبان سایبر می‌خواهند به مقام نفس أماره برسند و از موضعی جبروتی، اعمال قدرت بکنند. در این صورت، انسان با صورت جدیدی از جبر و اجبار، مواجه و آشنا خواهد شد.

مراجع

[۱] الفراهيدي، ا. ب. أ. (۱۳۹۱). کتاب العین مندرج در نرم‌افزار کامپیوتری جامع‌الاحادیث ۳٫۵. قم: مرکز تحقیقات کامپیوتری علوم اسلامی.

[۲] جامع‌الأحادیث ۳٫۵. (۱۳۹۱). قم: مرکز تحقیقات کامپیوتری علوم اسلامی.

[۳] سعیدی، ع. (۱۳۹۹). بیت جبرین. دائرة المعارف بزرگ اسلامی، وب‌سایت: https://cgie.org.ir/fa/article/229232

[۴] صاحب‌بن‌عباد. (۱۳۹۱). المحیط في اللغة مندرج در نرم‌افزار کامپیوتری جامع‌الاحادیث ۳٫۵. قم: مرکز تحقیقات کامپیوتری علوم اسلامی.

[5] Beekes, R., & van Beek, L. (2010). Etymological Dictionary of Greek. https://doi.org/10.1108/09504121011091114

[6] Brown, F., & Robinson, E. (1975). A Hebrew and English Lexicon of the Old Testament: With an appendix containing the Biblical Aramaic, based on the lexicon of William Gesenius (p. 50). p. 50. Oxford: Clarendon Press.

[7] Durkin, P. (2006). Etymology (K. B. T.-E. of L. & L. (Second E. Brown, Ed.). https://doi.org/https://doi.org/10.1016/B0-08-044854-2/00423-5

[8] Klein, E. (2003). Kleins Comprehensive Etymological Dictionary of the English Language. Amsterdam,: Elsevier Publishing Company.

[9] Koehler, L., & Baumgartner, W. (2000). The Hebrew and Aramaic Lexicon of the Old Testament (M. E. J. Richardson, Ed.). Leiden: BRILL.

[10] Lamb, W. R. M. (1950). Plato. Vol. VIII. Charmides, Alcibiades I and II, Hipparchus (etc) with an English Translation By W. R. M. Lamb. London: WILLIAM HEINEMANN LTD.

[11] Liddell, H. G., & Scott, R. (1996). A Greek-English Lexicon (10th ed.). Oxford University Press.

[12] McMahon, A. (2001). Historical Linguistics: Overview (N. J. Smelser & P. B. B. T.-I. E. of the S. & B. S. Baltes, Eds.). https://doi.org/https://doi.org/10.1016/B0-08-043076-7/03049-7

[13] Stanley-Jones, D., & Stanley-Jones, K. (1960). The Kybernetics of Natural Systems: A Study in Patterns of Control. London: Pergamon Press.

[14] T. F. Hoad. (1996). The Concise Oxford Dictionary of English Etymology (2nd ed.). Retrieved from https://archive.org/details/conciseoxforddic00tfho

[15] Tsien, H.-S. (1954). Engineering Cybernetics. McGraw Hill.

[16] Wiener, N. (1948). Cybernetics: Or Control and Communication in the Animal and the Machine. Paris: MIT Press.

[17] Wiener, N. (1989). The human use of human beings: cybernetics and society. In Fifty Key Figures in Cyberpunk Culture. https://doi.org/10.4324/9781003091189-51

تبیین فضای سایبری و پیامدهای اجتماعی ناشی از آن در سیاست جنایی ایران

سودا آقامحمدزاده [۱]

[۱] کارشناسی حقوق، دانشگاه آزاد اسلامی، واحد شبستر، ایران
sevda81amzd@gmail.com

چکیده

با توجه به رشد تکنولوژی رایانه‌ای و تحول اطلاعات وهمچنین گسترش ارتباطات در فضای سایبری و متعاقباً سهولت ارتکاب جرایم مرتبط با فناوری‌های نوین، بحث روزآمد شدن و لزوم تدوین قوانین بسیار ضروری است. هدف این تحقیق ارائه راهبردهایی برای پیشگیری از آسیب‌های فضای مجازی است. در این پژوهش که به روش توصیفی-تحلیلی می‌باشد سعی بر آن شد سیاست جنایی ایران در رابطه با فضا و تدابیر پیشگیری از جرم در حوزه پدافند سایبری مورد بررسی قرار بگیرد که یافته‌ها نشان از آن دارد که در زمینه راهبردهای پیشگیری وضعی از آسیب‌های فضای مجازی، ابعاد حذف توجیه‌کننده‌ها، کاهش منافع حاصل از جرم، افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم و افزایش خطرهای مدنظر برای ارتکاب جرم به‌ترتیب بالاترین تا پایین‌ترین میانگین رتبه‌ای تأثیر در پیشگیری از آسیب‌های فضای مجازی را دارند. مهم‌ترین نتیجه این تحقیق، استخراج تدابیری در قالب راهبردهای پیشگیری وضعی برای جلوگیری از آسیب‌های فضای مجازی است که استفاده از آنها می‌تواند تاثیر زیادی در پیشگیری از آسیب مجازی، کاهش جرایم، حبس‌زدایی، و غیره داشته باشد.

کلمات کلیدی: آسیب‌های فضای مجازی، پیشگیری، سیاست جنایی ایران، فضای سایبر.

۱ مقدمه

در عصر حاضر، پیدایش و رشد سریع فناوری‌های رایانه‌ای شبکه محور، تحولات شگرف و دستاوری‌های سترگی را در جهت پیشروی جامعه انسانی به‌سوی قله‌های پیشرفت اجتماعی همراه داشته است. شکل‌گیری و گسترش فضای مجازی بسیاری از حوزه‌ها و ساختارهای کلان از جمله فرهنگ، سیاست و اجتماع را دچار تغییرات بنیادین کرده است به‌گونه ای که امروزه با مفاهیم جدیدی همانند جامعه مجازی، سیاست فضای مجازی و فرهنگ دیجیتال مواجه هستیم و فهم ما از جهان واقعی، منهای درک جهان مجازی میسر نیست (عاملی، ۱۳۸۶: ۴۵). گفتنی است که در فضای مذکور به تعامل افقی و متکثر شدن ارتباطات کمک کرده است و فناوری‌های نوین در سایه ارتباطات افقی اینترنت و شبکه‌های ارتباطی موبایل، فرایندهای ارتباطی

عمدتاً خودگردانی را میسر ساخته‌اند که کنترل آنها با بروکراسی دولتی دشوار است (کاستلز، ۱۳۹۶ :۱۲). ناگفته نماند بی‌تردید، عمده‌ترین دلیل شکل‌گیری این دنیای جدید (فضای سایبری)، رهایی از این قالب خاکی بوده است که محدودیت‌ها و موانع، بشر را بر آن داشت تا به آرمان خود که دستیابی به دنیای بی‌مرز است، دست یابد. با این همه، این ارمغان ستودنی در کنار امتیازات بی‌همتایی که دارد، گستره‌ی بی‌پایانی از فرصت‌های منحرفانه و مجرمانه را فراهم آورده است که نه‌تنها بزهکاران را بر شیوه‌های جدید ارتکاب جرم توانمند ساخته است، بلکه افرادی را که بیشتر منحرف نبودند را نیز به رفتارهای مجرمانه واداشته است (ویلیامز، ۱۳۹۱: ۴۶). فضای مجازی با توجه به قابلیت‌ها و ظرفیت‌های ویژه خود ماهیتی دوگانه دارد که گرچه مانند ظرفی برای تبلور اندیشه و عمل کاربران می‌نماید، مختصات و ویژگی‌های منحصر به‌فرد آن را نمی‌توان نادیده گرفت. به‌دلیل وجود همین ماهیت دوگانه، حذر از آسیب‌ها و آفت‌های فضای مجازی دشوار است. با وجود تمهیدات گوناگون و ظرفیت‌سازی گسترده‌ای که برای رشد، بالندگی و حاکمیت فرهنگ اسلامی-ایرانی در محیط مجازی اندیشیده شده، متاسفانه در حال حاضر فضای مجازی با آسیب‌های فراوانی در حوزه اخلاق، فرهنگ، مذهب و ادب فردی و اجتماعی مواجه است؛ به‌گونه‌ای که پیوسته امنیت روانی والدین و اولیای امور جامعه را نسبت به ورود و استفاده کاربران جوان آسیب‌پذیر و متزلزل کرده است (شاه محمدی، ۱۳۹۵: ۱۰۲).

۲ روش تحقیق

روش تحقیق در این پژوهش توصیفی- تحلیلی می‌باشد و در این راستا از منابعی چون کتاب‌ها، اسناد، مدارک و مقالات جهت اخذ داده‌های خام استفاده خواهد شد. روش گردآوری اطلاعات به‌صورت کتابخانه‌ای بوده و با مراجعه به کتابخانه‌های عادی و دیجیتالی (الکترونیکی) انجام یافته است. ابزار گردآوری اطلاعات فیش‌برداری از نوشته‌ها و اسناد و متون حقوقی مرتبط (کتب علمی، تخصصی، مقالات علمی-پژوهشی و غیره) و استفاده از سایت‌های مختلف حقوقی می‌باشد. روش تجزیه و تحلیل اطلاعات که در واقع نحوه‌ی آزمون فرضیه‌های تحقیق است. توصیفی-تحلیلی می‌باشد و با استفاده از طریق استدلال حقوقی مثل برهان عادی و برهان خلف یا وحدت ملاک و نظایر آن خواهد بود.

۳ مفاهیم و ادبیات نظری

در این قسمت به برخی از مفاهیم و ادبیات نظری می‌پردازیم:

۱.۳ مفهوم فضای سایبری

سایبری در زبان انگلیسی پیشوند و در زبان فارسی پسوندی است که به کلمات جدید و امروزی متصل می‌شود تا به آنها معنا و مفهوم دهد به‌گونه‌ای که مرتبط با فضای رایانه یا برخط باشد. سایبر از کلمه "Cyberspace" مشتق شده است که به مطالعه مکانیزم‌های مورد استفاده در کنترل و تنظیم سیستم‌های پیچیده اعم از انسان یا ماشین اطلاق می‌شود (عالی پور، ۱۳۹۳: ۲۹). فضای مجازی (فضای سایبری) عبارت است از مجموعه

ارتباطات درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی. به‌عبارتی، فضای مجازی فضایی است که در آن فعالیت‌های مختلف در ابعاد داده‌ورزی و اطلاع‌رسانی، ارتباطات و ارائه خدمات، مدیریت و کنترل از طریق سازوکارهای الکترونیکی و مجازی صورت می‌پذیرد (صدری و کروبی، ۱۳۸۴: ۵۸). بنیان فضای سایبری که بر استفاده از شبکه جهانی وب به‌منزله یکی از فضاهای قدرتمند حاضر در فضای واقعی مجازی استوار است، کاربردی وسیع یافته و به‌علت سهولت استفاده، صرف نظر از کلاهبرداری‌های صورت گرفته و استفاده‌های نادرست، باعث جذب بسیاری از محققان و پژوهشگران شده است. ناگفته نماند که واژه سایبر را به مجازی ترجمه کرده‌اند. این واژه از لغت سکاندار یا راهنما گرفته شده است و نخستین بار توسط ویلیام گیبسون نویسنده داستان‌های علمی- تخیلی در کتاب نورومنسر به‌کار برده شد. سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده یا یک فضا که مربوط به دنیای رایانه و اطلاعات است. امروزه فضای سایبر دارای معانی متعددی است، از جمله اینکه ترکیبی است از ده‌ها هزار رایانه به هم پیوسته، سرویس‌دهنده‌ها، شبکه‌های ارتباطی، سوئیچ‌ها وکابل‌های فیبرنوری که امکان ایجاد ارتباطات را در یک سامانه جامع فراهم می‌آورد (افتخاری، ۱۳۸۲: ۵).

۲.۳ مفهوم آسیب

واژه آسیب در لغت نامه دهخدا به معنی زخم، کوب و ضرب بیان شده است. این واژه معانی دیگری نیز دارد مانند: صدمه، عیب و نقص یا شکستگی که از زخم و ضرب پیدا آید. جرح، خستگی، مصیبت و ... . در معنای اصطلاحی و عرفی در دایرةالمعارف علوم اجتماعی آمده است: هر پدیده نامطلوب و مضر در سلامت جامعه (نظیر جنایت، جرم و ارتشا) را آسیب اجتماعی می‌نامند. مفهوم آسیب‌شناسی از علوم زیستی گرفته شده است. یعنی مطالعه بی‌سامانی‌ها و آسیب‌های اجتماعی مانند فقر، بیکاری، تبهکاری و غیره همراه با علل و شیوه‌های درمان آنان و همچنین شرایط بیمارگونه و نابهنجار را آسیب اجتماعی گویند (ساروخانی، ۱۳۷۰).

۳.۳ مفهوم آسیب اجتماعی

آسیب اجتماعی به هر نوع عمل فردی یا جمعی اطلاق می‌شود که در چارچوب اصول اخلاقی و قواعد عمل جمعی رسمی و غیررسمی جامعه محل فعالیت قرار نمی‌گیرد و در نتیجه قانونی ویا قبح اخلاقی و اجتماعی روبه‌رو می گردد. به همین دلیل، کجروان سعی دارند کجروی‌های خود را از دید ناظران قانون، اخلاق عمومی و نظم اجتماعی پنهان نمایند. زیرا در غیر این صورت با پیگرد قانونی، تکفیر اخلاقی و طرد اجتماعی مواجه می‌شوند (عبدالهی، ۱۳۸۱). در واقع آسیب‌شناسی اجتماعی، مطالعه ناهنجاری‌ها و نابسامانی‌های اجتماعی نظیر بیکاری، فقر، اعتیاد، خودکشی، ولگردی، زورگیری و غیره همراه با علل و شیوه‌های پیشگیری و درمان آنها و نیز شرایط بهینه اجتماعی است.

۴.۳ سوابق تحقیق

الف: جلالی (جلالی فراهانی، ۱۳۸۴) در مقاله‌ای، ضمن مرور جرایم سایبر و پیشگیری وضعی از جرم، پیشگیری وضعی از جرایم سایبر را در قالب تدابیر محدودکننده یا سلب‌کننده دسترسی، تدابیر نظارتی، تدابیر

صدور مجوز و ابزار ناشناس‌کننده و رمزگذاری مطرح می‌کند. در تحقیق جلالی با وجود ارائه راهکارهایی برای پیشگیری وضعی از جرایم سایبر، نظر کارشناسان درباره این راهکارها اخذ نشده است.

ب: تقی‌زاده و اشترایه (۱۴۰۰) در مقاله‌ای با عنوان «بازشناسی فضای سایبری و تدابیر پیشگیرانه آن در سیاست جنایی ایران» آورده است که: اولین گام برای تحقق عدالت کیفری، پیشگیری از جرم است. باتوجه به رشدتکنولوژی رایانه‌ای وتحول اطلاعات و همچنین گسترش ارتباطات در فضای سایبری و متعاقباً سهولت ارتکاب جرایم مرتبط با فناوری‌های نوین، بحث‌روزآمد شدن و لزوم تدوین قوانین بسیار ضروری است. از طرفی جهانی بودن فناوری اطلاعات و ارتباطات اینترنت نشان از فراملی بودن جرم سایبری دارد. به‌همین دلیل برای پیشگیری مؤثر از چنین جرایمی، همکاری به‌موقع و مؤثر بین کشورها ضروری است. بخشی از شیوه‌های مقابله مستلزم ایجاد فرهنگ بهره‌گیری از شبکه‌های اینترنتی، آموزشی و آگاه ساختن افراد جامعه علی الخصوص در محیط خانواده ومحیط‌های آموزشی، رسانه‌ها و همچنین نظارت دائمی سازمان‌ها بر روی سیستم رایانه‌ای و تدابیر امنیتی از جمله حفاظت فیزیکی، حفاظت کارکنان، حفاظت ارتباطات و اطلاعات در مقابله با جرایم سایبری می‌تواند از اهمیت ویژه‌ای برخوردار باشد. اما با توجه به وجود مشکلات در فراروی تدابیر کیفری، سیاست پیشگیری از وقوع این جرایم مناسب‌ترین تدابیر سیاست جنایی است. هدف این تحقیق ارائه راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی است. درمقاله پیش رو که به روش توصیفی- تحلیلی به‌صورت کتابخانه‌ای و ازطریق فیش‌برداری می‌باشد سعی بر آن شده که مباحث پیرامون فضای سایبری از جمله مفاهیم، ویژگی‌ها، آسیب‌ها، شیوه‌ها و تدابیر پیشگیری، و ... مورد بحث و بررسی قرار گیرد که نتیجه آن می‌تواند بهره‌وری بهتر از شبکه رایانه‌ای بوده که متعاقباً درجهت پیشرفت اقتصادی کشور مؤثر خواهد بود (تقی‌زاده و اشترایه، ۱۴۰۰: ۱).

ج: جلالی (۱۳۸۹) در مقاله خود به ابعاد مختلف نظارت همگانی پلیس و سازمان مجازی پلیس در فضای مجازی به‌عنوان یکی از عوامل مؤثر در پیشگیری جرایم در فضای مجازی پرداخته است. هر چند دیدگاه‌های خوبی در این مقاله مطرح شده است، اما این دیدگاه‌ها اعتبارسنجی نشده است.

۴ شیوه‌های پیشگیری

در این مقاله دو عنوان کلی پیشگیری اجتماعی و پیشگیری وضعی را مورد بررسی قرار می‌دهیم.

۱.۴ پیشگیری اجتماعی

پیشگیری اجتماعی مجموعه اقدامات و تدابیری است که بر خود فرد تأثیر می‌گذارد و پیش از ارتکاب جرم صورت می‌گیرد. در پیشگیری اجتماعی سعی بر این است که با افزایش آگاهی افراد و تربیت صحیح آنها، به‌ویژه قشر جوان و نوجوان جامعه و همچنین از بین بردن زمینه‌های اجتماعی وقوع جرم، نظیر فقر و بیکاری، انگیزه‌های مجرمانه از مجرمان سلب گردد (نجفی ابرندآبادی، ۱۳۸۲: ۱۲۰۸). شیوه پیشگیری اجتماعی عوامل اجتماعی جرم‌زا و انحراف‌زا در یک جامعه معین را هدف قرار می‌دهد و به دنبال از بین بردن زمینه‌های اجتماعی بروز انگیزه‌های مجرمانه می‌باشد و به دو شاخه پیشگیری اجتماعی جامعه‌مدار و

فردمدار (رشدمدار) تقسیم می‌شود (ذوالقدر، ۱۳۹۰: ۱۰۹). همچنین افراد یک جامعه باید بتوانند مراقب افشای اطلاعات خود در فضای مجازی باشند و عدم اطلاع کافی فرد از اینترنت و قابلیت‌ها و مخاطرات آن، موجب انتشار و افشای اطلاعات خصوصی وی در فضای سایبر می‌شود. با ارائه آموزش‌های لازم می‌توان به افراد جامعه آموخت که به چه شیوه‌هایی احتمال آسیب دیدگی فردی و اجتماعی در مقابل فعالیت‌های مجرمانه سارقان اینترنتی را کاهش داده و بتوانند خانواده، اموال و حیثیت اجتماعی خود را تا حدّ زیادی از چنین مخاطراتی مصون دارند (معاونت کشف جرایم ناجا، ۱۳۷۹: ۱۰۲). زیرا بزرگ‌ترین آسیب‌پذیری در هر سیستم رایانه‌ای و بزرگترین تهدیدی که متوجه حفاظت رایانه است، خود کاربران می‌باشند و مسائل حفاظتی مرتبط با آنها موضوع گسترده‌ای است که چیزی بیشتر از جلوگیری از سرقت‌های اینترنتی را شامل می‌شود (آیکاو، ۱۳۸۳: ۱۸۱). در نتیجه و با توجه به پیشرفت‌های علمی و صنعتی و تکنولوژی در عصر معاصر، تمامی افراد جامعه اعم از پژوهشگر، معلم، دانش‌آموز و ...، در تمامی سطوح ، به این تکنولوژی‌ها نیازمند هستیم و نمی‌توان فناوری‌های نوین را بدون در نظر گرفتن این عوامل به‌درستی به کار گرفت.

۲.۴ پیشگیری وضعی

پیشگیری وضعی عبارت است از «ایجاد تغییر نظام‌مند و دائمی در محیط ، به‌منظور کاهش فرصت‌های مجرمانه و افزایش خطر ارتکاب جرم». پیشگیری وضعی، رویکردی موقعیت‌مدار داشته و «موقعیت ارتکاب جرم» را یکی از عوامل اساسی جرم محسوب می‌کند و به همین دلیل در صدد از بین بردن موقعیت جرم از طریق برهم زدن عناصر تشکیل‌دهنده موقعیت است (مقیمی، ۱۳۹۱: ۳۸۲). در این روش، با هدف حمایت و تقویت بزه‌دیده بالقوه، اقدام به تغییر وضعیت‌های ماقبل بزهکاری شده و وضعیت فرد یا شرایط بیرونی مانند مکان، زمان و ... به‌گونه‌ای تغییر داده می‌شوند تا از ارتکاب جرم پیشگیری گردد. در حقیقت می‌توان گفت که این شیوه از پیشگیری، متوجه وضعیت «پیش از وقوع جرم» است و تلاش می‌کند فرآیند تبدیل از «اندیشه مجرمانه» به «عمل مجرمانه» قطع شود. در پیشگیری وضعی دو جهت‌گیری اصلی «مداخله در وضعیت پیش از جرم» و «ایمن‌سازی اهداف جرم» وجود دارد که دو هدف عمده را دنبال می‌کنند: یکی دشوار یا ناممکن‌سازی وقوع جرم، در حالی که انگیزه مجرمانه وجود دارد، و دیگری جلوگیری از پیدایش و شدت گرفتن انگیزه مجرمانه (عابدی، ۱۳۸۸: ۲۵-۲۶). با وجود اینکه عملی کردن پیشگیری وضعی در مورد جرایم سایبری بسیار مشکل است، اما باز هم از جایگاه خاصی در سیاست جنایی پیشگیری کشورها برای مقابله با این جرم برخوردار است. یکی از دلایلی که می‌توان جهت توجیه پیشگیری وضعی از جرایم مذکور برشمرد قابلیتی است که فضای اینترنت برای افراد به وجود آورده است. اصولاً جرایم اینترنتی یا سایبری به‌خصوص کلاهبرداری به‌گونه‌ای هستند که علاوه بر ابزارها و لوازم کافی و قصد انجام جرم نیز ضروری است. اما این مسئله بدین معنا نیست که برای ارتکاب این جرایم لزوماً مجرم باید تخصص و مهارت فوق‌العاده‌ای داشته باشد، بلکه اگر وی از دانش ابتدایی برای استفاده از کامپیوتر و اینترنت برخوردار باشد، خود فضای اینترنت امکاناتی را در اختیار وی قرار می‌دهد که زمینه وقوع جرم خود به خود فراهم می‌شود (عطارزاده و انصاری، ۱۴۰۰ :۱۵۴). در نهایت شاید بتوان گفت که هدف تدابیر پیشگیرانه وضعی، سلب فرصت و ابزار ارتکاب جرم از دسترس مجرمان بالقوه می‌باشد. این نوع پیشگیری برخلاف پیشگیری اجتماعی به‌جای

تکیه بر فرد، بر محیط توجه دارد.

۵ بحث و نتیجه‌گیری

با توجه به مطالب مطرح شده در پژوهش حاضر می توان عنوان نمود که جرم در طول زمان‌های مختلف از زمان‌های دور و از خلقت بشر تا بدین روز وجود داشته و جرایم به مرور زمان قابل تغییر بوده و پژوهشگران و نویسندگان از عمل مجرمانه تعریف‌های مختلف ارایه کرده‌اند. هدف‌اصلی ما در پیشگیری از جرایم اعم از کیفری و غیر کیفری تربیت و اصلاح جامعه و افراد حاضر در آن می‌باشد. گفتنی است که برای مقابله همه جانبه و کارآمد باجرایم سایبری و در فضای مجازی و متعاقباً کاهش ارتکاب آن توسط کاربران، استفاده و بکارگیری تمامی شیوه‌های مقابله با جرم به صورت توأمان تأثیرگذار می‌باشد و بایستی قبول نمود که استفاده از یک روش به‌تنهایی از کارآیی لازم برخوردار نخواهد بود و نمی‌توان تنها با یک روش با جرایم سایبری مقابله کرد. به نظر می‌آید پیشگیری از جرم تنها با سرکوبی و اجرای کیفری محقق نمی‌شود، چرا که در سیاست جنایی ایران پیشگیری کیفری عمدتاً ماهیت کیفری دارد و بر عهده قوه قضاییه است. با توجه به این که پیشگیری از جرایم، بر عهده قوه قضائیه است، می‌توان با یک برنامه‌ریزی دقیق و همچنین اصلاح و تدوین قوانین، با نظارت کردن بر این فضا تدابیری اندیشید که مردم به استفاده صحیح از آن رغبت پیدا کنند، لذا اتخاذ تدابیر برای پیشگیری از آسیب‌های فضای سایبری امری ضروری و اجتناب‌ناپذیر است و غفلت از این امر مهم می‌تواند صدمات جبران‌ناپذیری را در ابعاد مختلف از نظر مادی و معنوی بر افراد و کشور از جمله از لحاظ اقتصادی وارد سازد، که پیشگیری وضعی می‌تواند یکی از بهترین روش‌ها برای پیشگیری از جرایم سایبری باشد چرا که این نوع پیشگیری متوجه وضعیت مجرم پیش از وقوع جرم است که به رفتارهای مجرم می‌پردازد و این امر باعث کاهش موقعیت‌ها و ابزار ارتکاب برای سودجویان می‌شود. فلذا به نظر می‌رسد با برنامه‌ریزی و سازمان‌دهی مناسب و با عملکرد و کنترل در برابر این جرایم در فضای سایبری و با آگاه‌سازی جامعه از طریق رسانه‌ها و علی الخصوص در محیط‌های خانواده و آموزشی و ... در برابر این سودجویان می‌توان ارتکاب این جرایم را به حداقل رساند که نتیجه آن می‌تواند کاهش جرایم، حبس‌زدایی، و به دنبال آن از نظر اقتصادی به حداکثر ممکن برسد.

مراجع

[۱] آیکاو، دیوید جی و سیگرو، کارل الف و وان استروچ، ویلیام آ. (۱۳۸۳). راهکارهای پیشگیری و مقابله با جرایم رایانه‌ای، مترجمان اکبر سرگی و دیگران، تهران: دانشگاه علوم انتظامی، معاونت پژوهش، اداره چاپ و نشر.

[۲] افتخاری، اصغر (۱۳۸۲). استراتژی ملی برای تأمین امنیت درفضای مجازی، تهران: پژوهشکده مطالعات راهبردی.

[۳] تقی‌زاده ،امیر و اشترایه، عطیه (۱۴۰۰). بازشناسی فضای سایبری و تدابیر پیشگیرانه آن در سیاست جنایی ایران، سومین کنفرانس ملی پدافند سایبری، دانشگاه آزاد اسلامی مراغه، صص ۱ - ۲۰.

[۴] جلالی فراهانی، امیرحسین (۱۳۸۴). پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر، مجله فقه و اصول، ش ۶.

[۵] جلالی، اکبر (۱۳۸۹). نظارت همگانی عامل پیشگیری جرایم در فضای مجازی، فصلنامه علمی-ترویجی کارگاه، ش ۱۲، دوره دوم.

[۶] حیدرنژاد، کیوان و تقی‌زاده، امیر (۱۴۰۰). سیاست جنایی ایران در پیشگیری از جرایم قماربازی و شرط‌بندی‌های اینترنتی در حوزه پدافند سایبری، سومین کنفرانس ملی پدافند سایبری، دانشگاه آزاد اسلامی مراغه، ص ۱ - ۱۷.

[۷] ذوالقدر، محمد باقر و توکل پور، محمد هادی (۱۳۹۰). مدیریت پیشگیری از وقوع جرم و آسیب‌های اجتماعی، تهران، مرکز مطالعات اجتماعی و جرم‌شناسی معاونت اجتماعی و پیشگیری از وقوع جرم قوه قضاییه.

[۸] زینالی، حمزه (۱۳۸۱). پیشگیری از بزهکاری و مدیریت آن در پرتو قوانین و مقررات جاری ایران، فصلنامه رفاه اجتماعی، سال دوم، شماره ششم، صص ۱۲۴- ۹۷.

[۹] ساروخانی، باقر، (۱۳۷۰) درآمدی بر دایرة المعارف علوم اجتماعی، انتشارات کیهان.

[۱۰] ستوده، هدایت‌الله، (۱۳۸۴). آسیب شناسی اجتماعی، انتشارات آوای نور.

[۱۱] شاه محمدی، غلامرضا (۱۳۹۵). راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی، فصلنامه مطالعات راهبردی ناجا، سال اول، شماره یکم.

[۱۲] صدری، سید محمدرضا و کروبی، محمد تقی (۱۳۸۴). ابعاد حقوقی محیط سایبر در پرتو توسعه ملی، تهران: نشر بقعه.

[۱۳] عالی‌پور، حسن (۱۳۹۳). حقوق کیفری فناوری اطلاعات، چاپ دوم، تهران: انتشارات خرسندی.

[۱۴] عطارزاده، سعید و انصاری، جلال (۱۴۰۰) حقوق جزای اختصاصی جرایم رایانه ای. چاپ دوم، تهران: بنیاد حقوقی میزان

[۱۵] علی‌نژاد ساروکالیی، عارف (۱۳۹۰). سیاست جنایی امنیت محور، پایان‌نامه کارشناسی ارشد دانشگاه آزاد اسلامی تهران مرکزی، به راهنمایی مهرداد رایجان اصلی.

[۱۶] عایدی، محمد (۱۳۸۸). وظایف دولت در پیشگیری از جرم، (در جامعه اسلامی)، قم: نورالسجاد.

[۱۷] عباچی، مریم (۱۳۸۳). رهنمودهای حقوق کیفری ماهوی در قبال کودکان بزه دیده، مجله حقوقی دادگستری، شماره ۵۲ - ۵۴.

[۱۸] عباسی شوازی، محمدتقی و معینی، مهدی و پوردیان، روح الله (۱۳۹۷). فضای مجازی، همنشینی و رفتارهای پرخطر: مطالعه رابطه همنشینی دانشجویان در فضای مجازی با رفتارهای پرخطر در فضای واقعی و مجازی، فصلنامه پژوهش‌های انتظام اجتماعی، سال دهم، شماره سوم، صص ۷۷-۱۰۴.

[۱۹] عبدالهی، م (۱۳۸۱). آسیب‌های اجتماعی و روند تحول آن در ایران، جلد یکم، انتشارات آگه.

[۲۰] عاملی، سعید رضا (۱۳۸۶). دین مجازی؛ دوفضایی شدن محیط دینی و ارتباطات درون‌دینی و بین‌دینی، تهران: انتشارات طرح آینده.

[۲۱] قیاسی، جلال الدین (۱۳۸۵). اصول سهولت و مدارا در ساست جنایی حکومت اسلامی، انجمن معارف اسلامی، ۷(۳)، ۲۵.

[۲۲] کاستلز، مانوئل (۱۳۹۶). قدرت ارتباطات ترجمه حسین بصیریان جهرمی، تهران: انتشارات علمی و فرهنگی.

[۲۳] لازرژ، کریستین (۱۳۹۲). درآمدی برسیاست جنایی، ترجمه علی حسین نجفی ابرندآبادی، چاپ چهارم، تهران، بنیاد حقوقی میزان.

[۲۴] میرخلیلی، سیدمحمود (۱۳۸۸). پیشگیری وضعی از بزهکاری، ناشر: سازمان انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی.

[۲۵] معاونت کشف جرایم ناجا (۱۳۷۹). ابعاد حقوقی جرایم رایانه‌ای، فصلنامه دانش انتظامی، تابستان و پاییز، ش ۲ و ۳، صص ۸۶-۱۰۹.

[۲۶] مقیمی، مهدی و جعفری، سیداصغر (۱۳۹۱). مؤلفه‌های مکانی پیشگیری وضعی و پلیسی از جرم، مجموعه مقالات همایش رهیافت‌های نوین پیشگیری از جرم ، ج ۱، صص ۴۲۶-۳۷۹.

[۲۷] نجفی ابرند آبادی، علی حسین (۱۳۸۱). تقریرات درس جرم‌شناسی، تهران: مجتمع آموزش عالی قم دانشگاه تهران.

[۲۸] نجفی ابرند آبادی، علی حسین (۱۳۸۲). تقریرات درس جرم‌شناسی دوره کارشناسی ارشد، تنظیم: رضا فانی، نیمسال اول سال تحصیلی ۱۳۸۲-۸۳.

[۲۹] نیازپور، امیرحسین (۱۳۹۳). حقوق پیشگیری از بزهکاری درایران، مجله حقوقی دادگستر، شماره ۴۹.

[۳۰] ویلیامز، ماتیو (۱۳۹۱). بزهکاری مجازی؛ بزه، انحراف و مقررات‌گذاری بر خط، ترجمه امیرحسین جلالی فراهانی و مجموعه منفرد، تهران، میزان.

[۳۱] یوسفی، تیمور، شیداییان، مهدی (۱۳۹۹). ارزیابی ساختار پیشگیری از جرم در قوه قضائیه با نگاهی بر آموزه‌های فقهی، مبانی فقهی حقوق اسلامی، دوره ۱۳، شماره ۲۶.

[32] Van den Bulck, H., Puppis, M., Donders, K., & Van Audenhove, L. (Eds.). (2019). The Palgrave handbook of methods for media policy research. London: Palgrave Macmillan.

بررسی نقش و تأثیر قلمروگذاری و مرزبانی فضای سایبری در اعمال حاکمیت بر فضای سایبر ملی

محمدرضا حسینی[۱]، مهراب رامک[۲]، احسان کیان‌خواه[۳]، سید حسین علوی[۴]

[۱] دانشیار گروه مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
rezahsn88@gmail.com
[۲] دکترای تخصصی مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
m.ramak@aut.ac.ir
[۳] دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
e.kiankhah@sndu.ac.ir
[۴] دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی
h.alavi@aut.ac.ir

چکیده

با گسترش روزافزون بهره‌برداری از فناوری‌ها و تجهیزات سایبری در زندگی فردی و اجتماعی انسان‌ها، شاهد توجه بیش از پیش کشورها به پدیده قلمرو سایبر ملی با هدف اعمال حاکمیت و ممانعت از تسلط بیگانگان در فضای سایبری ملی هستیم. این پژوهش با بررسی ادبیات مرتبط با حاکمیت بر قلمرو سرزمینی و چگونگی انطباق اصول و قواع حقوق بین‌الملل مرتبط با حاکمیت ملی بر فضای سایبر ملی به تحقیق پیرامون نقش و جایگاه قلمروگذاری و مرزبانی فضای سایبری در اعمال حاکمیت بر فضای سایبر ملی می‌پردازد. تحقیق حاضر با توجه به هدف، از نوع توسعه‌ای-کاربردی است و روش تحقیق مورداستفاده در این پژوهش توصیفی-تحلیلی است که برای گردآوری اطلاعات، از منابع کتابخانه‌ای و اینترنتی استفاده شده است و سعی شده تا مبانی لازم جهت تبیین موضوع از منابع به روز داخلی و خارجی استخراج گردد. محققین پس از تجزیه و تحلیل اطلاعات نتیجه‌گیری کردند قلمروگذاری و مرزبانی فضای سایبری می‌تواند نقش بسزایی در اعمال حاکمیت بر فضای سایبر ملی داشته باشد و برخورداری از اصول و قواعد حقوق بین‌الملل، پیگیری‌های قانونی و دفاع از فضای سایبر ملی مستلزم تعریف و اعلان قلمرو سایبری ملی و مرزبانی مؤثر این فضا می‌باشد. به‌علاوه تعریف نشدن قلمرو و مرز ملی در فضای سایبری، رفتار قانون‌مند کنشگران خصوصی و دولتی در یک فضای قانونی را به همراه نخواهد داشت و منجر به تضعیف نظام حاکم و امنیت ملی خواهد شد. نتایج حاصل از این تحقیق گسترش دانش و شناخت بهتر تصمیم‌گیران و متولیان امر در کشور را به همراه خواهد داشت.

کلمات کلیدی: اصول و قواعد حقوق بین‌الملل، حاکمیت ملی، قلمرو گذاری و مرزبانی فضای سایبری.

۱ مقدمه

تهدیدات متنوع و روزافزون پیش روی فضای سایبری که به واسطه ماهیت به هم پیوسته این فضا امکان‌پذیر گردیده، موجب شده است ساختارهای اینترنت و فضای سایبری از دهه ۱۹۹۰ میلادی با رشد چشم‌گیری به نفع تمرکز و کنترل بیشتر تغییر نمایند. از این رو دولت ها طی سال‌های گذشته به‌طور مداوم نظارت و کنترل خود برای محافظت از فضای سایبری ملی را افزایش داده‌اند. البته هیچ‌گاه رابطه و مرز بین تمرکز و عدم تمرکز ساختارهای به هم پیوسته فضای سایبری ملی به هیچ وجه آشکار نبوده است. عدم تمرکز به‌دلیل انعطاف‌پذیری و دردسترس بودن ارتباطات و تعاملات در فضای سایبری و تمرکز به واسطه نیازهای کنترل و مراقبت از منابع و منافع ملی سایبری اعمال شده است.

هنگام پیدایش فضای سایبری و اینترنت، بسیاری پیش‌بینی می‌کردند این فضا چالش بزرگی برای حاکمیت ملی (سرزمینی) کشورها ایجاد می‌کند. اما تفسیر های اخیر حاکی از این است که اگر چه فضای سایبری و به‌خصوص رسانه‌های اجتماعی به کنشگران غیردولتی نیز قدرت داده است، ولی دولت‌ها همچنان به دنبال تقویت مواضع و اعمال حاکمیت ملی (سرزمینی) از طریق/ بر فضای سایبری هستند.

همچنان که برخلاف پیش‌بینی برخی صاحب‌نظران مبنی بر کم‌رنگ شدن مرزهای سرزمینی طی سال‌های آتی و مطرح شدن ایده «دنیای بدون مرز»، که منجر به تحولات اساسی در حاکمیت دولت‌ها بر قلمرو سرزمینی ملی می‌گردد؛ موضع‌گیری کشورها در مقابله با انتشار ویروس کرونا و پس از آن سیاست‌های واکسناسیون کووید ۱۹ نشان داد، راهبردهای قلمرو سرزمینی هنوز در سراسر جهان دارای استحکام و در حال استفاده مؤثر هستند. در بهار سال ۲۰۲۰ میلادی کشورها به‌سرعت مرزهای خود را بستند و عبور و مرور انسان‌ها را ممنوع یا حداقل به‌شدت کنترل کردند. حتی در برخی موارد با اجبار، افراد را از قلمرو سرزمینی ملی اخراج نمودند. پس از آن نیز اعمال سیاست‌های واکسناسیون کووید ۱۹ و اولویت شهروندان در زدن واکسن کووید، نشان از تحکیم مبانی سرزمینی داشت. همچنین وضع قوانین و مقررات مهاجرتی در بسیاری از کشورها که طی سال‌های گذشته اعمال گردیده است، نمونه دیگری از راهبرد ملی مبتنی بر صیانت از قلمرو ملی می‌باشد. این شواهد بیانگر اهمیت و جذابیت قلمرو ملی در نظام سیاسی مدرن می‌باشد و به ما یادآوری می‌کند، یک واقعیت عمیق در مورد جهان سیاسی ما این است که جهان دارای دولت‌های سرزمینی مستقل است و دولت‌ها مدعی حقوقی در برابر شهروندان خود و در مقابل بیگانگان هستند و از حق کنترل مستقل بر قلمرو خود برخوردار می‌باشند (Paasi et al., 2022).

از آنجایی که حاکمیت در هر عرصه‌ای از چهار عنصر قلمرو و مرز، شهروندان، منابع و نظام تشکیل می‌گردد، پیش شرط اعمال حاکمیت در فضای سایبر نیز تعریف و تحقق این چهار عنصر می‌باشد. یعنی اینکه افراد، تجهیزات و داده‌های موجود در قلمرو سایبری هر کشور تابع حکمرانی آن کشور بوده و از سوی دیگر هیچ کشوری نباید در فضای سایبر واقع در قلمرو کشورهای دیگر مداخله کند. همچنین تمام کشورها (و دولت به‌عنوان نماینده قانونی حاکمیت) مشروعیت دارند از قلمرو خود در برابر تجاوز محافظت نمایند (کریمی قهرودی محمدرضا و زارعی وحید، ۱۳۹۹). از این رو به‌کارگیری فضای سایبر در شئونات مختلف زیست بشری موجب گردیده است اعمال حاکمیت در فضای سایبر کشورها یکی از ابعاد جدید حاکمیت ملی

و به‌تبع آن قلمروگذاری و مرزبانی این فضا امری ضروری به حساب آید.

هم‌اکنون قلمروگذاری و مرزبانی فضای سایبر ملی به درجات مختلف توسط دولت‌ها اعمال می‌شود و حتی آزادترین کشورهایی که ادعای آزادی عمل و آزادی بیان دارند (مانند ایالات متحده امریکا) قلمرو سایبری کشور را به‌گونه‌ای متفاوت تعیین و مرزهای سایبر ملی را پایش، نظارت و کنترل می‌نمایند. در بسیاری دیگر از کشورها مثل چین و روسیه، با اعمال رویکردهای دولت‌محور که به‌نوعی قلمروگذاری و مرزبانی فضای سایبر ملی محسوب می‌گردد، حاکمیت بر فضای سایبر داخلی را تقویت می‌نمایند. حتی کشورهای دموکراتیک نیز اخیراً از طریق تدوین راهبردهای ملی سایبری با هدف بومی‌سازی داده‌ها، در جهت ارتقاء حاکمیت فضای سایبری ملی (سرزمینی) حرکت کرده‌اند.

به این ترتیب قلمروگذاری و مرزبانی فضای سایبر ملی اولین گام در صیانت از فضای سایبری کشور و همچنین نقش برجسته و مهمی در حاکمیت ملی و پیشگیری از چالش‌های ناشی از فضای سایبری به فضای واقعی کشور دارد.

۲ مفهوم شناسی و ادبیات تحقیق

۱.۲ حاکمیت ملی

قدرت غایی و انحصاری بر قلمرو سرزمینی یک کشور را حاکمیت ملی می‌گویند. بنابراین دولت به‌عنوان بالاترین مرجع حقوقی، از امتیاز اعمال حاکمیت بر قلمرو ملی برخوردار است. صلح وستفالیا با به رسمیت شناختن انحصار اقتدار سیاسی دولت بر قلمرو سرزمینی، به ظهور مفهوم مدرن دولت منجر شد. نظم پیش از وستفالیا به گونه‌ای بود که قدرت لزوما سرزمینی و البته انحصاری نبود و اعمال حاکمیت اغلب با همپوشانی و پیچیدگی همراه بود. چگونگی بروز اقتدار سیاسی نیز از قاعده و اصول خاصی پیروی نمی‌کرد (Douzet, F. 2020).

در ۲۴ اکتبر ۱۶۴۸ با امضای پیمانی موسوم به پیمان وستفالیا، جنگ خانمان‌سوز سی‌ساله در اروپای مرکزی پایان یافت. وستفالیا -منطقه‌ای در شمال غربی آلمان- میزبان این رخدادِ تاریخ‌ساز بود. عهدنامه وستفالیا را یکی از نقاط عطف در تاریخ روابط بین‌الملل می‌دانند. وستفالیا نخستین پیمان صلح چند جانبه پس از رنسانس در اروپا است. این پیمان بعدها منجر به معاهدات بزرگ مشابهی بین کشورها شد که در نهایت به تدوین قانون بین‌الملل انجامید. صلح وستفالیا، الگو و پایه جامعه‌ی ملل و سپس سازمان ملل متحد گردید. این معاهده مرزهای ملی در قاره اروپا را تعیین کرد، استقلال و حاکمیت کشورها را به رسمیت شناخت و نشان داد حاکمیت ملی، قلمرو ملی و استقلال ملی به اصولی تبدیل شده‌اند که باید در روابط بین‌الملل مورد توجه قرار گیرند. در این پیمان حقوق برابر و یکسان کشورها به عنوان واحدهای سیاسی مستقل برای نخستین بار مطرح و مورد پذیرش قرار گرفت. مطابق این پیمان کشورهای مستقل حق تعیین سرنوشت خود را دارند، برابرند و حق دخالت در امور هم را ندارند (کامران دستجردی، حسن، ۱۴۰۱).

فرهنگ جغرافیای انسانی حاکمیت را «ادعایی برای اقتدار غایی و نهایی بر یک جامعه سیاسی» تعریف می‌کند. حاکمیت در حقوق اساسی و در پهنه حقوق عمومی نیز به معنای «قدرت برتر و عالی و صلاحیت

اتخاذ تصمیم نهایی و قدرت جمع‌کننده انرژی‌های سیاسی درون جامعه» تفسیر شده است که دارنده آن می تواند در مسائل قلمرو تحت پوشش امر و نهی کند. حاکمیت ملی (مردمی) یک ابداع قانونی است که این ابداع قانونی دارای قدرت، برای شکل دادن به نهادهاست. استفاده از این برداشت در واقع ناظر بر امور داخلی کشورهاست که حکومت ها بر اساس اختیارات و اقتداری که به طرق دموکراتیک یا دیگر روش های مرسوم در دوران حاضر کسب کرده‌اند، قدرت و سلطه مشروع خود را بر قلمرو ملی و مردم خویش اعمال می‌کنند (بدیعی، مرجان و همکاران، ۱۳۹۹).

با این توضیح حاکمیت از آن رو بعد جغرافیایی می‌یابد که چهره قانونی اعمال اراده حکومت بر سرزمین (قلمرو) و مردمان (ملت) است و مفهوم اجرای قوانین حکومت برای کنترل مردم و سرزمین در محدوده جغرافیایی‌اش را می‌رساند.

اغلب نظریه‌های حاکمیت ملی، «قلمرو» را به عنوان عنصر اساسی حکومت تشخیص می‌دهند و حاکمیت معمولاً مرتبط با یک قلمرو تحدید شده است. در واقع، زمانی که حکومت درون یک متن جغرافیایی قرار می‌گیرد، اولین مشخصه مهم، ویژگی قلمرویی آن است و حکومت از حق تعریف آنچه قانونی است و اجرای قانون درون یک فضای دارای مرز مشخص برخوردار است. مفهوم حاکمیت در مقیاس‌های فضایی گوناگون قابل بررسی است که عبارتند از: فروملی (محلی)، ملی و فراملی. در نگاه کلی‌تر حاکمیت ملی از دو سطح داخلی و خارجی برخوردار است: حاکمیت داخلی به اقتدار مطلق و نهایی دولت بر همه قلمرو افراد، گروه ها، نهادها، و سازمان‌ها در درون مرزها مربوط می‌شود. اما حاکمیت خارجی (فراملی) به رابطه میان دولت مورد نظر با سایر دولت‌ها مربوط می‌شود و مکمل حاکمیت داخلی (ملی) است. به عبارت دیگر حاکمیت خارجی به معنای شناسایی متقابل از سوی دیگر دولت‌ها درون سیستم بین‌دولتی (بین المللی) است.

امروزه بر اساس منشور سازمان ملل متحد، تمام کشورها از حق دفاع از خود در عرصه بین‌المللی، حق استقلال و حق برابری بین‌المللی در حوزه حاکمیت ملی برخوردار هستند. این سه حقوق حاکمیت ملی توسط کشورهای جهان حمایت و اجرا می‌شوند و قلمروگذاری و مرزبانی سرزمینی نقش اساسی در اعمال حاکمیت ملی و برخورداری از حقوق مرتبط بین‌المللی دارد.

۲.۲ قلمرو و مرز

واژه قلمرو ترکیبی از اسم «قلم» و فعل امر «رو» می‌باشد که ظرف مکان و به معنی محل روا بودن قلم کسی و به معنای ملک مطیع است (لغت‌نامه دهخدا، ۱۳۹۲). قلمرو در عرف نشان‌دهنده محدوده مالکیت و حاکمیت یک موجودیت زنده مانند حیوان یا انسان یا گروه و سازمانی از آنها بر یک محدوده جغرافیایی اعم از سرزمین، منابع و منافع مادی آن محدوده است. جانوران برای زندگی و فعالیت های زیستی‌شان، محدوده مشخصی برای خود برمی‌گزینند. حیوانات از رهگذر نشانه‌های ساده بصری، آوایی، چشایی و خواص بویایی مرزهایشان را تعیین، نشانه گذاری (اعلان) و در نگاه‌داشت قلمروشان می‌کوشند. میزان وضوح این نشانه‌ها و اعلان‌ها در فضای مربوطه، به نوعی جدیت و اقتدار بر محدوده قلمرو (مرزها) را القا می‌نماید (بدیعی، مرجان و همکاران، ۱۳۹۹).

واژه قلمرو در جوامع انسانی نیز ناظر به فضای محدود شده‌ای است که افراد و گروه‌ها از آن به عنوان

محدوده اختصاصی، استفاده می‌کنند و در مقابل هر گونه تهاجم و دست‌اندازی بیگانگان از آن محدوده دفاع می‌نمایند. در نتیجه به فراخور وسعت و توان مادی، قلمروهای مختلفی وجود دارد که زمینه بروز کنش‌های متنوعی از همکاری تا جنگ بین ساکنان را در پی دارد. در حوزه رفتار انسان اجتماعی، قلمرو بخشی از سطح زمین می‌باشد که گروهی خاص یا موجودیتی سیاسی مدعی مالکیت و حاکمیت بر آن است. بنابراین، قلمروها نشان دهنده اعمال قدرت بر فضا هستند که در عالی‌ترین سطح در قالب کشور– ملت‌ها سر برآورده اند. امروزه، قلمرو گستره فضایی قدرت یک کشور و منابع مادی تأمین‌کننده آن قدرت است (کاویانی راد، مراد، ۱۳۹۲).

با توضیح ارایه شده، قلمرو در هر عرصه‌ای با ترسیم «مرز» در آن عرصه شکل می‌گیرد و مرزها مهم‌ترین ابزار برای کنترل و محافظت از قلمرو به شمار می‌روند. یعنی ابزار تعیین حدود و کنترل دسترسی به یک قلمرو که به برخی اجازه ورود و از دسترسی برخی دیگر ممانعت به عمل می‌آورد، «مرز» است. در نتیجه مرز نقطه‌ای است که تهدیدات خارجی به واقعیت‌های داخلی تبدیل می‌شود. تحدید مرزها توسط فرآیند قلمروسازی باعث ایجاد یک منطقه خاص می‌شود که در آن قدرت اعمال می‌شود و آن را به یک سرزمین یا فضا تبدیل می‌کند (Medeiros, B. P., & Goldoni, L. R. F. 2020). بنابراین برای شکل‌گیری قلمرو در هر عرصه یا فضایی، ترسیم و تبیین مرزها نقش مؤثری دارد.

در سطح ملی تعیین محدوده قلمرو به عنوان فضایی که دولت ملی در آن مشروعیت داشته و قدرت دولتی در آن به رسمیت شناخته می‌شود بر عهده «مرزهای ملی» است. به عبارت دیگر، مرزهای ملی خطوطی هستند که قلمرو بیرونی حاکمیت یک دولت ملی را تعیین می‌کنند و عاملی برای کشف و جدایی یک سازمان سیاسی واحد از کشورهای دیگر هستند. یعنی مرزها دو ملت، دو کشور و دو دولت را از هم جدا می‌کنند. مدیریت مرزی سازوکاری است که امنیت ملی و تنظیم قانونی ورود و خروج برای تأمین نیازهای مختلف ملت را فراهم می‌نماید. به همین ترتیب برخورداری از اصول و قواعد حقوق بین‌الملل مرتبط با حاکمیت سرزمینی (ملی) و اثبات موارد نقض حاکمیت توسط سایر کشورها، با تعریف و اعلان دقیق «قلمرو ملی» و در امتداد آن «مرزهای ملی» رابطه مستقیم دارد (Tsaugourias, N. 2017).

۳.۲ قلمروگذاری و مرزبانی

قلمروگذاری عبارت است از تلاش یک فرد یا یک گروه برای دستیابی، تاثیرگذاری یا کنترل افراد، پدیده‌ها و روابط، از طریق تحدید حدود و اعمال کنترل بر یک منطقه یا فضای خاص. تعیین قلمرو یک فرآیند است، ساخته و بازسازی می‌شود، شکل گرفته و مدام بروز رسانی می‌شود، یعنی قلمروگذاری یک فرآیند فعال و واکنشی است. به بیان دیگر قلمروها و فضاها به طور طبیعی داده نمی‌شوند، بلکه محصول کنش اجتماعی فعال هستند. با رویکرد بین‌المللی، قلمرو ملی فضایی است که به‌عنوان مبنای حاکمیت یک دولت شناخته می‌شود و دولت ملی در آن مشروعیت و قدرت کنترل بر منافع، جمعیت، سرمایه‌ها و سایر جنبه‌های مادی و معنوی حاکمیت را دارد. همچنین دولت‌ها با تعیین قلمرو، محدودیت‌هایی را برای دسترسی و بهره‌برداری قدرت‌های خارجی از منافع ملی وضع و اجرا می کنند (Medeiros, B. P., & Goldoni, L. R. F. 2020). به عبارت دیگر قلمرو ملی به «محدوده جغرافیایی یا فضای گسسته و جدا از سایر قلمروها و نشان دهنده

ظرفی که دولت توان اعمال قدرت بر آن دارد» گفته می‌شود. بنابراین قلمرو زیربنای اقتدار دولت است و مرزها، محدوده تخصیص اختیار دولت را تعیین می‌کنند (Tsaugourias, N. 2017).

از آنجا که حفاظت از شهروندان یکی از اهداف اساسی کشور است، امنیت مرزها به وضوح به عنوان یک مسئولیت اصلی دولت تلقی می‌گردد که از آن تحت عنوان «مرزبانی» یاد می‌شود. تلاش‌ها و سازوکارهای سنتی که برای حفظ امنیت مرزها (مرزبانی) توسط دولت‌ها در همه عرصه‌ها انجام شده، آشکار و تا اندازه بسیار زیادی قابل قبول است. این اقدامات مجموعه‌ای از بازدارنده‌های فیزیکی و قابلیت‌های بازرسی در مرزهای کشور برای شناسایی و کنترل آنچه مجاز به عبور از مرزهای کشور می‌باشد را تشکیل می‌دهند که مرزبانی نامیده می‌شود. در مرزبانی ملی حق و وظیفه دولت است که کنترل کند چه کسی و چه چیزی از مرزها عبور نماید تا از کشور و مردم آن در برابر تهدیدات خارجی محافظت کند. این تهدیدها از موارد آشکار مانند تروریست‌ها و متجاوزین که به‌دنبال انجام یک حمله یا ارتکاب جنایت هستند تا موارد کمتر آشکار مانند محصولات کشاورزی و مواد غذایی آلوده که می‌تواند صنعت کشاورزی کشور را به شدت تحت تأثیر قرار دهد یا جمعیت را بیمار کند متغیر است (Osborn, P. 2017).

۴.۲ چگونگی اعمال حاکمیت بر فضای سایبر ملی در پرتوی ویژگی‌های خاص فضای سایبری

در نگاه اول به نظر می‌رسد ویژگی بدون مرز بودن فضای سایبری با مفاهیم سنتی حاکمیت سرزمینی (ملی) و اصول و قواعد حقوق بین‌الملل در این زمینه سازگاری ندارد و عملا امکان اعمال حاکمیت سرزمینی (ملی) در فضای سایبری وجود ندارد. در این زمینه سؤالاتی مطرح می‌شود که آیا حقوق بین‌الملل می‌تواند به عنوان یک ابزار تنظیم‌کننده در فضای سایبری عمل کند و اینکه دامنه صلاحیت نظارتی آن چیست؟ به علاوه اینکه آیا دولت‌ها می‌توانند منبع مقررات در فضای سایبری باشند؟

در بازنمایی اولیه فضای سایبری اینگونه به نظر می‌رسید که این فضا غیرقلمروی و بدون مرز است و به همین دلیل نمی‌توان آن را مشمول اصول و قواعد به رسمیت شناخته شده دنیای فیزیکی و پایش، نظارت و اعمال قدرت دولتی دانست. پس این فضا را نیازمند ساختارهای قانونی متفاوت و مختص به خود می‌دانستند. یکی از دیدگاه‌های مطرح در این زمینه دیدگاه جان پری بارلو است که در «اعلامیه استقلال فضای مجازی» به آن اشاره شده است. جان پری بارلو در این اعلامیه که در سال ۱۹۹۶ میلادی منتشر شده است، با رد اعمال حاکمیت دولتی و قوانین مرتبط با فضای واقعی در فضای سایبری (مجازی) آورده است: «دولت‌های جهان صنعتی، شما غول‌های خسته فولاد، من از فضای مجازی، خانه جدید ذهن آمده‌ام. از طرف آینده از شما گذشته‌ها می‌خواهم که ما را تنها بگذارید. شما در میان ما خوش آمدید. شما در جایی که ما جمع می‌شویم هیچ «حاکمیتی» ندارید. ما هیچ دولت منتخبی نداریم و احتمالاً هم نخواهیم داشت ... ما فضای اجتماعی جهانی را بنا می‌نهیم. به‌طور طبیعی مستقل از ظلم‌هایی که می‌خواهید بر ما تحمیل کنید، اعلام می‌کنم، شما حق اخلاقی ندارید که بر ما حکمرانی کنید و هیچ روشی برای اجرا در این زمینه ندارید که باعث نگرانی ما باشد. دولت‌ها اختیارات ذاتی خود را از رضایت حکومت‌شوندگان می‌گیرند. شما نه درخواست از ما دارید و نه دریافت کرده‌اید. فضای مجازی در محدوده حاکمیت شما قرار ندارد. ما در حال شکل دادن به

قراردادهای اجتماعی خودمان هستیم. این حکومت بر اساس شرایط دنیای ما به وجود خواهد آمد و دنیای ما متفاوت از دنیای شما است. مفاهیم حقوقی مورد استفاده شما از دارایی، بیان، هویت، حرکت و زمینه در مورد فضای مجازی صدق نمی‌کند و همه آنها بر اساس ماده هستند. حال اینکه در فضای مجازی ماده‌ای وجود ندارد. ما امیدواریم بتوانیم راه‌حل‌های خاص خود را برای این فضا بسازیم. اما نمی‌توانیم راه حل‌هایی که شما دوست دارید بر ما تحمیل کنید را بپذیریم. ما باید دنیای خود را مصون از حاکمیت شما بسازیم، حتی اگر همچنان به حکومت شما بر بدن و دنیای فیزیکی رضایت دهیم. ما خودمان را در سراسر این سیاره پخش خواهیم کرد تا کسی نتواند افکار و اندیشه‌های ما را تسخیر کند. ما تمدن ذهن را در فضای مجازی ایجاد خواهیم کرد. باشد که از دنیایی که دولت‌ها ساخته‌اند، انسانی‌تر و عادلانه‌تر باشد.» (BARLOW'S, J. P. 1996).

همچنین جانسون و پست در مقاله‌ای با عنوان «قانون و مرزها: ظهور قانون در فضای مجازی» در سال ۱۹۹۶ میلادی، اعمال مفاهیم موجود حاکمیت و قانون در فضای سایبری را به دلیل ویژگی متمایز غیرسرزمینی و بدون مرز بودن آن رد می‌کنند و به همین دلیل، تدوین قوانین اختصاصی برای فضای سایبری را پیشنهاد می‌کنند. جانسون و پست نتیجه می‌گیرند که اگر چه فضای سایبری یک فضای بدون ضابطه نیست و نیاز به تنظیم‌گری و هنجارسازی دارد لیکن قوانین موجود مبتنی بر قلمروی فیزیکی برای اعمال بر فضای سایبری مناسب نیستند. جانسون و پست اعمال اصول و قواعد حقوق بین‌الملل در فضای سایبری را رد نمی‌کنند و علاوه بر این برای اعمال قوانین و مقررات در فضای سایبری، به قلمروگذاری و مرزبانی در این فضا تأکید دارند. هر چند آنها بین قلمرو در فضای سایبری و فیزیکی تفاوت قائل هستند و نوع متفاوتی از مرزها را برای فضای سایبری با توجه به ویژگی‌های خاص آن متصور هستند. به عقیده آنها اگر چه شخصیت بدون مرز فضای سایبری امکان پایش، نظارت و تنظیم قانونی این فضا را تضعیف می‌کند و به چالش می‌کشد؛ قدرت و اقتدار همان طور که پیش‌تر گفته شد، جوهره حاکمیت است و فقدان قلمرو و مرز، قدرت اعمال حاکمیت را از دولت‌ها سلب می نماید. بنابراین همچنان قلمرو و مرز نقش سازنده و کارکردی در قاعده‌گذاری، اعمال و اجرای قانون در فضای سایبری بازی می‌کند و مرزها سازمان حاکمیت در فضای سایبری را تعریف می‌نمایند (Johnson, D. R., & Post, D. 1996).

موضع جان‌پری‌بارلو و برخی دیگر از نظریه‌پردازان در مورد ماهیت استثنایی فضای سایبری توسط جک گلداسمیت در مقاله‌ای با عنوان «علیه هرج و مرج سایبری» به چالش کشیده شده است. از نظر او فضای سایبری نیز از افراد و اشیاء تشکیل شده است. بنابراین دولت‌ها می‌توانند بر مردم و اشیاء در قلمرو خود اعمال حاکمیت نمایند و فعالیت‌ها در این فضا را تنظیم کنند. همچنین گلداسمیت، نظر جانسون و پست را به چالش می‌کشد و استدلال می‌کند قواعد و هنجارهای پذیرفته شده فضای فیزیکی در برخی حوزه‌ها می تواند در فضای سایبری نیز دارای اعتبار و قابل اتکا باشد. به گفته گلداسمیت دولت می‌تواند بر فضای سایبر ملی اعمال قدرت و فعالیت‌ها در این فضا را تا حد زیادی از طریق تکنیک‌های موجود تنظیم کند. این دیدگاه هم اکنون به عنوان دیدگاه غالب نسبت به فضای سایبر ملی پذیرفته شده است (Goldsmith, J. L. 1998).

موارد فوق بیانگر دیدگاه‌هایی است که طی دهه‌های گذشته و به خصوص سال‌های اولیه ظهور فضای سایبری بیان شد. آنچه مشخص است، امروزه قریب به اتفاق صاحب‌نظران به هنگام رویارویی با فضای سایبری،

بر هنجارسازی و تنظیم‌گری این فضا و همچنین بر نقش قلمرو و مرز در این زمینه به طور صریح یا ضمنی تأکید دارند.

۵.۲ رقابت‌های دولتی مداوم در فضای سایبری و لزوم قلمروگذاری فضای سایبر ملی

ایجاد سازوکارهای مختلف کنترل مرزی در همه عرصه‌ها که با مقاصد گوناگون از پایش و نظارت بر مرزها، کنترل مهاجرت تا پیشگیری از جرم، جنایت و حملات نظامی انجام می‌پذیرد نشان می‌دهد حاکمیت سرزمینی و قلمرو دولتی حتی در جنبه های فیزیکی نیز هنوز معنای خود را از دست نداده‌اند و گاه با قدرت مضاعف ادامه دارد. بنابراین روند تقویت مرزهای ملی و کنترل‌های دولتی هنوز در دست انجام است. ویژگی‌های خاص فضای سایبری که بخش قابل توجهی از تهدیدات علیه امنیت ملی در فضای سایبری را به همراه داشته است و از سوی دیگر دشواری انتساب حملات در این فضا، موجب گردیده است شاهد رقابت‌های دولتی مداوم در قلمروگذاری فضای سایبری و اعمال سیاست‌های صیانت از قلمرو سایبری باشیم.

همان‌طور که در بالا اشاره شد، فعالیت‌های زیرسطح آستانه توسل به زور در فضای سایبری که با نادیده گرفتن قلمرو ملی کشورها و قواعد بین‌المللی انجام می‌پذیرد، به طور فزاینده‌ای در حال افزایش است. فقدان قلمروگذاری ملی و مرزهای تعریف شده در فضای سایبری به نفع کشورهای بسیار توسعه‌یافته با قابلیت‌های تهاجمی سایبری است. از آنجایی که فضای سایبری دستیابی به اهداف سیاسی را آسان‌تر، کارمدتر و بدون خطر قرار گرفتن در معرض انتقاد بین‌المللی، ممکن می‌سازد؛ فقدان قلمروگذاری ملی و به‌تبع آن پایش و اعمال قدرت دولتی در قلمرو ملی، اقدامات خصمانه زیر سطح آستانه توسل به زور در فضای سایبری علیه فضای سایبر ملی را تشدید می‌نماید (Dziwisz, D. 2022).

۶.۲ شواهد قلمروگذاری در فضای سایبری ملی در دیگر کشورها

امروزه اقدامات و فعالیت‌های پایش، نظارت و اعمال قدرت کشورها بر قلمرو سایبر ملی که به درجات مختلف در کشورها اعمال می‌شود به نوعی بیانگر قلمروگذاری و مرزبانی این فضا حتی در کشورهایی است که در ظاهر مدعی فضای سایبری بدون مرز هستند. یعنی برخی از کشورها در قلمروگذاری و مرزبانی فضای سایبر ملی شفاف‌تر عمل می‌کنند ولی حتی در کشورهایی که به ظاهر مدعی فضای سایبر به هم پیوسته جهانی و گردش آزاد اطلاعات در این فضا هستند نیز کنترل و اعمال قدرت بر قلمرو سایبری کشور خود را به گونه‌ای متفاوت اعمال می‌نمایند. هم‌اکنون طیف اقدامات بومی‌سازی و ملی‌گرایی داده‌ها در کشورهای دموکراتیک تا کشورهای اقتدارگرا آغاز شده و الزامات وضع شده توسط دولت‌ها مبتنی بر مکان تولید داده‌ها در حال افزایش است.

با یک گونه‌شناسی و تجزیه و تحلیل از اشکال مختلف اعمال کنترل ملی بر داده‌ها می‌توان پی برد این اقدامات با اهدافی نظیر حفاظت از داده‌ها و حریم خصوصی شهروندان، نظارت و پایش اطلاعات در گردش در قلمرو سایبری ملی و در برخی موارد نیز به منظور کنترل نوع اطلاعاتی که از مرزهای فضای سایبری کشور جریان می‌یابند اعمال می‌شوند.

دولت چین از مدت‌ها پیش با ترویج نسخه قوی از ملی‌گرایی داده‌ها که به آن «حاکمیت سایبری» نیز گفته می‌شود، اقدامات مرتبط با این حوزه را دنبال می‌کند. روسیه از طریق فعالیت‌های خود در فضای سایبری نوعی «خط مقدم دیجیتال» را ایجاد می‌کند که به‌نوعی تداعی‌کننده خط مقدم نظامی در سایر عرصه‌ها است. در کنار پیاده‌سازی الزامات ذخیره‌سازی داده‌ها در قلمرو سرزمینی یا به اصطلاح «بومی‌سازی داده‌ها» در کشورهایی مثل روسیه، هند و چین؛ اتحادیه اروپا نیز مجموعه‌ای از محدودیت‌های انتقال داده از قلمرو سرزمینی این اتحادیه را اعمال نموده است که برای محافظت از حریم خصوصی شهروندان و ساکنان اتحادیه اروپا طراحی شده است (Stadnik, I. 2021).

در ایالات متحده امریکا، علاوه بر الزام شرکت‌های تحت مالکیت روسیه و چین به ذخیره‌سازی داده‌های مربوط به شهروندان امریکایی در قلمرو سرزمینی ایالات متحده امریکا؛ طی سال‌های گذشته کنگره امریکا تغییراتی را در کمیته سرمایه‌گذاری خارجی به تصویب رسانیده است تا شرکت‌ها و برنامه‌های کاربردی خارجی را که داده‌های شخصی و حساس را جمع‌آوری و نگهداری می‌کنند، با هدف محافظت در برابر استفاده‌های ناپسند خارجی در معرض بررسی‌های امنیت ملی قرار می‌دهد (Stewart, D. P. 2018).

فرانسه بر حق حاکمیت بر قلمرو سایبری ملی تأکید دارد و هر گونه عملیاتی که منجر به نقض محرمانگی، یکپارچگی و دسترس بودن سامانه‌های سایبری شود نقض حاکمیت به حساب می‌آورد. این نقض نه‌تنها زمانی رخ می‌دهد که اثرات آن در قلمرو فرانسه نمایان شود بلکه حتی زمانی که به فضای سایبر ملی فرانسه نفوذ می‌شود هم صادق است (Broeders, D., & van den Berg, B. 2020).

هم‌اکنون ابزارهای متنوعی برای دولت‌هایی وجود دارد که به دنبال بازسازی قلمرو ملی خود در فضای سایبری هستند. دیوارهای آتش ملی یکی از شناخته شده‌ترین روش‌ها برای دولت‌ها است تا هم ادعای سرزمینی خود را اعلام کنند و هم قدرت خود را در فضای محدود نشان دهند. این فایروال‌ها طیف وسیعی از مکانیسم‌های فیلترینگ مانند مسدود کردن IP و جستجوی کلمات کلیدی را برای سانسور بحث در مورد موضوعات حساس و عدم دسترسی به وب‌سایت‌هایی که خرابکارانه تلقی می‌شوند، ترکیب می‌کنند. «دیواره آتش بزرگ چین» مشهورترین مثال در این زمینه است، اما سایر کشورها نیز سامانه‌های مشابه را توسعه داده یا در حال توسعه هستند. کره شمالی احتمالاً افراطی‌ترین نمونه‌ای است که تا همین اواخر، کاربران فقط می‌توانستند به شبکه داخلی[1] در سراسر کشور دسترسی داشته باشند. امروزه دسترسی به برخی از سایت‌های اینترنتی تحت محدودیت‌های شدید و نظارت دقیق دولت امکان‌پذیر است.

۳ روش‌شناسی تحقیق

این پژوهش از منظر هدف توسعه‌ای-کاربردی می‌باشد. روش تحقیق مورداستفاده در این پژوهش توصیفی-تحلیلی است که با استفاده از روش جمع‌آوری اطلاعات کتابخانه‌ای و اینترنتی، مجموعه اسناد و مقالات مرتبط با موضوع تحقیق مورد بررسی جامع قرار گرفت. در ادامه با تجزیه و تحلیل اسناد در این حوزه، نقش و جایگاه قلمروگذاری و مرزبانی فضای سایبری در اعمال حاکمیت بر فضای سایبر ملی مورد پژوهش قرار

[1] Kwangmyong

گرفت. نتایج حاصل از این پژوهش می‌تواند ارتقاء دانش مدیران و متولیان کشور را در زمینه اعمال حاکمیت بر فضای سایبر ملی به همراه داشته باشد.

۴ تجزیه و تحلیل

با تجزیه و تحلیل موارد یاد شده می‌توان استنباط کرد که در وهله نخست باید از تشبیه ساده قلمرو در فضای سایبری با سایر قلمروهای سنتی اجتناب کرد. زیرا ساختار به هم‌پیوسته و جهانی فضای سایبری ایجاب می‌نماید قلمرو در این فضا متخلخل باشد و با توجه به وجود بازیگران مختلف که در فضای سایبر جهانی کنش و اعمال قدرت می‌نمایند با همپوشانی قلمرو کنشگران روبرو هستیم. این موضوع سبب شده است دولت‌ها در صورت اراده، با استفاده از راهکارها و فناوری‌های نوین به قلمرو ملی دیگر کشورها تعرض نمایند.

در وهله بعد اگر چه احترام به حاکمیت ملی کشورها یک اصل اساسی در حقوق بین‌الملل به شمار می‌رود و از آن قواعد و هنجارهای بازدارنده‌ای از حقوق بین‌الملل مانند احترام به صلاحیت دولت‌ها در کنترل و مدیریت منابع و زیرساخت‌ها در قلمرو سرزمینی، ممنوعیت تهدید و توسل به زور علیه دولت دیگر و ممنوعیت مداخله در امور داخلی دیگر کشورها ناشی می‌شود که مورد پذیرش همگان است؛ قوانین و هنجارهای فعلی بین‌المللی، اقدامات زیر سطح آستانه این قواعد را نهی نمی‌کند و دولت‌ها را ملزم نمی‌کند از هرگونه فعالیتی که حاکمیت دولت سرزمینی را خدشه‌دار می‌کند خودداری نمایند. به خصوص اینکه تعیین سطح آستانه اقدامات ناقض حاکمیت سرزمینی کشورها در فضای مجازی و همتراز شمردن اقدامات و عملیات‌های سایبری با اقدامات و عملیات‌های ناقض حاکمیت سرزمینی در فضای واقعی، به دلیل عدم شفافیت و قطعیت اسناد حقوق بین‌الملل در این زمینه، دوچندان مشکل است. به‌علاوه، با توجه به خصوصیات و ویژگی‌های فضای سایبری، انتساب اقدامات ناقض حاکمیت سرزمینی به دولت متخاصم، در قریب به اتفاق موارد امکان‌پذیر نیست. شواهد این امر را می‌توان در این واقعیت مشاهده کرد که دولت‌ها عملیات‌های نفوذ، جاسوسی و جمع‌آوری اطلاعات حیاتی و حتی تخریب منابع، زیرساخت‌ها و سامانه‌های دیگر کشورها را از طریق فضای سایبری انجام می‌دهند و پیگرد قانونی آنها از طریق حقوق بین‌الملل مقدور نیست.

افزون بر این در کنار این موضوعات، بی‌علاقگی یا ناتوانی کشورها در تدوین نظامات حقوقی شفاف و متقن برای فضای سایبری در جهت ممانعت و مقابله با فعالیت‌های مخرب و ناقض حاکمیت ملی و سرزمینی کشورها در فضای سایبری (با توجه به ویژگی‌های منحصر به فرد این فضا)، منجر به پیدایش ابهامات و روزنه‌هایی برای نقض حاکمیت کشورها و عدم امکان تعیین زمان دقیق نقض حاکمیت و به‌تبع آن عدم پیگیرد بین‌المللی در این زمینه شده است.

از این رو قلمروگذاری و مرزبانی فضای سایبر ملی، به‌عنوان راهکاری برای محافظت بیشتر از داده‌ها و شهروندان در برابر تهدیدات خارجی و مهم‌تر از آن اعمال حاکمیت ملی سایبری، می‌تواند مورد توجه ویژه قرار گیرد. از این رو دولت‌ها که وظیفه اساسی محافظت از منابع و منافع ملی، مدیریت و تنظیم‌گری در تمامی عرصه‌ها و به تبع آنها اعمال حاکمیت ملی را بر عهده دارند قادرند با اعمال سیاست‌های قلمروگذاری و مرزبانی فضای سایبر ملی، اعمال حاکمیت در این فضا را ارتقاء دهند.

۵ نتیجه‌گیری

حاکمیت در هر عرصه‌ای از چهار عنصر قلمرو، شهروندان، منابع و سیاست تشکیل می‌گردد و پیش‌شرط اعمال حاکمیت در فضای سایبر نیز تعریف و تحقق این چهار عنصر می‌باشد. یعنی اینکه افراد، تجهیزات و داده‌های موجود در فضای سایبری هر کشور، تابع حکمرانی آن کشور بوده و هیچ کشوری نباید در فضای سایبر واقع در قلمرو کشورهای دیگر مداخله کند. از سوی دیگر تمام کشورها حق دارند از قلمرو خود در برابر تجاوز محافظت نمایند. به‌علاوه، قلمروگذاری و مرزبانی در تمامی عرصه‌ها یکی از راهکارهای مهم در تولید قدرت ملی و بازسازی و حفظ هویت ملی محسوب می‌گردد. در نتیجه حق، وظیفه و خواست دولت است که کنترل کند چه کسی و چه چیزی از مرزهای کشور عبور می‌کند تا از کشور و مردم آن در برابر تهدیدات خارجی محافظت نماید. این موضوع در عرصه سایبری نیز صدق می‌کند. در نتیجه قلمروگذاری و مرزبانی فضای سایبری کشور می‌تواند نقش بسزایی در اعمال حاکمیت بر فضای سایبری ملی داشته باشد.

از سوی دیگر با توجه به اینکه هنوز هیچ‌گونه قواعد و هنجار اختصاصی برای اقدامات زیرآستانه استفاده از زور و مداخله آشکار در فضای سایبر سایر کشورها توسعه نیافته است، تعیین دقیق مرز بین اقدامات مجاز و غیر مجاز سایبری با استناد به قوانین، مقررات و هنجارهای بین‌المللی امکان‌پذیر نیست و در بسیاری از موارد دولت‌ها آزاد هستند در این زمینه مطابق تفسیر و میل خود عمل کنند. ولی به هر حال برخورداری از اصول و قواعد حقوق بین‌الملل، پیگیری‌های قانونی و دفاع از فضای سایبر ملی مستلزم تعریف و اعلان قلمرو سایبری ملی و مرزبانی مؤثر این فضا می‌باشد. در نتیجه تعریف نشدن قلمرو و مرز ملی در فضای سایبری، رفتار قانون‌مند کنشگران خصوصی و دولتی در یک فضای قانونی را به همراه نخواهد داشت و این مسئله منجر به تضعیف نظام حاکم و امنیت ملی خواهد شد.

مراجع

[۱] بدیعی ازنداهی، مرجان و میراحمدی، فاطمه سادات و غلامی، بهادر (۱۳۹۹). مقایسه‌ی مفهوم «حاکمیت ملی» در قوانین اساسی مشروطه و جمهوری اسلامی ایران.

[۲] کریمی قهرودی، محمدرضا و زارعی وحید (۱۳۹۹). حاکمیت فضای سایبری، انتشارات مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

[۳] کامران دستجردی حسن (۱۴۰۱). کاربرد حاکمیت در مقیاس‌های فضایی. نشریه تحقیقات کاربردی علوم جغرافیایی، سال بیست و دوم، شماره ۶۵.

[۴] کاویانی‌راد، مراد (۱۳۹۲). پردازش مفهوم «قلمرو» از دیدگاه جغرافیای سیاسی. برنامه‌ریزی و آمایش فضا (مدرس علوم انسانی)، ۱۷(۴)، ۴۳-۶۱.

[۵] اسمعیل‌زاده ملاباشی، پرستو، عبدالهی (۱۳۹۹). حملات سایبری و نقض اصل عدم مداخله. فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ۵۰(۲)، ۷۱۱-۷۳۶.

[6] Paasi, A., Ferdoush, M. A., Jones, R., Murphy, A. B., Agnew, J., Ochoa Espejo, P., & Fall, J. J. (2022). Locating the territoriality of territory in border studies. Political Geography, 95, 102584.

[7] Douzet, F. (2020). Cyberspace: the new frontier of state power. Handbook on the Changing Geographies of the State.

[8] Medeiros, B. P., & Goldoni, L. R. F. (2020). The Fundamental Conceptual Trinity of Cyberspace. Contexto Internacional, 42, 31-54.

[9] Tsaugourias, N. (2017). Law, Borders and the Territorialisation of Cyberspace. Indonesian J. Int'l L., 15, 523.

[10] Osborn, P. (2017). Cyber Border Security–Defining and Defending a National Cyber Border. Homeland Security Affairs, 13.

[11] BARLOW'S, J. P. (1996). Declaration ofindependence for cyberspace.

[12] Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. stanford law review, 1367-1402.

[13] Goldsmith, J. L. (1998). Against cyberanarchy. The University of Chicago Law Review, 65(4), 1199-1250.

[14] Lambach, D. (2020). The territorialization of cyberspace. International Studies Review, 22(3), 482-506.

[15] Möllers, N. (2021). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. Science, Technology, & Human Values, 46(1), 112-138.

[16] Broeders, D., & van den Berg, B. (Eds.). (2020). Governing Cyberspace: Behavior, Power and Diplomacy. Rowman & Littlefield Publishers.

[17] Janparvar, M., Ghasri, M., & Hosseinpour Motlagh, M. (2015). Border Management of Cyberspace, First Step of Cyber Defense. Research on Humanities and Social Sciences, 5.

[18] Heintschel von Heinegg, W. (2013). Territorial sovereignty and neutrality in cyberspace. International Law Studies, 89(1), 17.

[19] Dziwisz, D. (2022). Non-War Activities in Cyberspace as a Factor Driving the Process of De-Bordering. Politics and Governance, 10(2).

[20] Assaf, A., & Moshnikov, D. (2020). Contesting sovereignty in cyberspace. International Cybersecurity Law Review, 1(1), 115-124.

[21] Goel, S. (2020). National cyber security strategy and the emergence of strong digital borders. Connections, 19(1), 73-86.

[22] Deibert, R. J., & Pauly, L. W. (2019). Mutual entanglement and complex sovereignty in cyberspace. In Data Politics (pp. 81-99). Routledge.

[23] Stadnik, I. (2021). Russia: An independent and sovereign Internet?. Power and Authority in Internet Governance, 147-167.

[24] Stewart, D. P. (2018). Recent Developments in US Cyberlaw. Agenda Internacional, 25(36), 113-131.

زندگی در ناواقعیتِ ماتریکس و فضای سایبری

مرتضی سعیدی ابواسحاقی [۱]، راضیه سعیدی ابواسحاقی [۲]

[۱] دانشجوی دکتری فلسفه دانشگاه تهران، پژوهشگر پژوهشگاه فضای مجازی
morteza.saeidi@ut.ac.ir
[۲] دانش آموخته کارشناسی تعلیم و تربیت، دانشگاه فرهنگیان
raziyesaeedi9819@gmail.com

چکیده

فیلم ماتریکس (۱۹۹۹) انسان‌ها را به‌نحوی تصویر می‌کند که در فضایی کامپیوتری اسیر شده‌اند و بدن آنها در خمره‌ای لزج و مغذی به‌عنوان منبع انرژی ماتریکس قرار دارد و ماتریکس جهانی می‌سازد و به ذهن انسان‌ها این را القاء می‌کند که همین، واقعیت است. فضای ماتریکس را با فضای سایبری و شبکه‌های مجازی مقایسه کرده‌ایم که در فضای مجازی نیز واقعیتی شبیه به ماتریکس در حال رقم خوردن است و انسان‌ها در حال تخدیر شدن هستند، تا جایی که زندگی در ماتریکس و زندگی در فضای سایبری همانند زندگی در ناواقعیت است. ناواقعیتی که انسان‌ها به دلیل تخدیر و احساس لذت خیلی وقت ها نمی‌خواهند از آن آزاد شوند. در این مقاله بیان شده است که این امکان بر اساس حقیقت سوبژکتیوته و ریاضیاتی شدن جهان و ابژه شدن انسان وقوع پیدا می‌کند، و فیلم ماتریکس را تذکری هوشمندانه از طرف هنر هفتم برای انسان‌ها می‌دانیم.

کلمات کلیدی: ماتریکس، سوبژکتیویته، فضای سایبری، ابژه، انسان.

۱ مقدمه

همواره هنر این امکان را داشته است که زودتر از دیگران و به نحوی با درک شهودیِ هنرمند، زودتر از دیگران مسئله را بفهمند و به تصویر بکشند، آیا این همان چیزی نبوده است که هنر هفتم زودتر از سایرین آن را گوشزد کرده است، یعنی چیزی که اکنون در واقعیت آن را می‌بینیم و متجلی در شبکه‌های مجازی و فضای سایبری و هوش مصنوعی و علوم شناختی و متاورس و ... است، که انسان گرفتار و اسیر هوش مصنوعی و فضای سایبری و شبکه‌های مجازی و ... می‌شود و تفسیری کامپیوتری از ذهن انسان در علوم شناختی ارائه می‌شود، همه و همه به‌نحوی یک سال مانده به هزاره سوم (یعنی سال ۱۹۹۹) توسط برادران واچوفسکی در فیلم ماتریکس به پرده سینما رفت و اقبال از آن نیز نشان از همدلی با آن داشت.

این فیلم در ژانر سایبرپانک، یکی از شاخه‌های ژانر علمی-تخیلی ساخته شده است. موضوع این ژانر عمدتا مربوط به داستان‌های پادآرمان‌شهری محسوب می‌شود که جوامع در آینده به وضعی مهلک و دارای

اختلالی های شدید دچار می‌شوند که مربوط به تکنولوژی‌های پیشرفته و هوش مصنوعی و کامپیوتر و ارتباطات و سایبرنتیک است. زمان و مکان این نوع داستان‌ها در ابتدا در فضاهای دوردست بوده است ولی هر چه به قرن ۲۱ نزدیک شدیم داستان آن در کره زمین دنبال می‌شد، مثلاً در فیلم ماتریکس مربوط به نابودی کره زمین و اشغال آن توسط هوش مصنوعی یا AI است که تنها یک شهر از کره زمین باقی مانده است و مقاومت می‌کند و البته جایگاهش را در نزدیکی مرکز زمین قرار داده است.

فیلم موفق برادران واچوفسکی یعنی ماتریکس، فیلمی است که بیش از هر فیلم دیگری بحث‌های فلسفی را برانگیخته است (Wartenberg, 2015). برای مثال کتاب «خوردن قرص قرمز: دانش، فلسفه و مذهب در ماتریکس» و مقاله‌های «از اهریمن شریر دکارت تا ابررایانه خبیث ماتریکس؛ نگاهی به فرضیه‌های فلسفی ماتریکس» یا مقاله‌های «همه آنچه را که به تو خواهم گفت درک نخواهی کرد!»، «مذهب، هگل و هایدگر به زبان تکنولوژیک»، «ماتریکس به مثابه متافیزیک» و «اتوپیای پراگماتیستی» و ... هر کدام به‌نحوی فیلم را مورد بررسی و مداقه قرار داده اند. از این حیث که این فیلم متناسب با مباحث فلسفی مهمی درباره اینترنت و هوش مصنوعی و فضای سایبری و سایبرنتیک و ... به وجود آمده است، اهمیت آن را چندین برابر می‌کند، و از این نظر که در فلسفه از وجود بما هو موجود سخن می‌گویند، و اکنون مباحث مهمی درباره این فیلم مطرح می‌شود، نشان از آن دارد که آن وجودی که در قرن ۲۱ ظهور پیدا کرده است می‌تواند مباحث مربوط به تکنولوژی کامپیوتری و فضای سایبری باشد، و به‌همین دلیل توجه اهالی علم و فلسفه و سینما و فرهنگ و اندیشه را معطوف به خود کرده است.

این فیلم چیزهایی را متذکر می‌شود که امکان داشت انسان و بشریت در آنها گرفتار شود و البته از برخی حیثیت به آن دچار شد. در این مقاله بر آنیم که این مطلب را با نگاه به ماتریکس و شباهت آن به فضای سایبری که برآمده از حقیقت و اصالت مدرنیته و غرب (یعنی سوبژکتیویته و ریاضیاتی شدن جهان و تکنولوژی ماشینی یا کامپیوتر) هستند، به بحث گذاریم.

۲ ریاضیاتی شدن جهان و سوبژکتیویته

پس از قرون وسطی و در دوره رنسانس اتفاقاتی در غرب رقم می‌خورد که بر اساس آن نگرشی مکانیستی درباره جهان به وجود آمد که جهان را به‌صورت ماشینی بزرگ تلقی می‌کنند. دکارت، هابز و اسپینوزا هر کدام به‌نحوی آن را صورت‌بندی کرده‌اند. دکارت که تنها دو جوهرِ اندیشه و امتداد را باور دارد (دکارت، ۱۳۷۱، ص ۷۳) جهان را به‌مثابه امتداد همچون ماشینی بزرگ می‌داند؛ اما تلاش میکند که اندیشه را از این نگرش مکانیستی به دور نگه دارد، یعنی انسان را فدای نگرش مکانیستی‌اش نمی‌کند، اما اسپینوزا که همانند دکارت جهان را ماشینی بزرگ تلقی می‌کند، اندیشه و آگاهی و اراده را خارج از این ماشین بزرگ نمی‌داند و این‌گونه انسان همانند طبیعت درون ماشینی بزرگ به نام جهان قرار دارد. اسپینوزا درباره اعمال و اراده انسان می‌گوید: «من اعمال و امیال انسان را همان‌طور ملاحظه کردم که خطوط و سطوح و اجسام را ملاحظه کردم» (اسپینوزا، ۱۳۹۲، ص۱۴۲) و این نگرش مکانیستی درباره جهان و انسان در هابز به نحوی دنبال می‌شود که او انسان را جسمی همچون دیگر اجسام می‌داند (هابز، ۱۳۹۳، ص ۵۴۳) و از نظر او در جهان

چیزی به جز جسم نداریم و در این نگرش مکانیستی انسان همچون دیگر اجسامی است که در فیزیک مطالعه می‌شوند.

این نگرش در غرب روز به روز عمق بیشتری پیدا می‌کرد تا جایی که در قرن بیستم این امر با آمدن کامپیوتر و هوش مصنوعی و فضای سایبری جان بیشتری گرفت. در سایبرنتیک بر آن بودند که همه شئون انسانی و حیوانی و نباتی همچون ماشینی کنترل‌شده است که بر اساس فیدبک یا بازخورد همواره سعی دارد که با محیط انطباق یابد و رشد کند. وینر معتقد بود که با پیشرفت علم که تشابهاتی میان ماشین و موجود زنده مشاهده کرده‌ایم، دیگر مشکل حیات و روح داشتن و ... نباید وجود داشته باشد واز شر این‌گونه مسائل بایست خلاص شد و آنها را مشکلاتی صرفاً سمانتیک (معنایی) دانست (Wiener, 1951, pp 31-32). یعنی آنها را بایست صرفاً اموری دانست که در زبان انسان ایجاد شده‌اند و بایست به‌نفع نگرشی ساینتیفیکی (علمی)–مکانیستی منحل شوند و همه چیز همچون ماشین رفتار می‌کند. در هوش مصنوعی نیز می‌خواهند ذهن و رفتار و احساس و عواطف و خرد انسان را به‌صورت الگوریتم یا برنامه تلقی کنند و به‌نحوی کامپیوتری (که می‌توان آن را ماشین پیشرفته دانست) تبیین کنند و در پی ایجاد انسان‌های مصنوعی هستند و در حقیقت نگرشی ماشینی و کامپیوتری به انسان و جهان دارند که سعی دارند آن را در فضای آزمایشگاهی و حتی در فضای کامپیوتری و کدنویسی و برنامه و الگوریتم تکرار کنند.

ولی اگر بخواهیم این مسئله را عمیق‌تر بررسی کنیم باید درباره کامپیوتر و تکنولوژی ماشینی اندیشه کنیم و به لایه‌های عمیق‌تر آن وارد شویم. باید بپرسیم خاستگاه و اصل آنها از کجا می‌آیند، و البته این کار ساده نخواهد بود چراکه هایدگر معتقد است حتی هگل و مارکس هم نمی‌توانستند درباره آن اندیشه کنند، چرا که در سایه ذات تکنولوژی حضور داشتند (هایدگر، ۱۳۸۸، ص ۱۱۰) و به همین دلیل نمی‌توانستند مسئله را به‌درستی درک کنند. هیدگر معتقد است «تکنولوژی ماشینی با ماهیت متافیزیک مدرن یکی است و در آن ابتدائاً به‌کارگیری علوم فیزیکیِ ریاضی را طلب می‌کند.» (هایدگر، ۱۳۹۵، ص۱). فیزیک ریاضیاتی شده همان مسئله اصلی است که می‌تواند ما را به یک لایه عمیق‌تر درباره ماشین و کامپیوتر ببرد، در حقیقت در فیزیک ریاضی است که تکنولوژی ماشینی و کامپیوتر امکان ظهور می‌یابند. فیزیک ریاضیاتی در عصر مدرن ماهیت اشیاء را شکل می‌دهد و دیگر صورت ارسطویی تعیین‌کننده ماهیت اشیاء نیست؛ بلکه ریاضیات است که ماهیت بخش اشیاء (اعم از انسان و موجودات زنده و غیرزنده) است و اینگونه فیزیک خصلتی ریاضیاتی پیدا می‌کند مثلاً برای شناخت انسان در دانش جدید باید معادله و چند عدد برای آن به‌کار برده شود تا شناخته شود، و این کار در کامپیوتر به‌صورت عمیق‌تری جریان می‌یابد. در حقیقت آنچه در عصر جدید و پس از رنسانس و حتی اواخر قرون وسطی رخ داده بود، این بود که همه معرفت و همه علوم را به علم طبیعی فرو کاستند و نگرشی مکانیستی به جهان به‌وجود آمد و علم طبیعی هم چیزی جز ریاضیات نبود؛ در آن هر چه در عالم وجود دارد همچون جسم و کمیت تفسیر می‌شد تا ریاضیاتی شود و این‌گونه از بقیه وجوه اشیاء صرف نظر می‌شد.

اما برای اینکه عمیق تر به تکنولوژی ماشینی و کامپیوتر که بر اساس فیزیک ریاضیاتی شده امکان ظهور پیدا کردند، بپردازیم بایست ریاضیات را در عمیق‌ترین معنای آن بفهمیم. «Ta mathemata (ریاضیات) از نظر یونانیان هر چیزی است که آدمی از قبل (یعنی به‌صورت پیشینی) به هنگام مشاهده آنچه هست و

در مراوده با اشیاء می‌داند: مثل جسمانی بودن جسم، انسانیت انسان، حیوانیت حیوان، خصوصیت نباتی گیاهان» (هیدگر، ۱۳۹۵، ص۳). صفت پیشینی بودن همان چیزی است که باعث می‌شود چیزی ریاضیاتی شود و کانت این صفت را را باعث ضرورت و کلیت برای معرفت و علم می‌دانسته است (kant,1998, A128-A131). بنابراین از آنجایی که اشیاء در عصر مدرن بایست به‌صورت پیشینی دیده شوند تا بتوانند امکان ریاضی شدن داشته باشند و موجودیت و تعین یابند «تعیین این شرط ضروری در واقع معادل برنامه ریزی یا فراافکندنِ آن چیزی است که بعد از این باید طبیعت باشد.» (هیدگر، ۱۳۹۵، ص۴) فرا افکندن طرحی پیشینی برای اشیاء باعث، باعث می‌شود که در فیزیکِ ریاضیاتی شده جای بگیرند و همه جهان به صورت ریاضیاتی شده درآید، به عبارتی اساس همه چیز در این طرح پیشینی تعین می‌یابد که سوژه آن را فرا افکنده است، و اینگونه سوژه یا انسان به مرکز همه عالم تبدیل می‌شود و همه چیز را سوژه بنیاد می‌نهد، و این همان ماهیت عصر مدرن یا سوبژکتیوته است که انسان یا سوژه همه نسبت‌های جهان را طرح‌اندازی می‌کند و بقیه چیزها به‌عنوان ابژه در خواهند آمد و سوژه است که ابژه‌ها را طرح‌اندازی می‌کند، یعنی اراده‌اش را بر آنها بار می‌کند و بر خلاف قرون وسطی که اشیاء و موجودات و انسان‌ها و ... در نظام خلقت در رتبه‌های خاصی قرار می‌گرفتند، در جهان مدرن و سوبژکتیویته هر چه هست بایست خصوصیت ابژه را داشته باشد. هایدگر ابژه شدن را همان بازنمایانده شدن توسط انسان می‌داند، یعنی تبدیل به تصویر شود (همان ، ص۱۳-۱۶). به این ترتیب عین یا ابژه در فراافکندن پیشینی سوژه بازنمایی می‌شود و به تصویر مبدل می‌گردد و جهان به‌مثابه تصویر یا ابژه در می‌آید که به‌صورت پیشینی طرح‌اندازی شده است یعنی ریاضیاتی شده است و بنیاد جهان مدرن در سوبژکتویته بنا نهاده می‌شود و این امر عین ریاضیاتی شدن و ابژه شدن جهان است.

سوبژکتیویته عبارت است اصالت من انسان که همه چیز بر محور آن قابلیت موجود شدن پیدا کنند. در حقیقت در رنسانس، اومانیسم و رسیدن به این معنا بود که بشر نیازی به هدایت غیبی ندارد، و اراده و عقلش او را کفایت میکند، و به نوعی خودبنیادی روی آوردند که اصالت با من انسانی خواهد بود و محوریت امور و دائر مدار عالم را نه خدا، بلکه انسان و عقل انسان و من انسانی می‌دانستند. این امر با نام سوبژکتیویته در فلسفه طرح‌ریزی شد، و دکارت با تأسیس اصل کوژیتو (cogito ergo sum: می‌اندیشم، پس هستم)، بنیاد هستی را سوژه یا من انسانی دانست که همه موجودات به او قائم و معتبرند و سایر موجودات در حکم بازنمودها یعنی ابژه‌های او هستند. در ادبیات فلسفی غرب من انسانی به عنوان سوژه به‌کار رفت که سایر موجودات قائم به آن هستند. به این ترتیب هم من انسانی یا سوژه بنیاد همه چیز گردید و هم موجودات دیگر به ابژه بدل شدند و سوژه اراده اش را در همه موجودات جاری می‌کند و عالَم به جز تصویر یا بازنمودی که انسان یا سوژه از آن می‌سازد، حقیقت دیگری ندارد. غرب با چنین نگرشی که انسان را خود بنیاد یا سوژه، و بقیه جهان را ابژه و قائمِ به سوژه تلقی کرده است، در مسیر جدیدی گام برداشته که از آن به سوبژکتویته تعبیر می‌شود و همه ساحات و شئونات فرهنگی، علمی، تکنولوژیکی و ... بر اساس آن بنا نهاده شده است.

ابژه در برابر سوژه است که درباره آن بایست گفت، همان چیزی است که سوژه به آن فکر می‌کند، و سعی دارد با طرحی پیشینی که بر آن می‌اندازد، آن را برساخته عقل و خرد خویش سازد، یعنی بنیاد آن را طرح‌اندازی کند و به این ترتیب اراده خودش را در آن جاری سازد. یعنی شأنیت ابژه، خالی شدن اراده از آن و بار کردن اراده سوژه بر آن است. در این حالت است که گفته می‌شود: «ابژه در برابر سوژه یا ذهن است

که درباره‌اش گفته می‌شود، بر خلاف سوژه یا ذهن که خود گوینده است. ابژه فکر می‌شود و به‌صورت طرحی درانداخته می‌شود ولی سوژه فکر می‌کند و طرح‌اندازی می‌کند. یعنی سوژه طرحی بر ابژه بار می‌کند که از این طریق اراده و خرد سوژه در ابژه جاری می‌شود و ابژه حقیقتش را از سوژه دریافت خواهد کرد.»؛ تعریفی که از انسان در هوش مصنوعی و علوم شناختی و فضای سایبری ارائه می‌شود. از طرفی این نکته را یادآوری کنیم، انسانی که هوش مصنوعی و علوم شناختی و فضای سایبری می‌خواهند برساخته شود، در حقیقت ابژه خواهد بود. به عبارتی در سایبرنتیک و هوش مصنوعی و علوم شناختی و فضای سایبری سعی بر آن است که خرد، احساسات، عواطف و کنش‌های انسان را در الگوریتمی ریاضیاتی و پیشینی طرح‌ریزی و تبیین کنند که در این صورت می‌توان گفت که با انسان معامله‌ای ریاضیاتی می‌شود و سعی بر آن است که انسان در این فضا به‌صورت ابژه در آورده شود و اراده‌اش در اختیار سوژه قرار گیرد. مصداق این امر در جهان دوم و به‌عنوان مثال در متاورس دیده می‌شود. یکی از علت‌هایی که رسانه‌ها و فضای مجازی می‌توانند انسان را جهت‌دهی کنند و آن‌طوری که خودشان می‌خواهند پیش ببرند این است که تا حدی توانسته‌اند انسان را در طرح‌های پیشینی خودشان درآورند و نوعی از ابژه شدن انسان‌ها به دست اینترنت و کامپیوتر و رسانه‌ها رقم می‌خورد.

در حقیقت غرب به‌دنبال آن بوده است که بهشت را در زمین محقق کند، و همه چیز را در اراده انسان درآورد و معنا بخشد، و به‌صورت یک یوتوپیا درآورد که آن را «سوبژکتیویته» می‌نامیم. حال آیا ماتریکس تحقق یک یوتوپیا است؟ یعنی یوتوپیایی که در آن همه جهان ریاضیاتی شده است؟ و یا اینکه زنگ خطر برای یک یوتوپیا است؟ یعنی انتهای جایی که همه جهان ریاضیاتی شده باشد در ماتریکس و هوش مصنوعی است که سعی دارد بشریت را در خود هضم کند و اراده انسان را از او بگیرد؟ و اکنون چقدر این امر به سرانجام رسیده است؟ یوتوپیایی که در آن سوبژکتیویته است و سوژه سعی دارد جهانی را طرح‌اندازی کند و رقم بزند که در آن به نحوی خدای‌گونه شده باشد.

۳ ماتریکس

ماتریکس فضایی است که انسان‌ها را به اسارت و بندگی و بردگی خود درآورده است و انسان‌ها در خمره‌هایی شیشه ای در مایعی لزج‌مانند گرفتارند که بدن آن از همان تغذیه می‌کند و از انرژی بدنشان به عنوان سوخت ماتریکس استفاده می‌شود. انسان‌ها توسط ابرکامپیوتری کنترل می‌شوند که در آن با اتصال سیم‌هایی به بدن انسان، آنچه را در فضای کامپیوتری و کدبندی شده و برنامه‌نویسی شده ماتریکس وجود دارد بر ذهن آنها القا می‌کند، و در حالی که انسان‌ها در برنامه ماتریکس قرار دارند فکر می‌کنند که در حال زندگی روزمره و فعالیت‌ها و کار و تلاش در زندگی‌شان هستند.

اما در این میان برخی از افراد متوجه این موضوع شده و در اسارت ماتریکس نیفتاده‌اند و یا از آن گریخته‌اند، یکی از کسانی که در خود ماتریکس حضور دارد و اختلالاتی را مشاهده می‌کند، توماس اندرسون است که با نام نئو به‌عنوان هکر حضور دارد، و مورفئوس و گروه او سعی در نجات او از دست ماتریکس را دارند. آنها از نئو قدرتی را می‌بینند که امکان مبارزه و غلبه با ماتریکس را فراهم آورد یعنی او را ابرقهرمان می‌دانند.

مورفئوس که رهبر گروه است و به‌نحوی سعی دارد که انسان‌ها را از مخمصه و اسارت ماتریکس آزاد کند، تنها شهر باقی‌مانده از کره زمین (zion: زایون) را در امان نگاه دارد، در اولین دیدار با نئو به او دو قرص آبی و قرمز می‌دهد که اگر قرص قرمز را بخورد به حقیقت ماتریکس پی خواهد برد و باعث بیداری و آزادی او از ماتریکس می‌شود و اگر قرص آبی را انتخاب کند، به زندگی پیشین و روزمره و در اسارت ماتریکس برخواهد گشت. انتخاب قرص قرمز، باعث در هم شکستن واقعیتی می‌شود که نئو در آن قرار داشت و با بیدار شدن خودش را درون سفینه‌ای با اتصالاتی عجیب و غریب می‌بیند.

یکی از هوشمندی‌های نویسنده و کارگردان ماتریکس استفاده از اسطوره‌های گذشتگان در این فیلم است، مورفئوس که اسطوره خواب در اسطوره‌های باستان است، در اینجا نیز وظیفه دارد که انسان‌ها را بیدار کند. نئو پس از خوردن قرص قرمز متوجه می‌شود که عمری است در خمره‌ای تنگ خوابیده و در ماتریکس و در برنامه کامپیوتری به او القا می‌شده که زندگی می‌کرده است، مورفئوس او را از خواب بیدار می‌کند.

ماتریکس در جنگ میان انسان‌ها و هوش مصنوعی یا AI به وجود آمده است و ماتریکس توانسته است انسان ها و کره زمین را در اختیار بگیرد؛ انسان‌ها را همانند منبع انرژی استفاده کند و انسان‌ها را در محیطی برنامه‌نویسی شده و کدنویسی شده نگاه دارد و به آنها واقعیت شبیه‌سازی شده را القا کند و آن را برای اذهان انسان‌ها به‌صورت جمعی به نمایش بگذارد. به قول نیچه آنچه حقیقت است ناحقیقت است (نیچه، ۱۳۹۷، ص۱۴) و آنچه در ماتریکس به‌عنوان حقیقت به انسان‌ها خورانده می‌شود، عین ناحقیقت است و به‌عبارت دیگر هر آنچه که ماتریکس برای انسان صورت‌بندی کند و همان جهانی که برای انسان طراحی کند همان را حقیقت و واقعیت می‌پندارند یعنی اراده و حقیقت و واقعیت را ماتریکس برای انسان‌ها می‌سازد و انسان‌ها اراده شان را در اختیار ماتریکس قرار داده‌اند، و این همان چیزی است که در سوبژکتیویته رقم می‌خورد یعنی انسان اراده‌اش را به دیگری می‌سپارد و این بار متأسفانه اراده در اختیار ماشین قرار گرفته است.

اما انسان‌ها در آن گرفتار شده‌اند و چون از ابتدای زندگی در آن هستند، حس نمی‌کنند که در ناحقیقت و ناواقعیت باشند و آن را حقیقی‌ترین و واقعی‌ترین واقعیت می‌پندارند و نمی‌خواهند از آن جدا شوند، چراکه فهم حقیقت برای آنها دردناک و دلهره‌آور است. مورفئوس در پاسخ به سؤال نئو که: «آیا این وسایل واقعی نیستند؟» است، می‌گوید: «واقعیت اگر همان چیزی است که می‌توان چشید و حس کرد و دید، پس واقعیت تفسیر علائم الکتریکی توسط مغز انسان است» و چون زمین این بازی در دست انسان نیست، پس واقعیت توسط ماشین و کامپیوتر و ماتریکس ساخته و به انسان القا می‌شود. این نحوه نگاه به واقعیت باعث ایجاد شکاکیت می‌شود. مورفئوس می‌گوید که در ماتریکس «دنیا فقط به صورت شبیه‌سازی متقابل عصبی وجود دارد» و آنچه در آن می‌بینیم صرفا رؤیا است. بنابراین ماتریکس، چیزی نیست جز کنترل، که در آن دنیایی خیالی ساخته کامپیوتر به‌منظور کنترل انسان و تبدیل شدن انسان به یک منبع انرژی است.

این دنیای ایجاد شده در حالی است که هوش مصنوعی یا AI به جای انسان فکر می‌کند و تمدن انسان تبدیل به تمدن AI می‌شود. در فضای شبیه‌سازی شده از ماتریکس که به آن ساختار یا محل راه‌اندازی برنامه‌ها می‌گویند، می‌توانند هر چیزی را طراحی کنند و مثلاً لباس و تجهیزات و اسلحه و شبیه‌سازی تمرینات را می‌توان راه‌اندازی کرد یعنی در یک برنامه کامپیوتری قرار می‌گیرند، این فضا بازتاب ذهنیِ خودِ دیجیتالیِ هر فردی است که در آن قرار می‌گیرد و مثلاً نئو که در خارج از ماتریکس مو نداشت، اینجا مو در آورده است.

مورفئوس به‌همراه شهر زایون که آخرین امید و پناه انسان‌های آزاد از ماتریکس یا آزاد شده از ماتریکس است، سعی دارند با هک کردن ماتریکس و مبارزه علیه آن، انسان‌ها را آزاد کنند.

۴ شباهت ماتریکس و فضای سایبری

سوبژکتیویته یا ریاضیاتی شدن جهان با توجه به سوژه انسانی محقق شده است، حال در فیلم ماتریکس سوژه دیگر انسان نیست که همه چیز را معنا و تعین بخشد و به‌سان ابژه خودش در آورد بلکه سوژه ماشین است و این وضع خیلی خطرناک‌تر از حالتی است که انسان سوژه باشد و احساس خدایگانی کند، و برای عالم طرح‌اندازی کند. اینگونه برخلاف غایتی که غرب مدرن به‌دنبال آن بود، این دیگر انسان نیست که اراده‌اش و عقلش را خودبنیاد می‌کند، بلکه انسان اسیر و برده و ابژه هوش مصنوعی و ماتریکس می‌شود. یک نمونه عینی و ملموس و مهم که در آن این اتفاق افتاده است و هوش مصنوعی سعی در کنترل انسان دارد و تلاش دارد اراده انسان را در اختیار خود در آورده است، در هوش مصنوعیِ به کار رفته در یوتیوب و اینستاگرام و ... مشاهده می‌کنیم. در واقع هوش مصنوعیِ به کار رفته در آنها بر اساس لایک‌ها و فیلم‌ها و کلیپ‌هایی که هر کاربر در آنها مشاهده می‌کند، کلیپ و فیلم و عکس‌هایی به کاربر پیشنهاد داده می‌شود، و تریستان هریس کارمند ارشد شرکت گوگل این را تصریح کرده است و می‌گوید ۷۰ درصد فیلم‌هایی که در یوتیوب دیده می‌شود به پیشنهاد خود یوتیوب است (حراری و هریس، ۱۳۹۷). به این ترتیب اراده انسان ها را تا حد زیادی در اختیار خود گرفته است و بر اساس الگوریتم‌های خاصی ساعت‌ها انسان‌ها را همراه خود نگه می‌دارند، در حقیقت فیلم‌های پیشنهادی بعدی را به‌گونه‌ای طراحی می‌کند که گاهی بدون اینکه زمان فهمیده شود ۲ یا ۳ ساعت در آن برنامه‌ها وقت گذاشته می‌شود بدون اینکه آگاه باشیم این چند ساعت را در آنها گذرانده‌ایم و بسیار شنیده‌ایم که افرادی گفته‌اند ساعت‌ها در شبکه‌های مجازی و اینترنت چرخ می‌زدم بدون اینکه گذر زمان را بفهمم. این یعنی با الگوریتم‌های خاصی در حال برنامه‌ریزی و کنترل ذهن افراد هستند.

در فضای ماتریکس انسان‌ها در محیط برنامه‌نویسی و کدنویسی شده حضور دارند و بازتابِ ذهنیِ خودِ دیجیتالیِ هر فردی در ماتریکس به عنوان آن فرد شناخته میشود؛ مثلا نئو که در خارج از ماتریکس موهایش کوتاه بود، در فضای ماتریکس موهایی لخت و بلند داشت، یعنی بازتاب ذهنی اش از خودش با واقعیت جسمانی اش تفاوت داشت و این را می‌توانیم در متاورس ببینیم که در آن آواتار هر فردی همان چیزی است که در ذهنش اراده می‌کند و با واقعیت جسمانی‌اش ممکن است متفاوت باشد، حتی می‌تواند جنسیت خودش را در متاورس تغییر دهد.

مورفئوس در پاسخ به سؤال نئو که: «آیا این وسایل واقعی نیستند؟»، می‌گوید: «واقعیت اگر همان چیزی است که می‌توان چشید و حس کرد و دید، پس واقعیت تفسیر علائم الکتریکی توسط مغز انسان است» و چون زمین این بازی در دست انسان نیست، پس واقعیت توسط ماشین و کامپیوتر و ماتریکس ساخته و به انسان القا می‌شود، این بدان معنی است که اراده انسان توسط ماتریکس متعین می‌شود، یعنی انسان در ماتریکس به ابژه تبدیل شده است. از طرف دیگر با توجه به اینکه نئو واقعیت را تفسیر علائم الکتریکی توسط مغز می‌داند، یعنی واقعیت کاملاً ریاضیاتی شده و کدبندی شده است، یعنی انسان همچون ماشین

و کامپیوتر دانسته می‌شود که واقعیت برای او تفسیر علائم الکتریکی توسط مغز است. این مدل از تفسیر انسان را می‌توان در علوم شناختی دید، که نظریه محاسباتی ذهن در آن مهم‌ترین نظریه و با نفوذترین نظریه است. در پی تلاش برای پاسخگویی به آزمون تورینگ این ایده نیز به وجود آمد که انسان اساساً شبیه یک ماشین محاسباتی یا کامپیوتر است. از آنجا که گزاره‌های منطق را می‌توان به فرمان‌های محاسباتی برگرداند، و ماشین‌هایی که می‌توانستند فرمان‌های محاسباتی را اجرا کنند، یعنی ماشین‌هایی که قابلیت فکر کردن دارند و همین امر را درباره انسان‌ها نیز جاری می‌دانستند، یعنی انسان همچون این ماشین‌ها فرمان‌های محاسباتی و منطقی را اجرا می‌کند و مغز را سخت‌افزار یک کامپیوتر تلقی می‌کردند. در علوم شناختی، معتقد بودند که انسان‌ها همانند کامپیوتری هستند که اطلاعات را از محیط می‌گیرد و به‌صورت رمز در می‌آورد و بر روی آنها عملیات محاسباتی و پردازش اطلاعات انجام می‌دهند و به‌صورت اطلاعاتی پردازش شده یا محاسبه شده در می‌آورند (Loftus, 2019, pp1-13). این‌گونه در هوش مصنوعی سعی دارند که فرایندهای ذهنی را به نحو الگوریتمی توصیف کنند و مدل‌های صوری و ریاضیاتی برای رفتار و ذهن انسان کنند. مدل ریاضیاتی برای انسان و ذهن در عمیق‌ترین معنای آن این است که انسان به ابژه تبدیل می‌شود و با او معامله ریاضیاتی می‌شود و امکان کنترل او فراهم می‌شود.

مورفئوس در توضیح برای نئو درباره ماتریکس، آن را جهانی خیالی، ساخته کامپیوتر به‌منظور کنترل انسان معرفی می‌کند، که انسان را به‌مثابه انرژی نگهدارنده ماتریکس نگه دارد، چراکه انرژی ماتریکس از انسان‌ها تأمین می‌شود، یعنی انسان را همچون باتری و انرژی می‌داند که بقای آن به انسان است و برای اینکه ادامه پیدا کند بایست انسان را در کنترل خودش داشته باشد. سایبرنتیک (که cyberspace یا فضای سایبری از آن گرفته شده است) مطالعه بازخورد، ارتباطات و کنترل در حیوان و ماشین است. (Wiener, 1948, p18)، سایبرنتیک بر آن بود که علاوه بر ماشین و کنترل همه زمینه‌های اجتماعی و اخلاقی و انسانی و ... را به تسخیر خود درآورد و همه مسائل را بر اساس سایبرنتیک حل و فصل نماید، و همه شئون انسانی و حیوانی و نباتی را کنترل کند.

فضای سایبری که برگرفته از سایبرنتیک است، اولین بار توسط گیبسون در رمان‌های علمی تخیلی به کار گرفته شد همان‌گونه که ماتریکس نیز فیلمی علمی تخیلی است. گیبسون فضای سایبری را توهمی توافقی می‌داند که روزانه توسط میلیاردها کاربر بر اساس نمایشی گرافیکی از داده‌های انتزاعی در بانک‌های هر کامپیوتر در سیستم انسانی به‌وجود می‌آید (Gibson, 1984, p69). در ماتریکس نیز با همین امر روبرو هستیم که انسان‌ها در توهم‌شان در ماتریکس زندگی می‌کنند که این توهم روزانه توسط سیستم ماتریکس و بر اساس فضای گرافیکی و کدنویسی و برنامه‌نویسی شده ماتریکس بر ذهن انسان‌ها تحمیل می‌شود.

این توهم روزانه باعث زندگی‌ای در فضای ماتریکس می‌شود و مأمور اسمیت به نئو می‌گوید که تو دارای دو زندگی هستی، در یکی توماس اندرسون که در آن برنامه‌نویس یک شرکت معتبر برنامه‌نویسی هستی و دیگری نئو، که در آن هکری با نامی دیگر و هویتی دیگر. در حقیقت جهان ماتریکس که برای اداره‌اش قوانین خاصی را دارد، مأمورانی دارد که اجازه نمی‌دهد انسان‌ها از این توهم بیرون بیایند و توماس اندرسون در فضای ماتریکس حضور دارد اما دچار اختلالاتی می‌شود و احساس می‌کند همه چیز درست نیست، پس با نام نئو هویتی دیگر برای خودش می‌سازد که پس از آزاد شدن او از این فضا نیز نئو اسمی است که مورفئوس

برای او انتخاب می‌کند. اما این عبارت که نئو دارای دو زندگی است، در فضای سایبری نیز به‌عنوان زندگی دوم شناخته می‌شود که در فضای سایبری هر کس می‌تواند هویتی به غیر از هویت اصلی خودش داشته باشد و با آن زندگی کند و حتی پول درآورد و جنسیت خودش را تعیین کند و آواتاری از خود بسازد که دوست دارد آن باشد.

۵ برده شدن و اسارت انسان در ماتریکس

مورفئوس درباره ماتریکس به نئو می‌گوید ماتریکس را همه جا می‌شود حس کرد. اما این جهان (ماتریکس) پرده‌ای بر روی چشمان انسان‌ها انداخته تا حقیقت را نبینند. این حقیقت که انسان در ماتریکس برده است و در اسارت به دنیا آمده است. تولد در زندانی که طعم و رنگ و بوی آن را حس نمی‌کند چرا که در آن به دنیا آمده و از ابتدا با آن انس گرفته و چیزی غیر از آن را تصور نمی‌کند، یعنی در زندانی است که افکار و اندیشه‌ها را در بر گرفته و غیر از آن را نمی‌توان دید و فردی مثل نئو تنها ناسازگاری و ناهماهنگی‌هایی حس می‌کرد، به‌همین دلیل پس از آزاد شدن از ماتریکس مورفئوس به او گفت: به کسی نمی‌شود توضیح داد که ماتریکس چیست و باید خودت آن را ببینی.

و مورفئوس درباره آن توضیح میدهد که در ابتدای قرن ۲۱ انسان سرمست از عظمت خودش بود زمانی که موفق به ساختن هوش مصنوعی (AI) شد، یعنی شعوری منحصر به فرد که قالب نسل کاملی از ماشین‌ها شد. در ابتدای قرن ۲۱، هوش مصنوعی متکی به انرژی خورشیدی بود و بر این باور بودند که یک منبع انرژی که مثل خورشید بی‌پایان باشد برای ادامه زندگی نیاز دارند. جسم انسان بیش از یک باتری ۱۲۰ ولت برق و بیش از ۲۵۰۰۰ واحد انرژی حرارتی تولید می‌کند. ماشین‌ها با بهره‌گیری از نوعی آمیزش تمام انرژی‌ای که لازم داشتند به‌دست آورند و مزارعی بی‌پایان هست که انسان در آن متولد نمی‌شود، بلکه کِشت می‌شود. یعنی انسان در ماتریکس به نحوی تصویر می‌شود که همانند یک باتری و منبع انرژی و ماشین است و در این تفسیر از انسان، با انسان معامله‌ای ماشینی و ریاضیاتی شده است و دیگر قلب و کرامت و ایثار و ... برای انسان مطرح نیست بلکه انسان را به ماشین و ریاضیات فروکاستند، یعنی انسان به‌مثابه ابژه درآمد و اراده و آگاهی‌اش توسط ماتریکس گرفته شد و اراده ماتریکس بر او تحمیل شد و آن آگاهی‌ای که ماتریکس بخواهد برای او حاصل می‌شود و به‌همین دلیل انسان برده و ابژه می‌شود.

انسان‌ها در سیستم قدرتمند ماتریکس به‌صورت عادی متولد نمی‌شوند، بلکه در یک مزرعه کشت می‌شوند و پرورش می‌یابند و نهایت استثمار از جسم انسان می‌شود و روح و ذهن انسان را هم در اختیار گرفته‌اند و هر طور که بخواهند انسان فکر می‌کند.

حال سؤال مهمی پیش می آید که آیا انسان‌ها در شبکه‌های مجازی و فضای سایبری به‌صورت کنونی وضعیتی مشابه دارند یا نه؟ یعنی آیا ذهن انسان‌ها در حال کنترل است یا نه؟ این در حالی است که در علوم شناختی به سمتی می‌روند که انسان‌ها را همچون ماشین و ابژه و دستگاه محاسباتی کنند و برای انسان الگوریتم پیاده کنند، یعنی ذهن انسان را در اختیار بگیرند. درست است که همانند ماتریکس برده نشده‌اند اما تا حدی به دنبال آن هستند که انسان را به‌صورت ریاضیاتی در آورند و این زنگ خطر است.

بنابراین ریاضیاتی شدن و ابژه شدن و اسارت انسان در ماتریکس در دو جنبه کامپیوتری شدن و کدهای کامپیوتری و برنامه‌نویسی برای ایجاد ادراک و آگاهی در مغز انسان و همچنین ماشینی شدن انسان با توجه به این که در خمره‌های شیشه‌ای در مایعی لزج و مغذی به‌عنوان انرژی و باتری در ماتریکس است.

۶ خودآگاهی و آزادی انسان در ماتریکس و فضای سایبری

اما آزادی از ماتریکس چگونه رخ می‌دهد؟ با این فرض که در فضای سایبری و شبکه‌های مجازی تا حدی انسان دچار غفلت و ناآگاهی شده است، و سعی در کنترل انسان و آگاهی انسان دارند، در فضای سایبری چگونه این آزادی رخ می‌دهد؟

در اولین لحظه‌ای که نئو فهمید که ماتریکس دقیقاً چیست و چه می‌کند و انسان‌ها در آن کشت می‌شوند و انسان عملاً تبدیل به منبع انرژی شده و در حال کنترل کردن است، آنقدر برایش غیر قابل باور بود که دیوانه‌وار خواستار خروج از محیط شبیه‌سازی شده به ماتریکس را داشت، و پس از خروج از آن حالش بد بود. البته روز بعد به دلیل مسئولیت سنگینی که خودش حس می‌کرد و مورفئوس باور داشت که او شخص برگزیده و ابرقهرمان برای شکست دادن ماتریکس است، و البته هیجانی که در فضای ماتریکس حس می‌کرد، دوباره به فضای شبیه‌سازی شده ماتریکس برگشت تا مأموریتش –نجات انسان‌ها از ماتریکس– را انجام دهد.

اما شخصی دیگر به نام سایفر در سفینه مورفئوس بود که اگرچه با قرص قرمز از ماتریکس نجات یافته بود اما به دلیل سختی‌هایی که حس می‌کرد، نمی‌خواست ادامه دهد، یعنی همان حس خوبی که ماتریکس به همه انسان‌ها منتقل می‌کرد و زندگی خوبش در ماتریکس را بر آزادی‌اش ترجیح می‌داد، و زندانی بودن و برده بودن و استفاده از او به‌عنوان باتری و منبع انرژی در ماتریکس را به‌دلیل سختی‌هایی که مبارزه با ماتریکس داشت، به جان می‌خرید.

قصه کپسول آبی و قرمز و فهمیدن حقیقت و اینکه آیا انسان‌ها به حقیقت روی می‌آورند یا از آن گریزان هستند، همانند تمثیل غار افلاطون است که در آن افلاطون بیان می‌کند که بر دست و پای انسان‌ها زنجیرهایی بسته شده است و در تمام زندگی آنها فقط سایه‌هایی که روبرویشان وجود دارد را می‌بینند و این سایه‌ها از بیرون که خورشید حقیقت وجود دارد بر دیوار روبروی افراد در غار تابیده می‌شود، اما چون چشم‌ها و بدن‌ها به این تاریکی و زندانی بودن عادت کرده و نگاه به نور و خورشید را ناخوشایند و پرمشقت می‌بینند (Plato, 1997,$541)، پس اگر کسی از آنها آزاد شود و به بیرون از غار برود و بگردد و بخواهد آنها را نجات دهد، با او مبارزه می‌کنند و حتی ممکن است او را بکشند. این امر در ماتریکس رخ داده است و سایفر سعی داشت که گروه مورفئوس و نئو را بکشد و خودش به فضای اسارت در ماتریکس برگردد.

در شبکه‌های مجازی و فضای سایبری نیز به نحوی انسان در آن تخدیر می‌شود که کسانی که در آن حضور دارند حتی می‌گویند که واقعاً گذر زمان چند ساعته و گشت‌وگذار در آن را نفهمیدیم، اما ناظر بیرونی که بخواهد آنها را بنگرد متوجه تخدیر انسان‌ها در آن می‌شود؛ پس احتمالاً احساسی ناخوشایند برایش دارد (همان‌طور که نئو پس از فهمیدن و دیدن حقیقت ماتریکس این احساس برایش پدید آمد)، اما برای کسانی که در شبکه‌های مجازی سیر می‌کنند، نوعی لذت و حس خوشایندی هست که احتمالاً با استدلال و منطق

نتوان آنها را مجاب کرد، چون آن را نمی‌بینند بلکه حس و لذتی آنها را فرامی‌گیرد که امکان فهم حقیقت آن برایشان سخت می‌شود. به نظر مک‌لوهان این از اثرات تکنولوژی ماشینی و رسانه است که در آن سعی دارند الگوهای احساسی انسان را تسخیر کنند، و پس از تسخیر الگوهای احساسی هر کسی، او همانند موم در دست تسخیرکنندگان خواهد بود، اینکه الگوهای احساسی انسان را تسخیر می‌کنند و انسان را مسخر و مسحور خود می‌کنند به‌نحوی همانند این است که بگوییم انسان را به‌صورت ریاضیاتی کنترل کنند و اختیار و اراده انسان را تا حدی در کنترل خودشان بگیرند و انسان به‌مثابه ابژه درآورند.

اما با همه این اوصاف هر انسانی یک آستانه تحملی دارد و این احتمال وجود دارد که اگر آستانه تحمل انسان‌ها در حالتی که قرار است همچون ابژه شوند به سرآید، آنگاه همچون نئو دیوانه‌وار خروج از شبکه‌های مجازی و در اختیار گرفتن آن را طلب کنند و این البته به آگاهی و خودآگاهی انسان‌ها بستگی دارد.

آنجایی که انسان به صورت خودآگاه وارد ماتریکس می‌شود، آنگاه است که امکان گذار از آن و نجات انسان به‌وجود می‌آید، آیا در فضای سایبری و شبکه‌های مجازی و اینترنت که انسان دچار رخوت و سستی و ... می‌کند و سعی می‌کند اراده انسان‌ها را بگیرد، نسخه نهایی همین است؟ همان‌گونه که در نئو چیزی را تعبیه می‌کنند که در آن امکان رفتن به ماتریکس به‌صورت خودآگاه وجود داشته باشد یعنی با اتصال یک ورودی او را به فضای ماتریکس می‌فرستند و نئو همان قهرمانی می‌شود که امکان مبارزه علیه گرفتن اراده کامل از انسان در او فراهم می‌شود، انسان‌ها نیز اگر آگاهانه در این فضا حضور داشته باشند و الگوهای احساسی آنها توسط رسانه‌ها و فضای سایبری تسخیر نشود، آنگاه امکان حضوری فعال و به‌دور از ابژه شدن و ریاضیاتی شدن را خواهند داشت.

در فیلم ماتریکس نشان داده شد که تنها خودآگاهی برای غلبه بر ماتریکس کافی نیست و به دنبال ابرقهرمان یا برگزیده بودند تا نجات یابند. ویژگی نئو برای نجات دادن آنها حرکات عصبی نئو است که بالاتر از حد معمول بود و باعث می‌شد در دنیای ماتریکس، مبارزه‌ای قوی‌تر و سریع‌تر از مورفئوس ارائه دهد یعنی حرکات عصبی‌ای که در ماتریکس مبارزه را کنترل می‌کند. همین عامل چون در نئو بسیار سریع است در ماتریکس هیچ کس حریف او نمی‌شود و او به ابر انسان تبدیل می‌شود. البته شرط آن این است که ذهن نئو در ماتریکس آزاد شود که قابلیت‌های خودش را بفهمد، مورفئوس سعی دارد که ذهن نئو را رها کند تا از یک ساختمان به ساختمان دیگر پرشی به طول چند ده متر داشته باشد ولی چون هنوز ذهن نئو آزاد نشده است آن را انجام نمی‌دهد. پس در ماتریکس ذهن آزاد شده و حرکات عصبی است که باعث می‌شود نئو به ابرقهرمان تبدیل شود و کم کم نئو به آن دست می‌یابد و در انتهای فیلم به حدی می‌رسد که می‌تواند در ماتریکس حتی سرعت گلوله ها را متوقف کند. نئو وقتی پیشِ پیشگو رفته بود، توجهش به کودکی که قاشق را با قدرت ذهنش خم می‌کرد، افتاد، کودک به نئو گفت: «سعی نکن قاشق را خم کنی، چون نمی‌توانی. سعی کن حقیقت را درک کنی که قاشق وجود ندارد و آن وقت می‌فهمی آنچه خم می‌شود قاشق نیست، بلکه خود تو هستی که خم می‌شوی». در حقیقت نئو با همین قدرت توانست گلوله‌هایی را که به او شلیک می‌شود را متوقف کند چون حقیقت ماتریکس را دریافته بود و فهمیده بود که در حقیقت گلوله‌ای وجود ندارد و ماتریکس است که آن را بر ذهن‌ها تحمیل می‌کند. از طرفی به گفته مورفئوس قدرت و سرعت افراد ماتریکس (که مهم‌ترین و قدرتمندترین آنها مأمور اسمیت است) ریشه در جهانی دارد که متکی به قوانین آن

جهان است، پس در مقابله با نئو که قدرت و سرعت بیشتری دارد درمانده خواهند بود و نئو همان ابر قهرمانی است که می‌تواند فضای ماتریکس را بشکند.

اما اینها در فیلمی علمی تخیلی رخ داده بود، در فضای سایبری و شبکه‌های مجازی و رسانه‌ها که سعی در برده کردن انسانها دارند، سعی آنها بر آن است که انسان همچون شیء باشد و ریاضیاتی شود، این‌گونه سعی بر آن است که روح و قلب انسان‌ها را ضعیف کنند تا بتوانند او را ابژه کنند و در این فضا هر چقدر انسان‌ها از اصالت و قلب و روح اصیل خودشان جدا نشوند، ابژه نمی‌شوند اما اگر روح و قلب انسان‌ها ضعیف شد آنگاه اراده‌ها سست می‌شود و همچون شیئی قابل کنترل درخواهند آمد و وظیفه همین است که انسان‌ها از اصالت و روح و قلب خودشان جدا نشوند تا اسیر فضای سایبری و شبکه‌های مجازی و رسانه نشوند. البته این به معنای استفاده نکردن آنها نیست، بلکه اکنون جهان به نحوی است که بایست از آنها استفاده شود اما آگاهانه حضور داشتن در آن و تخدیر نشدن باعث می‌شود که بازیچه دیگران نشوند.

۷ نتیجه‌گیری: ماتریکس آمریکایی

ادوارد کورتین واقعیت جدید آمریکا را زندگی در ناواقعیت می‌داند که در آن مردم مصرف‌کنندگان غیرواقعیت شده و از تجربه مستقیم دلسرد شده‌اند. تماشای زندگی از نتفلیکس یا فیس‌بوک به فیلم زندگی تبدیل شده است و اعوجاج نورانی واقعیت دستکاری شده از یک جامعه نمایشگری به‌گونه‌ای است که گویی مردم را از واقعیت‌های بنیادین دور می‌کند و این ایده را تقویت می‌کند که واقعیتی که از طریق فانتزی‌های نمایشگری دیده شود واقعیت است و این را پورنوگرافی آمریکایی می داند که در ناواقعیت زندگی از طریق برنامه‌های تلویزیونی، فیلم‌ها و دل‌مشغولی‌های آن‌لاین زندگی می‌کند (کورتین، ۱۳۹۷)[۱]. این ایده ادوارد کورتین نه در فضایی غیر از زمین و در فیلم‌های سایبرپانکی و نه در آینده‌ای دور و نه در فیلمی علمی-تخیلی، بلکه در واقعیت و در جامعه‌ای که در آن زندگی می‌کند در حال رخ دادن است. مردمی که در ناواقعیت زندگی می‌کنند و از تجربه مستقیم با زندگی دلسرد شده‌اند، دقیقاً همانند ماتریکس است که مردمِ آن در فضای ناواقعیت که ماتریکس برایشان ساخته زندگی می‌کنند، و از روبرو شدن با حقیقت دلسرد هستند، همان‌گونه که سایفر بردگی در ماتریکس را بر زندگی واقعی ترجیح می‌داد.

در ماتریکس آمریکایی واقعیت و زندگی از طریق شبکه‌های مجازی -ننفلیکس یا فیس بوک- در جریان است و ناواقعیت را واقعی می‌پندارند و در دل‌مشغولی‌های فضای سایبری زندگی می‌کنند. البته این فقط برای آمریکا نیست -هر چند شاید در آمریکا به‌نحوی عمیق‌تر در جریان است- بلکه تذکری است برای تمامی جوامع که ممکن است همه در ناواقعیت زندگی کنند و تجربه مستقیم زندگی را رها کنند. اینها همه یعنی

[۱] «ایالات متحده جامعه‌ای پورنوگرافیک است. منظورم از پورنوگرافیک هم فقط به معنی فروش رایج و همه‌جایی سکس همراه با بهره‌کشی نیست؛ کاری که از طریق تمامی رسانه‌ها برای به جنبش درآوردن غرایز جنسی یک جامعه گرفتار معضل محظوظ شدن از طریق تماشای صحنه‌های جنسی انجام می‌شود؛ جامعه‌ای که در ناواقعیت «زندگی» نمایشگری و سکس نمایشگری از طریق برنامه‌های تلویزیونی، فیلم‌ها و دل‌مشغولی‌های آنلاین زندگی می‌کند. منظورم یک شعور کالاسازی شده است که در آن همه‌کس و همه‌چیز بخشی از یک حلقه روسپی‌گری با ژرف‌ترین معنایی که از پورنوگرافی مستفاد می‌شود است؛ برای فروش و خرید. و مصرف کردن ازطریق به‌دست آوردن، هزینه کردن و فروختن. گرفتار در تور برادر بزرگ که کار او اطمینان یافتن از این است که تمام چیزهای اساساً انسانی و فیزیکی از این روند متأثر می‌شود.» (کورتین، ۱۳۹۷)

گام‌هایی که انسان را تبدیل به برده و ابژه در فضای سایبری می‌کند که از طریق ریاضیاتی شدن جهان و انسان امکان وقوع می‌یابند.

مراجع

[۱] اسپینوزا، باروخ، ۱۳۹۲، اخلاق، ترجمه محسن جهانگیری، تهران، مرکز نشر دانشگاهی.

[۲] حراری، یووال نوح؛ هریس، تریستان، ۱۳۹۷، وقتی فناوری شما را بیشتر از خودتان می شناسد، وب‌سایت: https://www.farsnews.ir/news/13971025001399

[۳] دکارت، رنه، اصول فلسفه، ترجمه منوچهر صانعی، تهران، انتشارات بین‌المللی الهدی، ۱۳۷۱.

[۴] کورتین، ادوارد، ۱۳۹۷، واقعیت جدید آمریکا: زندگی در ناواقعیت، وب‌سایت: https://www.farsnews.ir/news/13971015001243

[۵] نیچه، ۱۳۹۷، چنین گفت زرتشت، ترجمه داریوش آشوری، تهران، انتشارات آگه.

[۶] هابز، لویاتان، تهران، نشر نی، ترجمه حسین بشیریه، ۱۳۹۳.

[۷] هیدگر، مارتین، ۱۳۸۸، چه باشد آنچه خوانندش تفکر، ترجمه سیاوش جمادی، تهران، انتشارات ققنوس.

[۸] هیدگر، مارتین، ۱۳۹۵، عصر تصویر جهان، ترجمه یوسف اباذری، مجله ارغنون شماره ۱۱ و ۱۲.

[9] Gibson, William (1984). Neuromancer. New York: Ace Books.

[10] Loftus ,Geoffrey R.; Loftus, 2019, Elizabeth F., Human Memory: The Processing of Information, New York, Psychology Press.

[11] Plato (1997), Complete Works, Trans by G. M. A. Grube Edited by Johnm Cooper, United States of America: Hackett Pulishing Company.

[12] Wartenberg, Thomas, 2015, Philosophy of Film, Stanford Encyclopedia of Philosophy.

[13] Wiener, Norbert, THE HUMAN USE OF HUMAN BEINGS, MIT Press, 1951.

[14] Wiener, Norbert, Cybernetics or Control and Communication in the Animal and the Machine, MIT Press, 1948.

بهبود بازشناسایی شخص با استفاده از یادگیری انتقالی و شبکه‌های سیامی

سجاد عموئی ششکل [۱]، کاظم فولادی قلعه [۲]، حسین آقابابا [۳]

[۱] دانش‌آموخته کارشناسی ارشد مهندسی فناوری اطلاعات، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
sajad.amouei@ut.ac.ir
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی یادگیری عمیق دانشگاه تهران
kfouladi@ut.ac.ir
[۳] دانشیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
aghababa@ut.ac.ir

چکیده

بازشناسایی شخص در جامعه تحقیقاتی محبوبیت بالایی به‌دست آورده و دلیل آن افزایش کاربردها و اهمیت آن در صنعت نظارت است. بازشناسایی شخص به‌دلیل وجود تغییرات درون‌کلاسی و بین‌کلاسی در دوربین‌های مختلف همچنان به‌عنوان یک مسئله‌ی چالشی مورد بررسی قرار می‌گیرد. در این مقاله یک شبکه از نوع سیامی معرفی می‌شود که جفت تصاویر را دریافت کرده و سپس با استفاده از شبکه پیش‌آموزش داده شده، ویژگی‌های تصاویر را استخراج می‌کند و در نهایت خروجی توسط یک تابع اتلاف تصدیق تعیین می‌شود. به‌منظور به‌دست آوردن ویژگی‌های عمیق‌تر از تصاویر عابران پیاده، از شبکه پیش‌آموزش داده شده EfficientNet B0 برای استخراج ویژگی‌ها استفاده کردیم. آزمایش‌ها را روی مجموعه داده CUHK01 برای نشان دادن دقت روش پیشنهادی انجام دادیم. دقت روش پیشنهادی در رتبه ۱، رتبه ۵، رتبه ۱۰، رتبه ۱۵ و رتبه ۲۰ به ترتیب ٪۷۰، ٪۹۵، ٪۹۹، ٪۹۹ و ٪۹۹ می‌باشد. نتایج نشان می‌دهد که روش ارایه شده نسبت به روش‌های به‌روز دارای عملکرد بهتری است.

کلمات کلیدی: بازشناسایی شخص، شبکه سیامی، اتلاف تصدیق، EfficientNet B0.

۱ مقدمه

معمولاً مسئله بازشناسایی شخص به‌عنوان یک مسئله بازیابی تصویر بررسی می‌شود، که هدف آن تطبیق عابرپیاده در چند دوربین است [۱، ۲، ۳]. تصویر عابرپیاده موردنظر به عنوان پرس‌وجو داده می‌شود، و بازشناسایی شخص تعیین می‌کند که این عابرپیاده در کدام یک از دوربین‌های دیگر مشاهده شده است

[۴]. اخیراً در حوزه تحقیقاتی بازشناسایی شخص پیشرفت‌های قابل توجهی انجام شده است که یکی از دلایل آن ایجاد مجموعه داده‌های بزرگتر از تصاویر عابران پیاده است. دلیل دیگر این پیشرفت‌ها مربوط به یادگیری توصیف‌گرهای عابرپیاده توسط شبکه‌های عصبی کانوولوشنال (CNN) است. علیرغم پیشرفت‌های صورت‌گرفته توسط محققان بینایی کامپیوتر، چالش‌های حل‌نشده بسیاری در این حوزه وجود دارد [۱].

مدل‌های بازشناسایی شخص بسیاری توسعه داده شده که از ویژگی‌های سطح پایین مانند رنگ [۵]، بافت و ساختار مکانی [۶] استفاده می‌کردند. این ویژگی‌های بصری در مقابل تغییرات نور، زاویه دید و عدم تراز مقاوم نبودند. درک انسانی، تفاوت افراد را به‌وسیله ویژگی‌های سطح بالا مانند موی بلند، رنگ پیراهن، رنگ کوله‌پشتی و غیره به‌آسانی تشخیص می‌دهد. این خصوصیت می‌تواند بازنمایی از ویژگی‌های معنایی سطح بالا یک شخص را استخراج کند و در برابر تغییرات نور و عدم تراز تصویر نسبت به ویژگی‌های سطح پایین مقاوم‌تر است. برای این منظور نیاز است که داده‌ها برچسب‌گذاری شوند که هزینه بسیار زیادی دارد. در نتیجه دستیابی به مجموعه داده آموزشی کافی دارای برچسب خصوصیت انسانی بسیار دشوار است.

زمانی که تعداد داده‌های آموزشی به مقدار زیادی موجود است، انتقال بازنمایی یادگرفته شده از مجموعه داده بزرگ اهمیت ویژه‌ای پیدا می‌کند. اکنون از یادگیری انتقالی در اکثر کارهای مربوط به بازشناسایی شخص استفاده شده است. در مسئله بازشناسایی شخص تعداد تصاویر برچسب‌گذاری شده به چند صد عدد می‌رسد و روش‌های موجود عموماً از مدل‌های پیش آموزش داده شده روی مجموعه داده‌های بزرگتر استفاده می‌کنند و سپس مدل را روی مجموعه داده هدف تنظیم می‌کنند. زمانی که از مجموعه داده بازشناسایی شخص بزرگتر برای یادگیری انتقالی استفاده می‌کنیم، ممکن است تفاوت زیادی در زاویه دوربین و شرایط تصویربرداری وجود داشته باشد. در نتیجه مدل‌هایی که از یادگیری انتقالی استفاده می‌کنند بهبود عملکرد کم یا دارای عملکرد منفی می‌شوند [۱].

روش ارایه شده برای استخراج ویژگی‌های سطح بالا از CNN استفاده می‌کند. در سال‌های اخیر معماری‌های CNN بهبود عملکرد چشمگیری در حل وظایف بینایی ماشین از خود نشان دادند. همچنین مطالعاتی در زمینه ویژگی‌های به‌دست آمده توسط CNN انجام شد. ویژگی‌هایی که توسط CNNها بدست می‌آید دارای ساختار سلسله مراتبی است. ویژگی‌های به‌دست آمده توسط لایه‌های پایینی CNN مشابه ویژگی‌های استخراج شده سطح پایین مانند فیلترهای رنگ و لبه است. لایه‌های بالاتر CNN ویژگی‌های بسیار متفاوت وسطح بالایی را استخراج می‌کنند که شبکه می‌تواند با این ویژگی‌ها کلاس مورد نظر را تشخیص دهد [۷]. شبکه پیشنهادی ما می‌تواند ویژگی‌های سطح بالا توسط لایه‌های بالایی CNN استخراج کند. شبکه پیشنهادی از مدل پیش‌آموزش داده شده EfficientNet B0 [۸] بهره می‌برد که روی مجموعه داده ImageNet آموزش داده شده است.

اگر تابع تطبیق مناسبی برای محاسبه فاصله بین ویژگی‌ها تعیین شود، استخراج کننده ویژگی می‌تواند ویژگی‌های متمایز کننده‌ای از بازنمایی شخص را آموزش ببیند. تعدادی از روش‌های موجود توزیع مشابهت روی جفت تصاویر پرس و جو و گالری براساس نقشه ویژگی[1] آنها می‌سازند. در روش ما شبکه محدود به

[1] Feature map

شکل ۱: نمونه‌ای از پرس‌وجو و تصاویر بازیابی شده روی مجموعه داده CUHK01

مقایسه نقشه ویژگی‌ها متناظر دو تصویر نیست و با مقایسه ویژگی‌های سطح بالا و ترکیب آنها دارای استراتژی جدیدی است. روش ارایه شده از چندین نقشه ویژگی برای مقایسه دو تصویر استفاده می‌کند. علاوه بر این، ارتباط بین این ویژگی‌ها را به‌صورت داده‌محور بررسی می‌کند.

در این مقاله هدف ما ایجاد یک شبکه انتها به انتها است که به هر دو تصویر عابرپیاده ورودی به شبکه، یک امتیاز مشابهت تعیین کند. مثالی از پیش‌بینی شبکه در شکل ۱ نشان داده شده است. روش ارایه شده از شبکه پیش‌آموزش داده شده EfficientNet B0 به‌عنوان استخراج‌کننده ویژگی‌های سطح بالا بهره می‌برد که می‌تواند با استفاده از آن رابطه بین‌کلاسی[۲] و درون‌کلاسی[۳] در ویژگی‌های عمیق سطح بالا را پیدا کند. براساس مشاهدات، شبکه پیش‌آموزش داده EfficientNet B0 به‌وسیله‌ی متعادل کردن عمق، عرض و وضوح به کارآیی بهتری دست می‌یابد. EfficientNet B0 از یک روش مقیاس‌گذاری ترکیبی برای ثابت نگه داشتن نسبت‌ها در سه بُعد بهره می‌برد که منجربه تقویت محاسبات و همچنین دقت می‌شود [۸]. امتیاز مشابهت به‌وسیله‌ی تجزیه و تحلیل رابطه بین ویژگی‌های استخراج شده محاسبه می‌شود. مقدار اولیه پارامترهای شبکه پیش‌آموزش داده شده براساس مجموعه داده ImageNet مقداردهی شده است. برای تنظیم پارامترها باید آن را روی مجموعه داده آموزشی بازشناسایی شخص مجدداً آموزش دهیم که باعث می‌شود پارامترهای شبکه طبق مسئله به‌روزرسانی شود و بتواند ویژگی‌های متمایزکننده از تصاویر عابران پیاده را به‌خوبی استخراج کند.

[2] Inter-Class
[3] Intra-Class

۲ کارهای گذشته

به‌طور کلی فرآیند بازشناسایی شخص شامل دو بخش است: یک بخش مربوط به استخراج ویژگی‌ها از تصاویر ورودی و بخش دیگر معیار مشابهت برای مقایسه ویژگی‌های سراسر تصویر. هدف اصلی جست‌وجو برای یافتن بازنمایی ویژگی‌ها، یافتن ویژگی متمایزکننده است که در مقابل تغییرات شرایط نور، حالت شخص و زاویه دوربین مقاومت بیشتری داشته باشد. روش‌های اولیه به ویژگی‌های دستی طراحی شده مانند HSV هیستوگرام رنگ [۶]، LBP و ویژگی‌های Garbo [۹]، SIFT [۲] و غیره متکی بودند. در کنار این ویژگی‌ها، از معیارهای مشابهت مانند یادگیری معیار Mahalanobis [۱۰]، LADF [۱۱] و مسافت‌های وزنی برابری [۱۲] و غیره استفاده می‌شد.

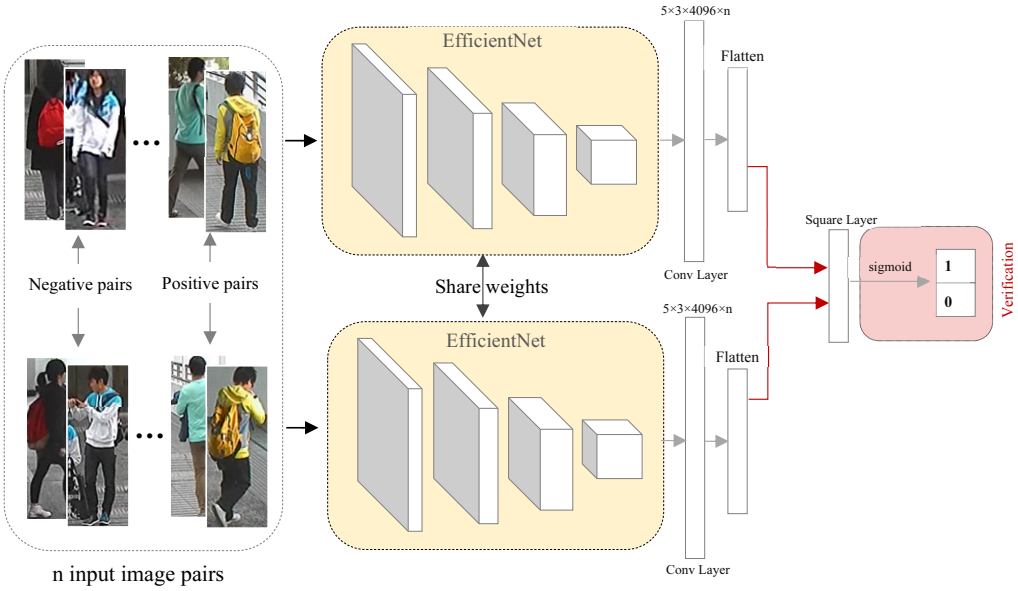
در سال‌های اخیر، عملکرد خوب یادگیری عمیق دلیلی شد تا بسیاری از محققان از آن برای به‌دست آوردن ویژگی‌های ظاهری و معیارهای فاصله برای بازشناسایی شخص استفاده کنند [۴]، [۱۳]، [۱۴]. روش یادگیری معیار عمیق [۱۵]، تصویر ورودی را به سه قسمت افقی بخش‌بندی می‌کند و این بخش‌ها از دولایه کانوولوشنال و یک لایه تمام متصل عبور می‌کند و در خروجی یک بردار برای تصویر به‌دست می‌آید. مشابهت دو بردار خروجی توسط فاصله کسینوسی محاسبه می‌شود. معماری FPNN [۴] با داشتن یک لایه تطبیق تکه نسبت به معماری قبل متفاوت است، که پاسخ‌های کانوولوشنال دو تصویر در راه‌راه‌های افقی متفاوت ضرب می‌کند. روش ImprovedReID [۱۳] مدل FPNN به‌وسیله محاسبه ویژگی‌های اختلاف همسایگی متقابل ورودی بهبود داده است، که ویژگی‌های تصویر ورودی با ویژگی‌های محلی همسایه تصویر دیگر مقایسه می‌کند. با این حال ممکن است استراتژی‌های تطبیق با کارآیی محاسباتی کم یا محدودیت اطلاعات ساختار مکانی مواجه شوند.

۳ روش ارایه شده

۱.۳ نمای کلی

معماری شبکه بازشناسایی شخص ارایه شده در شکل ۲ به تصویرکشیده شده است. این شبکه برپایه یک مدل کانوولوشنال سیامی است که از اتلاف تصدیق بهره می‌برد. هدف از مدل ارایه شده، یادگیری بازنمایی ویژگی‌های محلی جفت تصاویر ورودی است که با استفاده از آنها امتیاز مشابهت تعیین می‌شود یا ویژگی‌های متمایزکننده برای طبقه‌بندی تصاویر ورودی مربوط به کلاس مختلف را یاد می‌گیرد. این شبکه دارای اتلاف تصدیق است. ابتدا تصاویر برای استخراج ویژگی‌ها وارد شبکه می‌شوند. بعد از آخرین لایه مدل پیش‌آموزش داده شده، یک توصیف‌کننده ویژگی N بُعدی قرار دارد. سپس ویژگی‌های استخراج شده سطح بالا برای مقایسه وارد یک لایه مربع[۴] بدون پارامتر می‌شوند. این لایه ماتریس را به‌عنوان ورودی گرفته و بعد از تفریق و مربع کردن، یک ماتریس به عنوان خروجی می‌دهد. لایه مربع به صورت $f_s = (f_1 - f_2)^2$ نوشته می‌شود. جایی که f_1 و f_2 ویژگی‌های سطح بالا استخراج شده از جفت تصاویر ورودی می‌باشند و f_s ماتریس خروجی

[4] Square layer



شکل ۲: معماری روش پیشنهادی

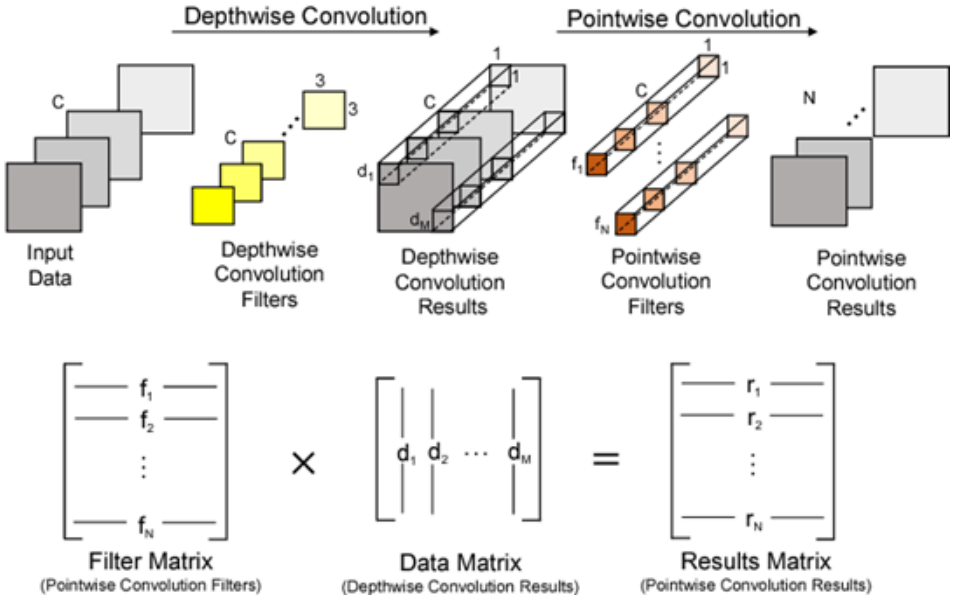
است. در ادامه یک لایه حذف تصادفی (برون‌اندازی)[5] برای جلوگیری از بیش‌برازش شبکه قرار دارد. در انتهای شبکه تابع سیگموید قرار دارد که تشابه یا عدم تشابه جفت تصویر ورودی را تعیین می‌کند.

۲.۳ مدل پیش‌آموزش داده EfficientNet B0

طبق مشاهدات با اعمال تعادل بین همه بُعدهای شبکه، در کارآیی و دقت آن بهبود حاصل می‌شود. در EfficientNet B0 برای بهبود عملکرد CNNها، در سه بُعد عرض، عمق و وضوح از مجموعه ثابت استفاده می‌شود که این ضرایب مقیاس‌گذاری ثابت برخی از محدودیت‌های خاص را برآورده می‌کند. در شکل ۳ بازنمایی از کانوولوشنال عمقی و نقطه‌ای استفاده شده در EfficientNet B0 ترسیم شده است. این شبکه پیش‌آموزش داده در مجموع دارای ۱۸ لایه کانوولوشنال است که $D = ۱۸$ و هر لایه دارای هسته‌های $k(۳,۳)$ یا $k(۵,۵)$ است. تصاویر ورودی شامل سه کانال رنگ R, G, B است. این شبکه روی تصاویر با ابعاد ۲۲۴ × ۲۲۴ آموزش دیده است. ابعاد مجموعه تصاویر بازشناسایی شخص ۸۰ × ۱۶۰ می‌باشد که شبکه EfficientNet B0 را در این ابعاد تصاویر تنظیم می‌کنیم تا یادگیری انجام شود. لایه‌های بعدی برای کوچک کردن اندازه نقشه ویژگی، مقیاس وضوح را کاهش می‌دهند ولی برای افزایش دقت، مقیاس عرض را افزایش می‌دهند. برای نمونه لایه کانوولوشنال دوم شامل $w = ۱۶$ فیلتر است، و تعداد فیلترهای لایه بعدی $w = ۲۴$ است.

روش متداول، استفاده از هسته‌های $k(۳,۳)$، $k(۵,۵)$ یا $k(۷,۷)$ است. [۱۶]. با این حال هسته‌های

[5] Dropout layer



شکل ۳: بازنمایی از کانوولوشن عمقی و نقطه‌ای [۱۸]

بزرگ می‌توانند باعث بهبود دقت و کارآیی مدل شوند. علاوه بر این، هسته‌های بزرگ به ضبط الگوهای با وضوح بالا کمک می‌کنند، در حالی که هسته‌های کوچک باعث بهتر استخراج شدن الگوهای با وضوح پایین می‌شوند [۱۷].

۳.۳ یادگیری انتقالی

برای آموزش شبکه‌های عصبی نیاز به جمع‌آوری مقدار کافی داده است. دستیابی به مقدار زیادی از داده‌ها دشوار می‌باشد، زیرا جمع‌آوری داده‌های برچسب‌دار نیاز به زمان و هزینه زیادی دارند و احتمال خطا در آنها بالا است [۱۹]. برای این منظور، یادگیری انتقالی به عنوان روشی مؤثر برای انتقال دانش استخراج شده از یک منبع به دامنه هدف در نظر گرفته می‌شود [۱۹]. در این روش، یادگیری انتقالی به ما این امکان را می‌دهد که از پارامترهای موجود و وزن‌های لایه کانوولوشن از یک مدل یادگیری شده روی مجموعه داده بزرگ برای مدل جدید خود با مجموعه داده کوچک استفاده کنیم. ما از وزن‌های مدل پیش آموزش داده شده روی مجموعه داده ImageNet استفاده کردیم که به دلیل داشتن تصاویر عمومی و محیط می‌تواند در مسئله بازشناسایی شخص مورد استفاده قرار بگیرد و نتایج خوبی بدهد.

۴.۳ اتلاف تصدیق

همان‌طور که در شکل ۲ مشاهده می‌شود، از لایه مربع برای مقایسه ویژگی‌ها استفاده شده است. در این شبکه، لایه مربع f_1 و f_2 را به عنوان ورودی دریافت کرده و f_s به عنوان خروجی لایه مربع می‌دهد. لایه

مربع به صورت زیر نمایش داده می‌شود:

$$f_s = (f_1 - f_2)^2 \quad (1)$$

برای حل مسئله تصدیق عابرپیاده همانند مسئله طبقه‌بندی دودویی رفتار می‌کنیم و برای احتمال پیش‌بینی شده از اتلاف آنتروپی متقاطع به صورت زیر استفاده می‌کنیم:

$$\hat{q} = \text{softmax}(\theta_s^* f_s) \quad (2)$$

$$\text{verify}(f_1, f_2, s, \theta_s) = \sum_{i=1}^{2} -q_i \log(\hat{q}_i) \quad (3)$$

جایی که ابعاد f_1 و f_1 برابر ۴۰۹۶ × ۱ × ۱، s کلاس هدف (یکسان/ متفاوت)، θ_s پارمترهای لایه کانوولوشنال و $\hat{q}$ احتمال پیش بینی شده است. اگر جفت تصویر ورودی مربوط به یک شخص باشد، $q_1 = 0, q_2 = 1$ در غیر اینصورت برابر با $q_1 = 0, q_2 = 1$ است.

۴ نتایج پیاده‌سازی

۱.۴ مجموعه داده

آزمایش‌های ما روی مجموعه داده CUHK01 انجام شده است. این مجموعه داده در دو زاویه دوربین، ضبط و جمع‌آوری شده است. مجموعه داده شامل تصاویر گرفته شده از ۹۷۱ شخص است و هر شخص دو تصویر از دوربین A و دو تصویر از دوربین B دارد. دوربین A از زاویه روبه‌روی شخص و دوربین B از زاویه نیمرخ شخص تصویر ضبط می‌کند.

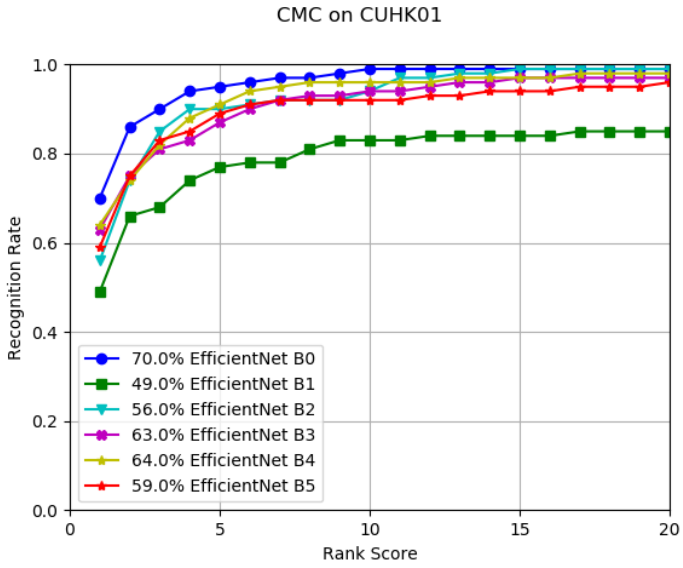
۲.۴ تنظیمات یادگیری

در فرآیند آموزش جفت تصاویر به دسته‌های ۴۸تایی به شبکه داده می‌شوند. از کاهش گرادیانی به‌عنوان روش بهینه‌سازی برای حداقل کردن خطای آنتروپی متقاطع استفاده می‌شود. نرخ یادگیری برابر با ۰/۰۰۱ است.

۳.۴ متعادل کردن زوج های مثبت و منفی

هر شخص در مجموعه داده دارای چهار جفت تصویر مثبت و تعداد زیادی جفت تصویر منفی است. به دلیل کم بودن جفت‌های مثبت نسبت به جفت‌های منفی ممکن است مشکل بیش‌برازش[۶] رخ دهد. برای جلوگیری از این مشکل و متعادل کردن جفت‌های مثبت و جفت‌های منفی از روش‌های افزایش داده استفاده

[6] Overfitting



شکل ۴: نمودار CMC مربوط به روش‌های مختلف روی مجموعه داده CUHK01

می‌کنیم. تصاویر هر شخص را با استفاده از تکنیک های افزایش داده مانند آیینه، نزدیک‌نمایی و جابه‌جایی تصویر افزایش دادیم. سپس تعداد جفت‌های مثبت افزایش داشته و تعادل آن نسبت به جفت‌های منفی برقرار شد.

در این بخش کارآیی مدل پیشنهادی با دیگر روش‌های توسعه یافته در سال‌های گذشته مانند LMNN، KISSME، ImprovedDeep، Quadruplet و غیره مقایسه می‌شود. از منحنی تطبیق CMC برای ارزیابی کمی روش‌ها استفاده می‌کنیم. در جدول شماره ۱ مقایسه روش ارایه شده با دیگر روش‌ها قرار گرفته است. در شکل ۴ نمودار CMC رسم شده است و مشاهده می‌شود روش پیشنهادی نسبت به روش‌های دیگر دارای بهبود است.

۵ نتیجه‌گیری

بازشناسایی شخص به عنوان یک زیرمسئله از مسئله بازیابی تصاویر درنظر گرفته می‌شود که می‌توان آن را با استفاده از روش‌های سنتی تجزیه و تحلیل تصاویر حل کرد. در این مقاله ما از یک روش انتها به انتها یادگیری عمیق برای حل مسئله بازشناسایی شخص استفاده کردیم. از لایه‌های کانوولوشنال و معماری سیامی در کنار شبکه پیش‌آموزش داده EfficientNet برای استخراج ویژگی‌ها استفاده کردیم. برخلاف روش‌های دیگر بازشناسایی شخص، روش ارائه شده توانست ویژگی‌های سطح بالا و متمایز کننده را به خوبی از تصاویر استخراج کند. به‌دلیل تعداد کم پارامترهای EfficientNet، سرعت یادگیری افزایش یافته و نیاز به تعداد کمتری از مجموعه داده است و در نتیجه کارآیی و دقت شبکه افزایش قابل توجهی داشته است. معیار

جدول ۱: مقایسه روش‌های بازشناسایی شخص

Paper	R-1	R-5	R-10	R-15	R-20	Year	Source Title
Pedestrian recognition with a learned metric (LMNN)	13.5	31.3	42.3	-	54.1	2010	Asian conference on Computer vision
Large scale metric learning from equivalence constraints (KISSME)	29.4	57.7	72.4	-	86.1	2012	CVPR
Person re-identification by local maximal occurrence representation and metric learning (LOMO+XQDA)	63.2	83.9	90.1	-	94.2	2015	CVPR
DeepReID: Deep filter pairing neural network for person re-identification (DeepReID)	27.9	58.2	73.5	-	86.3	2014	CVPR
An improved deep learning architecture for person reidentification (Improved-Deep)	47.5	72.3	80.1	-	83.9	2015	CVPR
Sample-specific SVM learning for person re-identification (LSSCDK)	66	-	90	93.3	95	2016	CVPR
Beyond triplet loss: a deep quadruplet network for person re-identification (Quadruplet)	62.6	-	86	88.9	89.8	2017	CVPR
Deepreid: Deep filter pairing neural network for person re-identification	27.87	-	-	-	-	2014	CVPR
Person re-identification using CNN features learned from combination of attributes	46.8	71.8	80.5	-	-	2016	ICPR
Learning deep feature representations with domain guided dropout for person re-identification	71.7	88.6	92.6	-	-	2016	CVPR
Person re-identification by multi-channel parts-based CNN with improved triplet loss function	53.7	84.3	91	-	-	2016	CVPR
Joint learning of single-image and cross-image representations for person re-identification	71.8	-	-	-	-	2016	CVPR
Deep ranking for person re-identification via joint representation learning	70.94	92.3	96.9	-	-	2016	IEEE Transactions on Image Processing
An improved deep learning architecture for person re-identification	65	89.5	93	-	-	2015	CVPR
Personnet: Person re-identification with deep convolutional neural networks	71.14	90	95	-	-	2016	arxiv
Embedding Deep Metric for Person Re-identification: A Study Against Large Variations	69.38	-	-	-	-	2016	European conference on computer vision
Beyond triplet loss: a deep quadruplet network for person re-identification	62.55	83.44	89.71	-	-	2017	CVPR
A new patch selection method based on parsing and saliency detection for person re-identification	83.2	-	97.1	98.4	98.8	2020	Neurocomputing
A Discriminatively Learned CNN Embedding for Person Re-identification	41	72	87	91	93	2017	ACM Transactions (TOMM)
Proposed	**70**	**95**	**99**	**99**	**99**		

شباهت این شبکه زیر نظر اتلاف تصدیق یادگیری را انجام می‌دهد. این شبکه روی مجموعه داده CUHK01 که یکی از چالشی‌ترین مجموعه داده‌های بازشناسایی شخص می‌باشد آزمایش شده است. تعداد تصاویر این مجموعه داده کم و تصاویر آن دارای وضوح و چالش‌های فراوانی هستند. آزمایش‌های ما روی این مجموعه داده کارآیی روش ارایه شده را نشان می‌دهد.

مراجع

[1] L. Zheng, Y. Yang, and A. G. Hauptmann, “Person re-identification: Past, present and future,” arXiv Prepr. arXiv1610.02984, 2016.

[2] R. Zhao, W. Ouyang, and X. Wang, “Unsupervised salience learning for person re-identification,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2013, pp. 3586–3593.

[3] Z. Wang et al., “Zero-shot person re-identification via cross-view consistency,” IEEE Trans. Multimed., vol. 18, no. 2, pp. 260–272, 2015.

[4] W. Li, R. Zhao, T. Xiao, and X. Wang, “Deepreid: Deep filter pairing neural network for person re-identification,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2014, pp. 152–159.

[5] C. Madden, E. D. Cheng, and M. Piccardi, “Tracking people across disjoint camera views by an illumination-tolerant appearance representation,” Mach. Vis. Appl., vol. 18, no. 3–4, pp. 233–247, 2007.

[6] L. Bazzani, M. Cristani, and V. Murino, “Symmetry-driven accumulation of local features for human characterization and re-identification,” Comput. Vis. Image Underst., vol. 117, no. 2, pp. 130–144, 2013.

[7] M. D. Zeiler and R. Fergus, “Visualizing and understanding convolutional networks,” in European conference on computer vision, 2014, pp. 818–833.

[8] M. Tan and Q. V Le, “Efficientnet: Rethinking model scaling for convolutional neural networks,” arXiv Prepr. arXiv1905.11946, 2019.

[9] W. Li and X. Wang, “Locally aligned feature transforms across views,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2013, pp. 3594–3601.

[10] M. Koestinger, M. Hirzer, P. Wohlhart, P. M. Roth, and H. Bischof, “Large scale metric learning from equivalence constraints,” in 2012 IEEE conference on computer vision and pattern recognition, 2012, pp. 2288–2295.

[11] Z. Li, S. Chang, F. Liang, T. S. Huang, L. Cao, and J. R. Smith, “Learning locally-adaptive decision functions for person verification,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2013, pp. 3610–3617.

[12] N. Martinel, C. Micheloni, and G. L. Foresti, “Saliency weighted features for person re-identification,” in European Conference on Computer Vision, 2014, pp. 191–208.

[13] E. Ahmed, M. Jones, and T. K. Marks, “An improved deep learning architecture for person re-identification,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2015, pp. 3908–3916.

[14] S. Paisitkriangkrai, C. Shen, and A. Van Den Hengel, “Learning to rank in person re-identification with metric ensembles,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015, pp. 1846–1855.

[15] D. Yi, Z. Lei, S. Liao, and S. Z. Li, “Deep metric learning for person re-identification,” in 2014 22nd International Conference on Pattern Recognition, 2014, pp. 34–39.

[16] H. Cai, L. Zhu, and S. Han, “Proxylessnas: Direct neural architecture search on target task and hardware,” arXiv Prepr. arXiv1812.00332, 2018.

[17] A. G. Howard et al., “Mobilenets: Efficient convolutional neural networks for mobile vision applications,” arXiv Prepr. arXiv1704.04861, 2017.

[18] H. T. Kung, B. McDanel, and S. Q. Zhang, “Adaptive tiling: Applying fixed-size systolic arrays to sparse convolutional neural networks,” in 2018 24th International Conference on Pattern Recognition (ICPR), 2018, pp. 1006–1011.

[19] B. Lavi, I. Ullah, M. Fatan, and A. Rocha, “Survey on Reliable Deep Learning-Based Person Re-Identification Models: Are We There Yet?,” arXiv Prepr. arXiv2005.00355, 2020.

تبیین نظری مؤلفه‌های نظام سایبرنتیک ومقایسه آن با مؤلفه‌های نظام ولایت

رضوان هامانی [۱]، زهرا حصارکی [۲]

[۱] طلبه سطح چهار حکمت متعالیه جامعة الزهراء سلام الله علیها و دانشجوی د کتری فلسفه فیزیک دانشگاه باقرالعلوم، قم
rezvanhamani1402@gmail.com
[۲] طلبه سطح چهار کلام اسلامی جامعة الزهراء سلام الله علیها، کارشناسی ارشد فلسفه اسلامی دانشکده هدی، کارشناس و پژوهشگر دوره نقد وهابیت جامعة الزهراء سلام الله علیها، قم
z.hesaraki.chmail.ir

چکیده

تئوری سیستم‌ها نظریه‌ای برای درک و تحلیل کلیت جهان هستی و وقایع و منظومه‌های درون آن است که توان تصمیم‌سازی، تصمیم‌گیری و کنترل‌گری را به شکل چشم‌گیری افزایش داده و به‌عنوان یک روش میان‌رشته‌ای تحولات زیادی را در بستر وسیع سازمان‌های جهان کنونی رقم‌زده است. این تئوری با ایجاد یک تفکر کل‌نگرانه در مدیریت سازمانها، نقش بسیار مهمی در پیدایش نظام سایبرنتیکی و الگوی مدیریت جامع آن داشته است. استفاده از این سیستم در پدیده‌های شناختی و روان‌شناختی برای کنترل و مدیریت جوامع انسانی و سلطه بر حاکمیت‌های محلی، با هدف رسیدن به نظم نوین جهانی، نظام سلطه را در جهان امروز رقم زده است. در مقابل سیستم مدیریت نظام توحیدی علاوه بر هدایت تکوینی عامه، که نظام و سازمان خلقت براساس آن تکوّن یافته و هدایتی همگانی و متحد به‌سوی غایتی است، و هدایت تکوینی خاص، که از طریق عقل و فطرت نوع بشریت را رهنمون است، هدایت تشریعی عامه را در ظرف اختیار و توان کنشگری انتخابی انسانها قرار داده، تا در سیستمی ورای تئوری سیستم‌های حاکم بر هدایت تکوینی، به تنظیم‌گری جامعه و هدایت انسان‌ها برای رسیدن به اهداف متعالی خلقت رهنمون باشد. در این پژوهش با تعریف تئوری جامع سیستم‌ها و با تاکید بر طبقه‌بندی بلدینگ، نظام سایبرنتیکی برآمده از آن معرفی شده و با روشی تحلیلی- توصیفی و بر مبنای هستی‌شناسی حاکم بر فلسفه اسلامی طبقه‌بندی سیستمی که می‌تواند توصیف‌گر نظام ولایت باشد، ارائه گردیده و با بهره از آیات قرآن به مقایسه نظام ولایت با نظام سایبرنتیک پرداخته شده است.

کلمات کلیدی: تئوری سیستم‌ها، نظام سایبرنتیک، نظام ولایت، کنترل، هدایت.

۱ مقدمه

در مقام قیاس بین دو نظام، پرداختن به زیربناها و مبانی ساختاری و کاربردی آن دو نظام اساس تمایزات آنها را روشن خواهد ساخت. در این مهم پرداختن به ریشه‌های فلسفی و دانشی هر نظام ما را ملزم به بررسی اصول موضوعه و روش‌شناسی دانش حاکم برآن می‌کند تا اختلافات بنیادین آن‌ها در این مقایسه آشکار گردد.

در قرن اخیر که مرزهای دانشی مختلف کم رنگ شده است، علوم میان رشته‌ای پا به عرصه وجود نهاده‌اند. از جمله این علوم، دانش سایبرنتیک است که در بحبوحه جنگ جهانی دوم و با هدف توسعه مغزهای الکترونیکی و سازوکارهای کنترل خودکار برای تجهیزات نظامی زاده شد. اما امروزه سایبرنتیک در واقع علمی است که به سامانه‌های ارتباطی و کنترل در موجودات زنده، ماشین و سازمان‌ها می‌پردازد و نظام سایبرنتیکی که بر مبنای این علم و در عرصه فضای سایبرنتیکی متولد شده، داعیه مدیریت کلان جامعه بشری و ایجاد نظم نوین جهانی را دنبال می‌کند و سامانه مدیریتی این نظام بر اساس نظریه سیستمی سایبرنتیکی با تفکری کل‌نگرانه به جهان، اهداف این نظام را دنبال می‌کند.

نظریه تئوری سیستم‌ها نخستین بار توسط زیست‌شناس اتریشی به‌نام لودویگ ون برتالنفی[۱] در کتاب «تئوری عمومی سیستم‌ها» در اوایل دهه ۱۹۳۰ تنظیم گردید. براساس این نظریه سامانه‌های پیچیده فارغ از هدفی که دنبال می‌کنند، برخی اصول سازمان‌دهی پایه‌ای مشترک دارند و این اصول می‌تواند به‌صورت ریاضی مدل شود. کنت بولدینگ[۲] و آناتول راپوپورت[۳] و نیکلاس لومان[۴] از چهره‌های مهم و بحث‌انگیز در این حوزه به شمار می‌آیند (J. Mingers, 2017, 67-71).

سیستم مدیریت سایبرنتیک برنامه کاربردی ساخته شده از قوانین سایبرنتیکی طبیعی برای تمام انواع سازمان‌ها و مؤسسات ایجاد شده توسط انسان‌ها و برای تعامل با آنهاست. قابلیت مداری این سیستم با عنوان فیدبک یکی از مفاهیم زیربنایی در تفکر سیستمی و نظریه سیستم‌های سایبرنتیکی است که موفقیت آن نسبت به روش مدیریت سنتی و بوروکراتیک، میزان استفاده ازاین روش در اداره سازمان‌ها را معیار توسعه‌یافتگی کشورها ساخته است.

اما این دستاورد دانش بشری قرن بیستم به عنوان یک پدیده تکنولوژیکال، تنها سومین سطح از طبقه‌بندی تئوری جامع سیستم‌هاست و غایت بشری محسوب نمی‌شود و تلاش دانشمندان برای کشف سطوح بالاتر طبقات سیستم‌ها همچنان ادامه دارد.

با این وجود نظام سایبرنتیکی با اتکا به این سامانه مدیریتی سعی در کنترل جوامع بشری و سلطه بر حاکمیت‌های محلی دارد، فارغ از این که خالق قادر متعال، سیستم حاکم بر اداره جهان و انسان را بر محور هدایت انسان‌های شعورمند و مختار آفریده و نظام ولایت را بر اساس آن سامان داده است و به‌حق می‌فرماید: «إنّ القوه للّه جمیعاً...».

---

[1] Ludwig von Bertalanffy
[2] Kenneth Boulding
[3] Anatol Rapoport
[4] Niklas Luhmann

۲ تئوری سیستم‌ها

در بررسی زیرساخت‌های نظام سایبرنتیکی لازم است ابتدا ریشه‌های شکل‌گیری تفکر کل‌نگر و سیستمی را مطرح کرد و به بیان تعریفی از تئوری جامع سیستم‌ها پرداخت. از جمله وظایف اصلی که در نظریه جامع سیستم‌ها محقق می‌شود عبارتند از: (۱) تعریف معنای «سیستم‌ها» و مفاهیم مرتبط. (۲) طبقه‌بندی سیستم‌ها و یافتن ویژگی‌های آنها در کلی‌ترین معنا (۳) کشف مدل رفتاری سیستم‌ها (۴) مطالعه مدل‌های سیستم‌های خاص به‌صورت منطقی و روش‌شناختی. به‌عبارتی هدف نظریه سیستم‌های عمومی ایجاد یک نظریه‌ی انتزاعی در سطح کلان است، بدون اینکه به ویژگی فیزیکی خاصی از سیستم بپردازد (YI LIN, 2002, p 9).

۱.۲ مفهوم‌شناسی تئوری سیستم‌ها

تئوری سیستم‌ها یا نظریه سامانه‌ها (Systems theory) دانشی است که به بررسی و مطالعه نظری و ریاضی سامانه‌های گوناگون می‌پردازد. این نظریه تقریباً در همه رشته‌ها کاربرد دارد اما در سال‌های اخیر رشته سامانه‌های اطلاعاتی رشد و توسعه چشمگیری داشته است. برای آشنایی با این تئوری لازم است تعریفی از مفهوم سیستم داشته باشیم.

۱.۱.۲ تعریف سیستم

با وجود اینکه امروزه ایده سیستم‌ها در تمام علوم مدرن رخنه کرده است، اما هنوز اتفاق‌نظری در تعریف ایده‌آل برای مفهوم سیستم وجود ندارد. بر اساس اجماع دپارتمان مدیریت بازرگانی جهانی در سال ۱۹۸۳، «سیستم» تعمیم مفهوم «ساختار» در فیزیک است، هرچند که تفاوت‌هایی با ساختار دارد. یک سیستم دارای سه ویژگی مهم است: (۱) نظم یا سطح‌بندی، (۲) کل‌گرایی، (۳) نسبیت و تمامیت، که بر این اساس زیرسیستم‌ها به‌طور نسبی و وابسته به یکدیگر در تعامل‌اند (YI LIN, 2002, p 11). به‌عبارت دیگر سیستم به مجموعه‌ای از اجزاء گفته می‌شود که میان آنها ارتباط معناداری وجود دارد و همه اجزاء با هم مجموعه مشترکی از اهداف را دنبال می‌کنند. یعنی درون‌داده را دریافت کرده و از طریق یک فرآیند تبدیل سازمان‌یافته آن را به برون‌داده تبدیل می‌کنند (ابراین و ماراکس، ۱۳۹۲، ص ۳۵). برتالنفی، بنیانگذار تفکر سیستمی نیز سیستم را موجودیتی تعریف می‌کند که حیات آن از طریق روابط متقابل میان اجزاء امکان‌پذیر است (علی‌احمدی و مشایخ، ۱۳۹۳، ص۷).

در روش سنتی بررسی سیستم‌ها به‌طریق تجزیه‌گرایی صورت می‌گرفت، یعنی برای شناخت مکانیزم یک کل به بررسی اجزاء می‌پرداختند، اما به‌طور کلی در تفکر سیستمی هر پدیده یک کلیت متشکل از اجزاء است که بررسی اجزا و عناصر آن نمی‌تواند کل پدیده را تبیین کند؛ زیرا کل ویژگی‌هایی دارد که در جمع جبری تک‌تک اجزاء آن نیست. لذا نظریه سیستم‌ها نگاه جدیدی به سازمان‌ها و روابط حاکم برآن ارائه می‌دهد که اثرات محیط و تغییرات آن را در عملکرد سیستم لحاظ کرده و به‌جای روش سنتی و بروکراتیک در اداره سازمان‌ها از روش‌های نوین و کل‌نگر بهره می‌گیرد (امیرخانی و هیهاوندزواری‌پور، ۱۳۹۶، ص۲).

۲.۱.۲ تئوری عمومی سیستم‌ها

تئوری عمومی سیستم‌ها (General System Theory) یکی از شاخه‌های تئوری سیستم‌ها و البته قدیمی‌ترین رویکرد آن است که بر اساس آن کل عالم هستی به‌مثابه یک سیستم پیچیده کلان که دربرگیرنده سیستم‌های دیگر از ساده‌ترین تا پیچیده‌ترین آنهاست، مطالعه می‌شود. به همین دلیل بود که برتالانفی معتقد بود که نظریه سیستم‌های عمومی به ویژگی‌های رسمی ساختارهای سیستمی می‌پردازد تا نتایج آن را بتوان در موضوعات تحقیقاتی در زمینه‌های مختلف علمی به‌کار برد، و می‌توان آن را نه تنها در سیستم‌های فیزیکی، بلکه در هر «کلی» به‌کار برد (von Bertalanffy, 1967, pp 125-126).

یک سیستم عمومی، بسته به نوع نگرش فلسفی به هستی، می‌تواند بخشی از عالم یا همه اجزاء آن، اعم از کهکشان‌ها و سیارات و ستارگان تا انسانها و حیوانات و جمادات را شامل شود و حتی در نگاهی فرامادی عوالم وجود و مجردات را نیز دربرگیرد. برهمین اساس دانشمندان همواره به دنبال طبقه‌بندی سیستم‌ها در یک تئوری جامع بوده‌اند.

۳.۱.۲ طبقه‌بندی سیستم‌ها

در قرن بیستم طبقه‌بندی‌های متفاوتی تنظیم شد که از میان طبقه‌بندی‌هایی که تا کنون ارائه شده است، سه سطح طبقه‌بندی نسبت به سایرین ارجح بوده که عبارتند از: طبقه‌بندی بلدینگ[۵]؛ طبقه‌بندی ایکاف[۶] و طبقه‌بندی چک‌لند[۷]. اما از آن جهت که در طبقه‌بندی بلدینگ به سطح سیستم‌های سایبرنتیکی پرداخته شده و علاوه بر آن سطحی را برای سیستم‌های ورای فیزیک و متافیزیک لحاظ کرده، پرداختن به آن به هدف این پژوهش و ساختار طبقه‌بندی هستی از منظر حکمت اسلامی نزدیک‌تر است.

۲.۲ طبقه‌بندی بلدینگ

بلدینگ، با در نظر گرفتن قواعد و ضوابطی عمومی، انواع سیستم‌های موجود در جهان را بر اساس «میزان پیچیدگی» آنها در سه فصل کلی به نه سطح طبقه‌بندی کرد، به گونه‌ای که هر چه از سطح یک به سطح نُه نزدیک‌تر شویم، میزان پیچیدگی سیستم‌ها افزایش پیدا می‌کند (هچ، ترجمه رسولی و آشوری، بی‌تا، صص ۶۴-۶۵):

- فصل اول شامل سامانه‌های فیزیکی در سه سطحِ سیستم‌های ایستا (Structure)، سیستم‌های مکانیکی یا ساعت‌گونه (Clockwork)، سیستم‌های سایبرنتیک (Cybernetic) یا سطح سازوکارهای کنترل خودکار و خودتنظیم.
- فصل دوم شامل سامانه‌های زیستی در سه سطح طبقه‌بندی شده است: سیستم‌های تک‌یاخته (Self-Maintaining)، سیستم‌های گیاهی (Genetic Societal) و سیستم‌های حیوانی (Animal).

[5] BOULDING'S Classification
[6] AKOFF'S Classification
[7] CHECKLAND'S Classification

- فصل سوم شامل سامانه‌های علوم انسانی و فرامادی، نیزمتشکل از سیستم‌های انسانی (Human)، سیستم‌های اجتماعی (Social Systems) و سیستم‌های متعالی و فوق طبیعی (Transcendental).

سه سطح اول دسته‌بندی بلدینگ شامل سیستم‌های بسته و سطوح بعد از آن شامل سیستم‌های باز هستند[۸]. سیستم‌ها در هر سطح، علاوه بر آن ویژگی‌های منحصر به‌فرد خود، تمام ویژگی‌های سیستم‌های سطوح قبلی خود را نیز دارا هستند. از این رو درک و شناخت سیستم‌های هر سطح، منوط به شناخت دقیق سیستم‌های سطوح قبلی و نوع کارکرد آنهاست.

تا کنون دانش بشرتوانسته است تا حدود زیادی سیستم‌های سه سطح اول را بشناسد، اما از سطح چهارم به بعد ناشناخته‌های فراوانی وجود دارد. به‌طوری که جهت شناخت سازمان‌های اجتماعی، که در جایگاه هشتم پیچیدگی قرار دارد، این طبقه را تا حد سامانه‌های فیزیکی ایستا و ساعت‌گونه و یا نهایتاً سایبرنتیکی پایین کشیده است و همچنین انسان که در جایگاه هفتم این طبقه‌بندی قرار دارد در صدد است تا سازمان‌های اجتماعی را که در سطح هشتم از طبقه‌بندی است سامان دهد.

در حالی که در سلسله‌مراتب سیستمی، سیستم‌های فوقانی به‌علت اشراف و برتری که بر سیستم‌های تحت خود دارند، قادر به تغییر و تحول در سامانه‌های پست‌تر از خود هستند و بر این اساس سامان‌دهی سیستم‌های اجتماعی باید توسط سیستم‌های متعالی و فرا-اجتماعی صورت پذیرد (علی احمدی و مشایخ، ۱۳۹۳، ص ۱۱). سیستم‌های متعالی سیستم‌هایی هستند که گیرنده‌های اطلاعاتی بشر، قادر به گرفتن اطلاعات از آنها نیست و انسان از طریق دانش نتوانسته است به آنها راه یابد. هرچند که در مکاتب توحیدی با توجه به ارتباط انبیاء با ماوراءالطبیعه و سرای دیگر، توانسته‌اند اطلاعاتی را فراتر از محدوده قدرت علم بشر در اختیار وی قرار دهند.

با این وجود عصر حاضر، عصر گذار از سیستم‌های ارگانیکی به سیستم‌های سایبرنتیکی است و متفکران و دانشمندان در تلاش هستند تا همه سیستم‌های موجود در طبقات بالاتر را بر اساس دانش سیستم‌های سایبرنتیکی تحلیل کنند. به‌طوری که امروزه یکی از پارامترها در اندازه‌گیری میزان توسعه‌یافتگی کشورها، نه‌تنها میزان گسترش سیستم‌های حکومتی آن کشور است بلکه نوع سیستم سایبرنتیکی نیز معیار توسعه‌یافتگی محسوب می‌شود.

۳ تئوری سیستم در نظام سایبرنتیکی

روش نظام مدیریت سایبرنتیکی بر اساس سومین سطح از طبقه بندی بلدینگ، یعنی سیستم‌های سایبرنتیکی طراحی شده است. سیستم مورد تحلیل زمانی سایبرنتیکی است که در یک حلقه بسته از سیگنال‌ها درگیر شده باشد به نحوی که برون‌داد سیستم تغییراتی را در محیط ایجاد می‌کند که این تغییرات از طریق مدار

[۸] منظور از سیستم‌های بسته، سیستم‌هایی هستند که با محیط اطراف خود تبادل و تعامل ندارند. اما سیستم‌های باز سیستم‌هایی هستند که با محیط اطراف خود تعامل داشته و بنابراین قادر به رشد، تغییر، انطباق و نگهداری از خود متناسب با شرایط محیطی هستند.

فیدبک در سیستم منعکس شده و منجر به خودتنظیمی و خود کنترلی سیستم می‌گردد. این سیستم از جمله سیستم‌های باز است که بر حلقه‌های فیدبک و فرآیندهای کنترلی تاکید دارند (آذرباد،۲۰۱۵، ص۷). مؤلفه‌های آن شامل کنترل کننده، کنترل شونده، متغیر کنترل شده و مدار فیدبک است. کنترل کننده بخش متفکر و هوشمند سیستم است که اطلاعات را از محیط دریافت و کنترل‌شونده نیز در تعامل با محیط، انرژی لازم برای بقای سیستم را تأمین می‌کند.

از این رو دوگانه اطلاعات و انرژی در این سیستم‌ها بسیار پراهمیت است. کنترل‌کننده به‌عنوان عضو متفکر سیستم در مقدار و نوع اطلاعات ارسالی به کنترل‌شونده مختار است، ولی کنترل‌شونده به عنوان عضو عملگر، همواره و به‌طور خودکار انرژی را به کنترل‌کننده ارسال می‌کند. در این سیستم‌ها مدار فیدبک مؤلفه اصلی است که قابلیت استفاده از اطلاعات خروجی ناشی از کنش کنترل‌شونده روی محیط را به کنترل‌کننده برمی‌گرداند. این اطلاعات در چرخه بعدی ملاک انتخاب میزان و نوع اطلاعات ارسالی توسط بخش کنترل‌کننده است.

بنابراین کنترل‌کننده با انتقال اطلاعات در داخل سیستم، تأثیرات آن را بر محیط سیستم‌های کنترل‌شده بررسی می‌کند و حتی در صورتی که ساختار سیستم مورد نظر به‌وضوح شناخته شده نباشد، یعنی سیستم یک جعبه سیاه ورودی-خروجی باشد، تئوری کل‌نگر سایبرنتیکی همچنان می‌تواند درک درستی از آن ساختار ارائه دهد (YI LIN, 2002, p 11).

هر چند در آغاز پیدایش، سایبرنتیک با هدف بررسی سیستم‌های فیزیکی مطرح شد، ولی امروزه با رویکردی فرارشته‌ای در تحلیل سیستم‌های نظارتی به مطالعه سیستم‌هایی نظیر شبکه‌های الکتریکی، مهندسی مکانیک، مدل‌سازی منطقی، زیست‌شناسی تکاملی، عصب‌شناسی، انسان‌شناسی، روان‌شناسی و جامعه‌شناسی می‌پردازد (آذرباد، ۲۱۵، صص ۳ و ۸). از مصادیق این سیستم‌ها که در علوم‌شناختی معاصر و در حوزه کنترل رفتار به آن پرداخته می‌شود، سامانه شناخت انسان است که با عنوان سایکوسایبرنتیک به بررسی علم کنترل مغز می‌پردازد. در عملکرد این سیستم اندام‌های حسی اطلاعات را از محیط دریافت و به مغز ارسال می‌کنند. مغز اطلاعات دریافتی را پردازش کرده و بر اساس آن به اندام‌ها فرمان می‌دهد و از آنها بازخورد دریافت می کند (حاجی شمسایی و نوشین فرد، ۱۳۹۳، ص۹۹).

هرچند دانشمندان در استفاده از سیستم‌های سایبرنتیکی برای تبیین برخی از رفتارهای پیچیده موجودات زنده اتفاق نظر دارند، اما این سؤال مطرح است که آیا پدیده‌های پیچیده‌ی شناختی و روان‌شناختی را نیز می‌توان به‌همین طریق بررسی کرد؟ این پرسش بسیار مهمی است و پاسخ مثبت به آن پیامدهای سهمگینی در پی خواهد داشت. شاید از این روست که مباحثات و اختلاف نظرهای جدی، میان دانشمندان در این زمینه وجود دارد.

اما نظام سایبرنتیکی با پاسخ مثبت به این سؤال، دستیابی به رفتار هدفمند را بی‌نیاز از عامل درونی یا امری که از ویژگی‌های غیرفیزیکی برخوردار باشد، می‌داند. این نگرش نقش مهمی در پیش‌برد فضای علوم شناختی به سمت جلو داشته است و کمک زیادی به پیشرفت حوزه‌ی هوش مصنوعی کرده است.

۴ سیستم مدیریت در نظام توحیدی

از آنجا که هر نظریه با فلسفه و حکمت آغاز می‌شود، اصولاً نظریه جامع سیستم‌ها نیز بر اساس زیربناهای عمیق فلسفی بنیان نهاده شده است. از این رو لزوماً در سیستم مدیریتی نظام توحیدی با مبانی فلسفه اسلامی محور طبقه‌بندی سیستم ها قرار می‌گیرد. نظریه وحدت وجود در حکمت اسلامی در واقع نگاه کل‌نگر و تفکرِ جامعِ سیستمی به هستی است که جهان را یک کل منسجم هدفمند می‌بیند که در قوس نزول فرود آمده و در قوس صعود در جهت تعالی انسان در حرکت است. از این رو می‌توان ساختار طبقه‌بندی سیستم جامع در این نظام را بر اساس چهار فصل اصلی و سطوح فرعی که در طول یکدیگر و از سیستم‌های پیچیده تا ساده‌ترین را شامل می‌شود، ترسیم نمود:

- فصل اول؛ سیستم تئولوژیکال یا خداشناختی
- فصل دوم؛ سیستم آنتولوژیکال یا هستی‌شناختی که به ترتیب سطوح مختلف سیستمی عالم عقول، عالم مثال و عالم ماده را در برمی‌گیرد.
- فصل سه؛ سیستم آنتروپولوژیکال یا انسان‌شناختی که ناظر به ساحت‌های فطری انسان شامل زیر سیستم‌های بینش‌ها، گرایش‌ها و کُنش‌هاست.
- فصل چهار؛ سیستم اپیستمولوژیکال یا معرفت‌شناختی که در ذیل فصل سه و در طبقه اول یعنی سیستم بینش‌های انسان‌شناسی قرار می‌گیرد.

در این طبقه بندی کل وجود به‌مثابه یک سیستم جامع واحد است که کثرت اجزاء به هم مرتبط آن کارکردهای مجزا ولی هم‌راستا را دنبال می‌کنند، به‌گونه‌ایی که همواره کثرت در وحدت و وحدت در کثرت تجلی می‌یابد (تصدیقی، ۱۳۸۹). بر این اساس این طبقه‌بندی در قیاس با طبقه‌بندی بلدینگ از جامعیت و شمولیت بیشتری برخوردار است. انسان به‌عنوان جزئی از این سیستم ذیل سیستم هستی‌شناسی قرار دارد؛ با این تفاوت که از جهت ویژگی منحصر به‌فرد و خلقتی متمایز با سایر موجودات، به‌جهت اراده و اختیاری که دارد و هدفی که برمی‌گزیند، در بین سطوح این فصل در نزول و صعود است و به تعبیر قرآن کریم گاه انسان به مرتبه «أُولَئِكَ كَالْأَنْعَامِ بَلْ هُمْ أَضَلُّ»[۹] پایین خواهد آمد و گاه در مقام «إِنِّي جاعِلٌ فِي الْأَرْضِ خَلِيفَةً»[۱۰] خلیفه خداوند در زمین و تجلی و آیینه تمام‌نمای صفات حق تعالی است. بدین لحاظ انسان می‌تواند تجلی صفت تدبیرگری خداوند بر جهان باشد و همان‌طور که خداوند مدیر و مدبر جهان هستی است، انسان نیز تدبیرگر خویش و جامعه خود باشد (محمدی و قشقایی‌زاده، ۱۳۹۳، ص ۱۰۲) و حتی فراتر از آن، می‌تواند بر کل عالم امکان ولایتی منتصب از سوی مبدأ هستی داشته باشد و از این رو عاملیت و غایت‌انگاری دو مؤلفه ضروری در رسیدن به این هدف است.

[۹] اعراف، آیه ۱۷۹
[۱۰] بقره، آیه ۳۰

۵ مقایسه سیستم مدیریتی نظام سایبرنتیک با نظام ولایت

از آنچه تاکنون ترسیم شد می‌توان اختلافات و تمایزات نظام برگرفته از نظریه جامع سیستمی نظام ولایت را با نظامی که بر مبنای تئوری سیستم‌های سایبرنتیکی بنا شده، در ترازوی مقایسه قرار داد. آنچه در رأس این تمایز حائز اهمیت است، اهدافی است که هر نظام دنبال می‌کنند. هدف نظام ولایت هدایت انسان‌ها در جهت رسیدن به کمال متعالی است که برای آن خلق شده است، در حالی که در نظام سایبرنتیکی هدف کنترل و سلطه بر کنترل‌شونده است که اگر این کنترل شونده انسان باشد لازمه رسیدن به این هدف عدم هوشمندی و سلب اختیار و اراده از اوست. از این رو در نظام ولایت به‌جای بحث از کنترل باید به بررسی ابعاد هدایت پرداخت و به جای کنترل‌کننده و کنترل‌شونده باید از هدایت‌کننده و هدایت‌شونده بحث کرد.

۱.۵ تمایز میان هدایت و کنترل

هدایت از ریشه «هدأ» و در لغت به‌معنای دلیل و ارشاد است (جوهری، ۱۴۰۴ق، ج۶، ص۲۵۳۳) و در اصطلاح برخورداری هر موجود از کمال مناسب او که با نظم خاص و صحیحی در جهت رسیدن به آن است؛ به دیگر سخن، برقراری ارتباط خاص میان موجود و آینده کمالی آن را «هدایت» میگویند (جوادی آملی، عبدالله، ۱۳۸۵، ص ۲۱).

کنترل یکی از پنج مؤلفه مدیریت است که هنری فایول در کتاب «مدیریت عمومی و صنعتی» به آن می‌پردازد. به بیان فایول کنترل یعنی نظارت دائمی بر یک فعالیت، تا اطمینان حاصل شود که همه چیز مطابق استانداردهایی که از پیش تعیین شده، در جهت هدف و در چارچوب اصول آن، پیش می‌رود. اما آیا می‌توان با ابزار کنترل بر انسان و جوامع انسانی سیطره یافت و انسان‌ها را به سلطه درآورد؟

یکی از شاخصه‌های روان‌شناسی شخصیت در انسان بحث از کانون کنترل شخص است. این مفهوم اولین بار در سال ۱۹۵۴ توسط خانم جولیان روتر[11]، روان‌شناس مشهور آمریکایی مطرح شد. این کانون کنترل در افراد می‌تواند درونی و یا بیرونی باشد و عوامل مختلف محیطی می‌تواند آن را دستخوش تغییر قرار دهد. تغییر کانون کنترل درونی در انسان‌ها به کانون کنترل بیرونی می‌تواند منجر به سلطه بر انسان‌ها و جوامع بشری شود.

آنچه که نظام سایبرنتیک در جهت اهداف خود دنبال می‌کند نتیجه پاسخ مثبت به سؤال فوق است. این نظام با هدف رسیدن به یک قدرت منسجم بر مدیریت کل عالم، رویای سلطه بر انسانها را در قالب نظم نوین جهانی در سر دارد. از این رو در تلاش است تا با تلفیق تئوری سیستم‌های سایبرنتیکی و روان‌شناسی شناختی کانون کنترل درونی افراد را به کانون بیرونی تبدیل کند و در راستای تحقق این هدف، اصول و قوانین خود را در قالب سند دستوری به حکومت‌های محلی تحمیل می‌کند.

برخلاف نظام سایبرنتیک که کنترل در آن برای همه متغیرهای کنترل و همه کنترل‌شونده‌ها به یک سیاق است؛ سنت هدایت در قرآن کریم بر دو گونه تکوینی و تشریعی است. هدایت تکوینی که در تطابق با سرشت موجودات است و همه موجودات را در برمی‌گیرد، به‌معنای اعطای همه ابزار کمال و رساندن هر

[11] Julian Rotter

موجود به هدفی است که برای آن خلق شده است و هدایت تشریعی که مختص انسان و جنیان است و به تشریع و قانون‌گذاری در هدایت اشاره دارد. قرآن کریم می فرماید: «ربّنا الّذی أعطی کلّ شیءٍ خلقه ثمّ هدی» خداوند همه اشیاء را از راه فطرت یا غریزه یا میل که درون او قرار داده، به کمالهای شایسته‌اش راهنمایی کرده است (جوادی آملی، ۱۳۸۵، ص ۴۷).

از این رو هدایت تکوینی را می‌توان در سه رتبه طبقه‌بندی کرد: (۱) هدایت تکوینی عامه؛ (۲) هدایت تکوینی خاص؛ (۳) هدایت تکوینی خاص الخاص. اما هدایت تشریعی منحصر در هدایت تشریعی عامه است و همین نوع از هدایت است که فصل ممیز نظام ولایت با نظام سایبرنتیکی است. زیرا لازمه برخورداری از این هدایت انتخابگری و غایت‌انگاری هدایت‌شونده است و از انجا که قرآن به ابعاد و ساحات وجودی انسان واقف است در هدایت‌گری خود بر این تمایزات توجه داشته است.

۲.۵ انواع هدایت

(۱) هدایت تکوینی عامه: این هدایت، همان نظام و سازمان خلقت است که خداوند موجودات را بر طبق آن آفریده، به‌طوری که تمام هستی، هماهنگ و متحد، به‌سوی غایتی در حرکت و تکاپویند. در برابر این هدایت، هیچ‌گونه ضلالتی وجود ندارد.

(۲) هدایت تکوینی خاص: هدایتی که منحصر در انسان‌هاست و لازمه آن برخورداری از عقل و فطرت است. در این نوع هدایت متعلّق هدایت و اراده تکوینی، فعل خود هدایت‌کننده و مرید، یعنی خداوند است و هیچگونه تخلّفی در آن راه ندارد. «و لله جنود السّماوات و الأرض و کان الله عزیزاً حکیماً» (فتح/ ۷) (جوادی آملی، ۱۳۸۵، ص ۵۷).

(۳) هدایت تشریعی عامه: این نوع هدایت، مخصوص انسان است؛ زیرا تشریع و قانون‌گذاری، در ظرف اختیار و توان کنش‌های انتخابی و گزینش، موضوعیت دارد و بدون آن، بی معناست. چنین هدایتی نیز از نظر قرآن در ظرف خود فراگیر و همگانی است؛ «وَ لِكُلِّ قَوْمٍ هادٍ» (رعد/ ۷).

در برابر این گونه هدایت نیز هیچ ضلالتی نیست و اراده‌ی الهی بر این قرار است که انسان ها با اختیار خود، راه درست را برگزینند؛ نه به‌نحو اجبار و با سلب اختیار. اگر اراده خداوند بر این بود که همه را جبراً، به راه راست بکشاند، نیازی به بعثت و رسالت انبیاء نبود. از این رو، فرمود: «وَلَوْ شَاءَ رَبُّكَ لآمَنَ مَنْ فِي الْأَرْضِ كُلُّهُمْ جَمِيعًا؛ أَفَأَنْتَ تُكْرِهُ النَّاسَ حَتَّىٰ يَكُونُوا مُؤْمِنِينَ» (یونس/ ۹۹).

از این رو متعلّق هدایت و اراده تشریعی، فعل هدایت‌شونده یعنی انسان است که با اراده خویش در کمال اختیار و آزادی، نه تفویض و نه جبر، عمل می‌کند و تخلّفپذیری از تشریع نیز برای انسان مقدور است؛ «و أمّا ثمود فهدیناهم فاستحبّوا العمی علی الهدی» (فصلت/ ۱۷) و «إنّا هدیناه السّبیل إمّا شاکراً و إمّا کفوراً» (انسان/ ۳) (جوادی آملی، ۱۳۸۵، ص۵۷).

بنابراین هدایت مذکور در آیه شریفه مرتبه‌ای از هدایت است که راه دستیابی به مقصد را بر همگان می‌نمایاند و به «ارائة الطریق» معروف است. در مقابل رتبه بعدی که متعلق به خواص است «ایصال الی

المطلوب» نامیده می‌شود و جنبه راهبردی دارد و راهیان طریق را به مقصد می‌رساند (طباطبایی، ترجمه موسوی، ۱۳۷۴، ج ۷، ص ۴۷۷).

(۴) هدایت تکوینی خاص الخاص: این هدایت، مخصوص مؤمنان است؛ یعنی کسانی که با اختیار خویش، در برابر هدایت رسولان الهی و در پرتوعقل و فطرت، تسلیم شدند و در نهایت خداوند باب هدایت دیگری را برتر از هدایت‌های قسم پیشین، برای آنان می‌گشاید و معنای ایصال به مطلوب که اشاره به این نوع هدایت تکوینی دارد، یعنی دست طرف را گرفتن و به مقصدش رساندن که در آیه «وَ لَوْ شِئْنا لَرَفَعْناهُ بِها وَ لكِنَّهُ أَخْلَدَ إِلَى الْأَرْضِ وَ اتَّبَعَ هَواهُ» (اعراف/ ۱۷۶) و آیه «فَمَنْ يُرِدِ اللَّهُ أَنْ يَهْدِيَهُ يَشْرَحْ صَدْرَهُ لِلْإِسْلامِ» (انعام/ ۱۲۵) به آن اشاره شده است (طباطبایی، ۱۴۰۲ق، ج ۷، ص ۴۷۷).

بر اساس مراتب هدایت نگرش به کانون کنترل از زاویه دید قرآن کریم، طریقی میان کنترل درونی و بیرونی را نشان می‌دهد با این تفاوت که کنترل درونی مقدم بر کنترل بیرونی است و خداوند متعال ایجاد تغییر از جانب خود را منوط به تغییر توسط انسان دانسته است: «إِنَّ اللَّهَ لَا يُغَيِّرُ مَا بِقَوْمٍ حَتَّىٰ يُغَيِّرُوا مَا بِأَنْفُسِهِمْ» (رعد/ ۱۱) (عمیدی مظاهری و درزی، ۱۳۹۲، صص ۱۲۱-۱۲۲).

بنابراین در نظام ولایت بنابر مراتب تشکیکی عالم وجود هدایت‌کننده در یک سیستم جامع پیچیده، علاوه بر شمولیت هدایت به تمایزات هدایت‌شونده‌ها توجه دارد و مراتب هدایت تکوینی و تشریعی را به فراخور کمال شایسته هر موجودی تبیین می‌کند. اما در نظام سایبرنتیکی با توجه به اشراف هر سطح فوقانی بر سطوح و طبقات پایین‌تر سیستم سایبرنتیکی قابلیت سامان‌دهی به سیستم انسان‌شناختی که شناور در سطوح مختلف هستی و فراتر از اوست را ندارد و جریان کنترل ناظر به امور مادی و فیزیکال است و لذا در این نظام تمایزی بین انسان و سایر کنترل شونده‌ها نیست و با نگاهی مادی‌گرایانه سعی در سیطره بر انسان است. از این جهت می‌توان نظام سایبرنتیکی را مرتبه‌ای نازله از نظام ولایت برشمرد. زیرا سنت هدایت در نظام ولایت در سیستمی پیچیده‌تر و کامل‌تر از سیستم‌های سایبرنتیکی و ناظر به همه ابعاد و ساحات وجودی انسان مطرح است.

۳.۵ تمایز میان هدایت‌شونده و کنترل‌شونده

در نظام سایبرنتیک انسان به‌منزلهٔ جزئی کنترل‌شونده از سیستم و موجودی مادی است و نهایت کمال متصور برای آن تنظیم و تعادل سیستماتیک و مادی است. در حالی که در نظام ولایت، انسان از فطرتی الهی و طبیعتی مادّی تکوّن یافته و هدف از آفرینش این موجود دو بعدی، رسیدن او به کمال در خور خویش و دستیابی وی به مقام «خلیفة اللّهی» است (جوادی آملی، عبدالله، ۱۳۸۵، ص ۳۰). در نگرش قرآن به انسان علاوه بر بعد جسمانی بعد نفسانی انسان مورد توجه است. بعد نفسانی ساحتی است که حقیقت انسان ناظر به آن است و فصل ممیز انسان از حیوان ناظر به همین بعد است. این بعد خود شامل سه ساحت است: ۱. ساحت معرفتی، شناختی یا بینشی؛ ۲. ساحت احساسی، عاطفی یا گرایشی؛ ۳. ساحت فعلی، رفتاری یا کرداری (رضوانی و شریفی، ۱۳۹۸، ص ۲۱). علامه مصباح با اشاره به این ساحات، ساحت بینش و گرایش را منتسب به قلب (فؤاد) و ساحت رفتار را ناظر به روح می‌داند (مصباح یزدی، ۱۳۹۴، ج۱، ص۵۵).

علاوه براین درنظام سایبرنتیکی، کنترل‌شونده موجودی فاقد هوشمندی واختیاراست، در حالی که براساس آیات قرآن شعور و آگاهی در همه هستی سریان دارد «وَ إِنْ مِنْ شَیْءٍ إِلاَّ یُسَبِّحُ بِحَمْدِهِ وَ لکِنْ لا تَفْقَهُونَ تَسْبیحَهُم» (اسراء/۴۴) (سبحانی، جعفر، ۱۴۲۱، ج ۱، ص ۲۵۵؛ جوادی آملی، عبدالله، ۱۳۸۵، ص ۳۳)؛ با این تفاوت که انسان تنها موجودی است که با اختیار خود سعادت و شقاوت خویش را انتخاب می‌کند «إنّا هدیناه السّبیل إمّا شاکراً و إمّا کفوراً» (انسان/ ۳). متعلّق هدایت و اراده تشریعی، فعل هدایت‌شونده یعنی انسان است که با اراده خویش در کمال اختیار و آزادی، نه تفویض، آن را انجام دهد و تخلّفپذیر نیز هست (جوادی آملی، عبدالله، ۱۳۸۵، ص ۵۷).

در حقیقت انسان موجودی ذوابعاد است و علاوه بر رفتارهای هوشمندانه‌ای، مشابه رفتار سایر حیوانات، توانایی تفکر انتزاعی دارد، که او را قادر می‌سازد اهداف بلند مدتی را برای خود تعریف و سبک خاصی از زندگی را برای دستیابی به این اهداف طراحی کند. به‌عبارتی بروز رفتارهای هدف‌مند در انسان به خاطر وجود عاملیتی همچون تفکر، اراده یا اختیار است و علت و محّرک این گونه رفتارها، هدف یا غایت اوست. بنابراین اغلب رفتارهای انسان باید بر اساس اهداف او بررسی گردد، نه علت‌های مادی. از این رو دو عامل مهم و تعیین کننده در نظام‌های شناختی رفتارهای هدف‌مند و پیچیده انسان‌ها، «عاملیت» و «غایی‌انگاری» است (آزادجو، ۱۳۹۷، ص۲).

موضوعی که محققان در حوزه سیستم‌های پیچیده بر آن اتفاق نظر دارند، چگونگی توصیف پدیده‌ها و رفتارهای پیچیده فیزیکی، زیستی، حتی انسانی و اجتماعی در قالب یک سیستم انتزاعی است. اما باید توجه داشت که در نظریه سیستم‌ها، رفتار خروجی سیستم حاصل فعالیت سیستم است، نه یک عامل درونی. اگر سیستمی از برخی ویژگی‌ها یا شرایط برخوردار باشد، رفتارهای هدفمند در آن پدیدار می‌شود. در این میان سیستم‌های سایبرنتیکی با دریافت فیدبک، به‌گونه‌ای هدفمند رفتار می‌کنند و از قابلیت خود تنظیم‌گری برخوردارند. اما اهمیت نظریه سیستم‌ها سایبرنتیک در این است که این نظریه مدل‌هایی را ارایه می‌دهد که در آن‌ها برای بررسی رفتارهای پیچیده نیاز به دو مؤلفه عاملیت و غایی‌انگاری وجود ندارد (همان، ص۶).

۴.۵ تمایز میان هدایت‌کننده و کنترل‌کننده

برخلاف نظام‌های سایبرنتیکی که کنترل‌کننده در سیستمی باز و در تعامل با محیط قادر به خود تنظیم‌گری و کنترل است؛ در نظام ولایت، هدایت‌گری در سیستمی بسته منحصر در اراده کمال مطلق و ورای وجود واحد غیری نیست که محیط برای سیستم باشد. قرآن کریم دلیل این انحصار را چنین بیان می‌فرماید: «قُلْ هَلْ مِنْ شُرَکائِکُمْ مَنْ یَهْدی إِلَی الْحَقِ قُلِ اللَّهُ یَهْدی لِلْحَقِّ أَ فَمَنْ یَهْدی إِلَی الْحَقِ أَحَقُّ أَنْ یُتَّبَعَ أَمَّنْ لا یَهِدِّی إِلاَّ أَنْ یُهْدی» (یونس/۳۵). فقط کسی حق هدایت کردن دیگری را دارد و باید از او پیروی کرد که به غیر خود بی‌نیاز باشد؛ یعنی ذاتاً مهتدی و هادی دیگران باشد، ولی کسی که به غیر خود نیازمند است و ذاتاً مهتدی نیست، حق هدایت دیگران را ندارد و نمیتوان از او پیروی کرد. زیرا آن که فاقد کمال هدایت است، چگونه میتواند کمالبخش دیگران باشد؟ (جوادی آملی، عبدالله، ۱۳۸۵، ص ۷۳).

بر این اساس بر مبنای نظام ولایت، مالکیت حقیقی عالم از آن کامل مطلق است و هدایت‌گری امری است

که از طرف او و در سیری تشکیکی و تنازلی، مبتنی بر اذن او، بر انسان کامل و سپس شبیه‌ترین انسان‌ها به ایشان جریان دارد: «وَجَعَلْناهُمْ أَئِمَّةً يَهْدُونَ بِأَمْرِنا» (انبیاء/۷۳) عبارت (وجعلناهم) نشان میدهد که انسان کامل و جانشینان او نیز هدایت استقلالی ندارند، بلکه آن را از خدای سبحان اخذ کرده است و از عبارت (بأمرنا) نیز برمیآید که هدایت آنان، نسبت به دیگران بر مدار اراده و امر خداوند است (جوادی آملی، عبدالله، ۱۳۸۵، ص ۷۸) و از این رو سریان قوانین و مبانی در این نظام، بر اساس تشریع حکیمانه خداوند پیش می‌رود (مصباح یزدی، ۱۳۹۴، ۲۷۱-۲۷۲).

کنترل‌کننده در نظام سایبرنتیک بر مبنای قدرت و ثروت تعیین می‌شود. امروزه اطلاعات ابزار کسب قدرت و ثروت شده است و کنترل‌گر با دریافتی که از بازخورد اطلاعات در محیط دریافت می‌کند، نوع و میزان اطلاعات ورودی را کنترل می‌کند تا چیرگی بر جوامع و انسان‌ها را تصاحب کند.

اما قرآن کریم هدایت‌گری را شایسته کسی می‌داند که از هرگونه نقص ضلالت و عیب غوایت پیراسته باشد «ما ضَلَّ صاحِبُكُمْ وَ ما غَوى» (نجم/ ۲) تا در هر شرایطی تن به رذالت ندهد و دنیای مادی او را نفریبد. چنانچه در زمان حاکمیت امیرالمؤمنین (ع)، با اینکه ایشان به دستگاه شناختی انسان‌ها علم لدنّی داشتند، اما راضی به سلب اختیار و اراده از مردم نشدند و فرمودند: «من به خوبی می‌دانم که چه چیز شما را اصلاح می‌کند و از انحراف باز می‌دارد، ولی به خدا قسم شما را با فاسد کردن خودم اصلاح نمی‌کنم.» (ثقفی، ترجمه زارعی، ۱۴۰۱، ص ۲۴۶). از این رو برترین نوع هدایت، رهبری بهترین موجود به سوی والاترین مقصد و کاملترین مقصود است (جوادی آملی، عبدالله، ۱۳۸۵، ص ۴۴).

۶ نتیجه‌گیری

در تئوری جامع سیستم‌ها کل عالم هستی به‌مثابه یک سیستم پیچیده کلان که دربرگیرنده سیستم‌های دیگر، از ساده‌ترین تا پیچیده ترین است، مورد مطالعه قرار می‌گیرد. سیستم سایبرنتیکی به عنوان یکی از سامانه‌های این سیستم کلان مبنای نظام سایبرنتیک قرار گرفته است. در نظام سایبرنتیک با توجه به نگاه ماتریالیستی و ماده‌انگار، کمال حقیقی فرد و جامعه رساندن سیستم به قدرت و ثروت هدف‌گذاری شده است؛ از این رو قوانین توسط عقل محدود بشری و بر اساس سیستم ساده سایبرنتیکی و با ابزار کنترل و به هدف سلطه و حاکمیت بر سیستم پیچیده جامع هستی و به‌جهت حکمرانی اجتماعی، بدون در نظر گرفتن ابعاد وجودی انسان، وضع می‌گردد.

بدیهی است چنین نظامی که در تمام شئون صعود و هبوط خود بر سیستم نازله سایبرنتیکی متّکی است، هیچگونه آثار وحدت حقیقی، معلولیت، مخلوقیت و سنّت الهی را در متن چنین نظامی مشاهده نمیکند؛ متدرجاً از شهود سنّت الهی محروم و از ادراک وحدت هستی، معلولیت و مخلوقیت و در نتیجه از نگاه به نظام فاعلی و غایی محجوب خواهد بود.

در مقابل نظام ولایت بر محور وجودی واحد، تئوری جامع ناظر به سیستم کل عالم هستی را به‌گونه‌ای سامان داده که هر موجودی بسته به استعداد و ظرف وجودی خود در مرتبه‌ای از این نظام تشکیکی از هدایتی که کمال شایسته او را تأمین می‌کند، برخوردار است. در این نظام قوانین توسط خالق نظام که موجودی کامل

و محیط بر کل سیستم است وضع می‌شود و در هدایت فرد، جامعه ونظام هستی به سمت کمال حقیقی‌شان، به ابعاد وجودی، خصائص و ویژگی‌ها، توانمندی و نیازها وسرشت ذاتی آن‌ها، توجه داد و علاوه بر اشراف بر کل سیستم جامع هستی، به تک‌تک اجزاء سیستم علم دارد.

مراجع

[۱] قرآن کریم

[۲] ابراین ج. ا.، ماراکاس. ج. (۱۳۹۲)، مبانی سیستم های اطلاعات مدیریت، ترجمه ا. مانیان، م. فتاحی، ب. وائق، نگاه دانش، تهران.

[۳] آذرباد، نسرین (۲۰۱۵)، چشم‌انداز سایبرنتیک در نظریه سیستمی، کنفرانس بین‌المللی معماری، شهرسازی، عمران، هنر، محیط زیست (افق‌های آینده و نگاه به گذشته)، ایران، تهران.

[۴] آزادجو، فرهاد (۱۳۹۷)، نظریه سیستم‌ها و سایبرنتیک در علوم شناختی، سایت ویرگول.

[۵] امیرخانی، امیرحسین و هیهاوندزواری‌پور، رسول (۱۳۹۶)، نظریه سیستمی، تفکر کل‌نگر و سیستمی و نقش آن در توسعه و تعالی سازمانی، دهمین کنفرانس بین‌المللی اقتصاد و مدیریت، دانشگاه آزاد اسلامی، ایران، رشت.

[۶] تصدیقی، محمدعلی (۱۳۸۹)، مولوی و تفکر سیستمی در مدیریت، نخستین همایش ملی ادبیات فارسی و پژوهش‌های میان‌رشته‌ای، بیرجند.

[۷] ثقفی، ابراهیم بن محمد، ترجمه سید محمود زارعی (۱۴۰۱)، ترجمه الغارات: سال‌های روایت نشده از حکومت امیرالمؤمنین، انتشارات بیان معنوی، نسخه الکترونیکی.

[۸] جوادی آملی، عبدالله (۱۳۸۵)، هدایت در قرآن، تحقیق علی عباسیان، اسراء، چ دوم، قم.

[۹] جوادی آملی، عبدالله (۱۳۸۴)، فطرت در قرآن، تحقیق محمدرضا مصطفی‌پور، ش سوم، اسراء، قم.

[۱۰] جوهری، اسماعیل بن حماد (۱۴۰۴ ق.)، الصحاح تاج الغه، دار العلم للملایین، بیروت.

[۱۱] حاجی‌شمسایی، علی و نوشین‌فرد، فاطمه (۱۳۹۳)، سایکوسایبرنتیک (سایبرنتیک در روانشناسی)، فصلنامه روان‌شناسی صنعتی/ سازمانی، سال پنجم، شماره نوزدهم، صص ۹۷-۱۰۱.

[۱۲] رضوانی، علی و شریفی، احمد (۱۳۹۸)، قرآن و ارزش‌های اخلاقی ناظر به ساحت‌های سه‌گانه وجودی انسان، معرفت اخلاقی، سال دهم، شماره دوم، صص ۱۹-۳۴.

[۱۳] محمدی، بهزاد و قشقایی‌زاده، نصرالله (۱۳۹۳)، جایگاه تفکر اسلامی به نگرش سیستمی در مدیریت، مجله پژوهش‌های تعلیم و تربیت اسلامی، پیاپی ۹، صص ۹۵-۱۲۳.

[۱۴] سبحانی تبریزی، جعفر (۱۴۲۱ ق.)، مفاهیم القرآن، مؤسسة الإمام الصادق (علیه السلام)، قم.

[۱۵] طباطبایی، محمدحسین (۱۴۰۲ ق.)، ترجمه تفسیر المیزان، تحقیق موسوی، محمد باقر، (۱۴۲۱ ق.)، جامعه مدرسین حوزه علمیه قم، دفتر انتشارات اسلامی، قم.

[۱۶] علی‌احمدی، علیرضا و مشایخ، محمدرضا (۱۳۹۳)، تحل ل نظریه سامانه ا از دیدگاه تطب قي مولوی و کنت بولدینگ م لر، نشریه مدیریت فردا، شماره ۴۰، صص ۵-۱۸.

[۱۷] عمیدی مظاهری، مریم و درزی، قاسم (۱۳۹۲)، کانون کنترل انسان در قرآن با تأکید بر مفهوم جبر و اختیار، دو فصلنامه تخصصی پژوهش‌های میان‌رشته‌ای قرآن کریم، سال چهارم، شماره اول، صص ۱۱۳-۱۲۴.

[۱۸] مصباح یزدی، محمدتقی (۱۳۹۴)، پند جاوید، مؤسسه آموزشی پژوهشی امام خمینی (ره)، قم.

[۱۹] هچ، مری جو و کانلیف، ان ال (بی‌تا)، نظریه سازمان: دیدگاه‌های مدرن، نمادین و پست مدرن، ترجمه مریم رسولی و ساغر آشوری، ویرایش سوم، نسخه الکترونیکی.

[20] Mingers, John (2017). “Back to the future: A critique of Demetis and Lee’s Crafting theory to satisfy the requirements of systems science”. Information and Organization 27, no. 1.

[21] von Bertalanffy, L. (1967). General systems theory: Application to psychology, social science. Inform. Sci. Soc., 6 , 125–136.

[22] YI LIN, (2002). General systems theory: a mathematical approach. Kluwer Academic Publishers. Created in the United States of America.

ابعاد و مؤلفه‌های ساختاردهی فرهنگ امنیت سایبری در سازمان‌ها

بهمن جهانی[۱]، سید نصیب‌اله دوستی‌مطلق[۲]

[۱]دانشجوی دکتری مدیریت راهبردی فضای سایبر گرایش امنیت سایبری، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران
bhjahani@gmail.com
[۲]استادیار، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی، تهران، ایران
doustimotlagh@chmail.ir

چکیده

نتایج بدست آمده از تحقیقات مراکز پژوهشی و خدمات امنیت سایبری نشان می‌دهد که توسعه فناوری‌های زیرساختی، تدوین و ابلاغ دستورالعمل‌های امنیت سایبری و تربیت متخصصین این حوزه، در دفع تهدیدات چندان موفق نبوده و همچنان خسارت و آسیب به سرمایه‌های سایبری سازمان‌ها رو به افزایش است. یافته‌های این تحقیقات نشان می‌دهد که کارکنان در ایجاد تهدیدات امنیت سایبری سازمان‌ها یا تأمین آن نقش بسیار مهمی دارند که عدم توجه به این موضوع از مهمترین دلایل شکست برنامه‌های امنیت سایبری است. براین‌اساس حوزه جدیدی تحت عنوان فرهنگ امنیت سایبری، به جهت کلیدی بودن فرهنگ در شکل‌دهی به رفتار کارکنان، مطرح گردیده است. این تحقیق در پی یافتن ابعاد و مؤلفه‌های کلیدی و اثرگذار در ایجاد و ساختاردهی فرهنگ امنیت سایبری در سازمان‌ها است. این پژوهش از نوع کاربردی بوده و با استفاده از روش توصیفی تحلیلی با استناد به منابع کتابخانه‌ای، و تحلیل و بررسی اسناد این حوزه و بهره‌گیری از نظرات خبرگان، به دنبال ابعاد و مؤلفه‌های کلیدی ایجاد فرهنگ امنیت سایبری است. نتایج حاصل از تحقیق در سطح راهبردی ۵ بعد و ۱۶ مؤلفه، سطح عملیاتی ۷ بعد و ۱۸ مؤلفه و سطح تکنیکی ۴ بعد و ۸ مؤلفه را بر فرهنگ امنیت سایبری سازمان‌ها مؤثر دانسته است.

کلمات کلیدی: فرهنگ امنیت سایبری، مدل فرهنگ امنیت سایبری، فرهنگ سازمانی.

۱ مقدمه

پس از بررسی حوادث سایبری در سال‌های اخیر، محققین دریافتند که امنیت سایبری صرفاً در مؤلفه‌های سخت‌افزاری، نرم‌افزاری و زیرساخت‌ها خلاصه نمی‌شود و انسان‌ها مؤلفه بسیار مهمی هستند که هم در مؤلفه‌های دیگر نقش مستقیم و غیرمستقیم دارند و هم خود، مؤلفه مستقل و مؤثر هستند. بنابراین مقوله

ایجاد تغییر در رفتار و نگرش کارکنان در سازمان‌ها در همسویی با امنیت سایبری مطرح گردید. البته در دستورالعمل‌ها و نظامات پیشین نیز توجه به عوامل انسانی وجود داشته، لیکن فرض آن‌ها در رابطه با عامل انسانی به عنوان یک مؤلفه فرعی بوده و برنامه‌های امنیتی کارکنان نیز به نسبت همین دیدگاه در آموزش‌های کوتاه‌مدت و ابتدایی خلاصه شده است.

از جمله عوامل تأثیرگذار و درعین حال کلیدی در شکل‌گیری بینش و رفتار کارکنان، فرهنگ سازمان است. لذا تبدیل امنیت سایبری در سازمان‌ها به فرهنگ، یکی از روش‌های ایجاد همسویی کارکنان با سیاست‌های امنیت سایبری است و بدین جهت مقوله فرهنگ امنیت سایبری[1] به عنوان یکی از راهکارهای مناسب در تقویت جایگاه مؤلفه انسانی در زنجیره تأمین امنیت سایبری پیشنهاد شده است.

فرهنگ امنیت سایبری سازمان‌ها به دانش، باورها، ادراکات، نگرش‌ها، مفروضات، هنجارها و ارزش‌های افراد در رابطه با امنیت سایبری و نحوه انعکاس آنها، در رفتار افراد نسبت به فضای سایبر اشاره دارد. موضوع فرهنگ سازمانی امنیت سایبری، ملاحظات امنیت سایبری را بخشی جدایی‌ناپذیر از شغل، عادات و رفتار کارکنان می‌داند و آنها را جزئی از اقدامات روزمره تلقی می‌کند. از طرفی با توجه به اینکه محیط‌های کسب‌وکار دائماً در حال تغییرند، لذا سازمان‌ها نیز باید به طور فعال فرهنگ امنیت سایبری خود را در پاسخ به فناوری‌ها و تهدیدات جدید و همچنین اهداف، فرآیندها و ساختارهای متغیر خود حفظ و تطبیق دهند. یک فرهنگ امنیت سایبری موفق، تفکر امنیتی همه کارکنان (از جمله تیم امنیتی) را شکل می‌دهد، انعطاف‌پذیری را در برابر همه تهدیدات سایبری بهبود می‌بخشد، و در عین حال از تحمیل مراحل و هزینه‌های امنیتی سنگین که مانع انجام مؤثر وظایف کلیدی کسب‌وکار است، پرهیز می‌کند [۸].

ایجاد فرهنگ امنیت سایبری مانند ایجاد و توسعه هر کلان طرحی در سازمان‌ها نیازمند برنامه‌ریزی است. برنامه‌ریزی نیز بدون شناخت دقیق مفهوم و درک ابعاد و مؤلفه‌های کلیدی و اثرگذار امکان‌پذیر نمی‌باشد. بدین منظور، این تحقیق بدنبال یافتن پاسخ به این پرسش است که جهت ایجاد فرهنگ امنیت سایبری کدامیک از ابعاد و مؤلفه‌های سازمان باید مدنظر قرار گرفته و نسبت به تغییر و همسو نمودن آنها برنامه‌ریزی لازم صورت پذیرد.

در راستای تحقق هدف تحقیق ابتدا در ادبیات نظری، تعاریف و مفاهیم فرهنگ سازمانی و فرهنگ امنیت سایبری مرور شده و سپس ضرورت توجه به این موضوع مدنظر قرار گرفته است. از آنجایی که تدوین مدل‌ها، مبتنی بر ابعاد و مؤلفه‌هاست، لذا در ادامه، مدل‌های مهمی که در حوزه ایجاد فرهنگ امنیت سایبری مطرح هستند، بررسی شده است. براساس مدل‌ها، ابعاد و مؤلفه‌ها استخراج شده و پس از طی فرایند تجزیه و تحلیل و تأیید خبرگان، در فصل یافته‌ها، ساختار کامل آنها ارائه شده است. نهایتاً در فصل نتیجه‌گیری توضیحاتی در رابطه با تحقیق و یافته‌های آن و تأثیر این تحقیق در حوزه‌های کاربردی و علمی امنیت سایبری ارائه شده است. همچنین پیشنهادهایی برای ادامه مسیر تحقیق و افزایش غنای علمی این حوزه ارائه گردیده است.

[1] Cyber Security Culture

۲ مبانی نظری و پیشینه تحقیق

۱.۲ پیشینه تحقیق

در رابطه با موضوع فرهنگ امنیت سایبری، تحقیقات مختلف و متنوعی در سال‌های اخیر خصوصاً از سال ۲۰۱۷ به بعد انجام شده که برخی از این تحقیقات که ارتباط بیشتری با این پژوهش دارند عبارتند از:

میکائیل وایل در مقاله خود که در راستای یافتن فرهنگ امنیت سایبری و رابطه آن با ابعاد مختلف سازمان انجام شده، ضمن تأیید رابطه فرهنگ سازمان با امنیت سایبری، مؤلفه‌های تعهد رهبر و چشم‌انداز سازمان را بر همسوسازی هنجارها، اقدامات رهبری و رفتار کارکنان در رابطه با امنیت سایبری مؤثر دانسته است [۱۱].

اخیار نصیر و همکاران در مقاله خود، عوامل ایجاد فرهنگ امنیت سایبری را در سازمان به چهار سطح تقسیم کرده‌اند؛ در سطح اول سیاست‌ها، دسترسی‌ها و مقررات، در سطح دوم و پائین‌تر، اهداف، راهبردها و اقدامات، و در سطح سوم هنجارها و رفتارهای امنیتی و در سطح آخر مجموعه اقدامات آگاهی و افزایش دانش در کارکنان را ذکر نموده‌اند [۱۲].

لین و وورن چارچوبی را در قالب سه فاز برای ایجاد امنیت سایبری در سازمان‌های نظامی پیشنهاد داده‌اند که در این تحقیق در فاز اول مؤلفه‌های سیاست‌ها، آموزش، برنامه‌ریزی و در فاز دوم، تمرینات سایبری، ارزیابی امنیت سایبری و در فاز سوم نیز که اجرای برنامه‌های تدوین شده است، مؤلفه‌ی آگاه‌سازی و ارزیابی را ارائه نموده‌اند [۱۰].

راملوکان و همکاران در تحقیق خود، چارچوب تغییرات مدیریتی در سازمان را جهت استقرار فرهنگ امنیت سایبری در قالب ۳ بعد در نظر گرفته‌اند: ۱) منابع: با مؤلفه‌های فناوری‌ها – فرایندها – افراد، ۲) قابلیت‌ها: با مؤلفه‌های کنترل‌های تکنیکی – حکمرانی – فرهنگ، ۳) مزیت رقابتی: با مؤلفه افزایش تاب‌آوری [۱۳].

۲.۲ مفاهیم و تعاریف

فرهنگ سازمانی

قبل از پرداختن به مفهوم فرهنگ امنیت سایبری باید منظور از فرهنگ سازمانی که مفهومی کلان‌تر است، مشخص گردد. برای فرهنگ سازمانی تعاریف متعدد و مختلفی در منابع ذکر شده که برخی از آنها عبارتند از [۱]:

- یک نظام اعتقادی، که بین اعضای یک سازمان مشترک است (Spender).
- ارزش‌های قوی که به‌طور گسترده مشترک است (Relly).
- مجموعه‌ای از باورهای مشترک و دائم که از طریق ابزارهای متنوع مادی منتقل می‌شوند و در زندگی افراد ایجاد معنا و مفهوم می‌کند (Kouzes, calwall and Posner).

- یک سلسله از نهادها، تشریفات، و اسطوره‌هایی که منتقل‌کننده ارزش‌ها و باورهای اساسی آن سازمان به کارکنانش می‌باشد (Petera and Waterman).

به‌طور کلی فرهنگ در سازمان، نقش‌های گوناگونی ایفا کرده و تعیین‌کننده مرز فکری و ارزشی سازمان است، نوعی احساس هویت در اعضای سازمان به‌وجود می‌آورد، باعث می‌شود نوعی تعهد جمعی در افراد به وجود آید، موجب ثبات و پایداری سازمان به‌عنوان یک سیستم اجتماعی می‌شود و بالاخره فرهنگ یک عامل قوی کنترل، کنترل مالی و بودجه‌ای در سازمان است [۲].

همچنین فرهنگ سازمانی به‌عنوان «ارزش‌ها و رفتارهایی تعریف می‌شود که به منحصر به‌فرد شدن محیط اجتماعی و روانی یک سازمان کمک می کند» [۲].

فرهنگ در سازمان تابع برخی نشانه‌ها و علائم است که برخی از آنها از نظر ادگار شاین عبارتند از [۲]:

۱. مقررات رفتاری مشاهده شده در تعاملات افراد با یکدیگر
۲. نُرم‌ها و هنجارهای گروهی
۳. ارزش‌های حمایت‌شده
۴. روش‌ها، عادت‌ها، تفکر، الگوهای ذهنی یا پارادایم‌ها
۵. مثل‌ها و استعاره‌ها

فرهنگ امنیت سایبری

اصطلاح «فرهنگ امنیت سایبری» در سال‌های اخیر مطرح شده و تعاریف مختلفی نیز برای آن ذکر شده است. اما تعریفی که مورد اجماع بیشتری است عبارت است از:

«فرهنگی که هر مشارکت‌کننده‌ای در جامعه اطلاعاتی، متناسب با نقش خود، از خطرات امنیتی مربوطه و اقدامات پیشگیرانه آگاه باشد، مسئولیت را بر عهده گیرد و برای بهبود امنیت سیستم‌ها و شبکه‌های اطلاعاتی خود گام بردارد» [۷].

تعاریف جامع دیگر در این رابطه توسط ICAO[۲] ارائه شده است. در این تعریف فرهنگ امنیت «مجموعه‌ای از هنجارها، باورها، ارزش‌ها، نگرش‌ها و مفروضاتی است که در عملکرد روزانه یک سازمان نهفته است و توسط اعمال و رفتار همه نهادها و پرسنل درون سازمان منعکس می‌شود و شامل امنیت همه سازمان است».

[۲] سازمان بین‌المللی هوانوردی کشوری

۳.۲ کارکنان و آسیب‌پذیری‌های سایبری

با مطالعه نقش کارکنان در آسیب‌پذیری‌های سایبری می‌توان به لزوم ایجاد فرهنگ سازمانی امنیت سایبری دست یافت، چرا که کارکنان و فرهنگ سازمانی دو موجودیت غیرقابل تفکیک و در تعامل با یکدیگرند. لذا بررسی آسیب‌پذیری‌های سایبری با منشأ کارکنان و ارتباط آن با فرهنگ سازمانی اجتناب ناپذیر است.

براساس تحقیقاتی که حاصل تحلیل داده‌های حوادث سایبری در شرکت‌ها و سازمان‌های مختلف دنیاست و توسط شرکت کسپرسکی[۳] انجام شده است، به‌طور کلی آسیب‌پذیری‌هایی که توسط کارکنان به‌صورت مستقیم یا غیرمستقیم ایجاد می‌گردند عبارتند از [۹]:

۱. خطا، بی‌احتیاطی و ناآگاهی کارکنان
۲. بی‌مسئولیتی کارکنان
۳. نداشتن دید جامع و کل‌نگر به امنیت اطلاعات در سازمان
۴. نادیده‌گرفتن امنیت اطلاعات در فرایندهای سازمان
۵. خطای تغییرات حفاظتی در زیرساخت‌های فنی توسط متخصصین امنیت
۶. خطای تدوین‌کنندگان سیاست‌های امنیت اطلاعات
۷. نادیده‌گرفتن تهدیدات و نشناختن صحیح سرمایه‌های سایبری و وابسته به سایبر
۸. خطای مدیران در نادیده گرفتن اهمیت جایگاه افسر امنیت سایبری در سازمان
۹. هزینه‌انگاری امنیت سایبری

۴.۲ ضرورت ایجاد فرهنگ امنیت سایبری

در ایجاد یک فرهنگ باید نسبت به چهار واقعیت آگاهی کامل داشت [۵]:

۱. در افزایش سطح آگاهی و تغییر رفتار، فرهنگ نقشی مهم ایفا می‌نماید.
۲. هر کسی جهان را از دریچه فرهنگ خود تفسیر می‌کند.
۳. فرهنگ درست و غلط وجود ندارد و فقط تفسیرهای متفاوت از یک وضعیت وجود دارد.
۴. کدام فرهنگ‌ها نقش آفرینند و مفروضات اساسی و مورد حمایت در آنها کدامند؟

[3] Kaspersky

مطابق نتایج تحقیقات ارائه شده، عوامل انسانی عامل اکثر نقض‌های داده در سازمان‌ها هستند، در حالی‌که سازمان‌ها دارای سیاست‌های امنیت سایبری هستند ولی کارمندان، آنها را به‌عنوان دستورالعمل‌های راهنما می‌بینند و نه قوانین لازم‌الاجرا [۳]. در مقابل، توسعه فرهنگ امنیت سایبری به جای تلاش برای وادار کردن افراد به رفتار ایمن، در بینش آنها تغییر ایجاد کرده، آگاهی امنیتی و درک مخاطرات را تقویت می‌کند و صمیمیت را در فرهنگ سازمانی به جای استفاده از قوانین سخت‌گیرانه و خشک حفظ می‌کند [۳].

تفاوت اصلی بین آگاهی امنیتی و فرهنگ امنیتی این است که فرهنگ چیزی بیش از آگاهی است. فرهنگ امنیتی ترکیبی از افراد، سیاست و فناوری است. نکته کلیدی این است که آگاهی یکی از مؤلفه‌های فرهنگ‌سازی است و نباید، تنها راه در رسیدن به سطح مطلوب پیشگیری از مخاطرات سایبری عوامل انسانی، در نظر گرفته شود [۳].

بنابراین هدف اصلی فرهنگ امنیت سایبری، توسعه و پیاده‌سازی زیست‌بوم فرهنگی برای حمایت از امنیت سایبری است. نیاز به پرداختن به فناوری و فرآیندهای امنیت سایبری مستلزم توسعه فرهنگ امنیت سایبری است. داشتن فرهنگ امنیت سایبری فرآیندی پویا است که توجه مستمر را می‌طلبد [۳].

۵.۲ مدل‌های فرهنگ امنیت سایبری

علی‌رغم نو بودن موضوع فرهنگ امنیت سایبری، به جهت اهمیت بالای این موضوع، مدل‌هایی جهت سنجش و ارائه تصویری از سطح سازمان در این حوزه، توسعه داده شده‌اند. عمدتا مدل‌های ارائه شده را می‌توان به دو گروه تقسیم نمود. گروه اول مدل‌هایی هستند که فرایند استقرار فرهنگ امنیت سایبری را مدنظر قرار داده‌اند و در آن‌ها کمتر به ابعاد و مؤلفه‌ها پرداخته شده است. گروهی دیگر به ابعاد و مؤلفه‌ها و ساختار مورد نیاز در کنار برنامه‌ها و فرایندها، برای ایجاد فرهنگ امنیت سایبری پرداخته‌اند. با توجه به موضوع، در این تحقیق به برخی از مهمترین مدل‌ها در گروه دوم اشاره می‌گردد.

مدل هفت‌بلوک فرهنگ امنیت سایبری

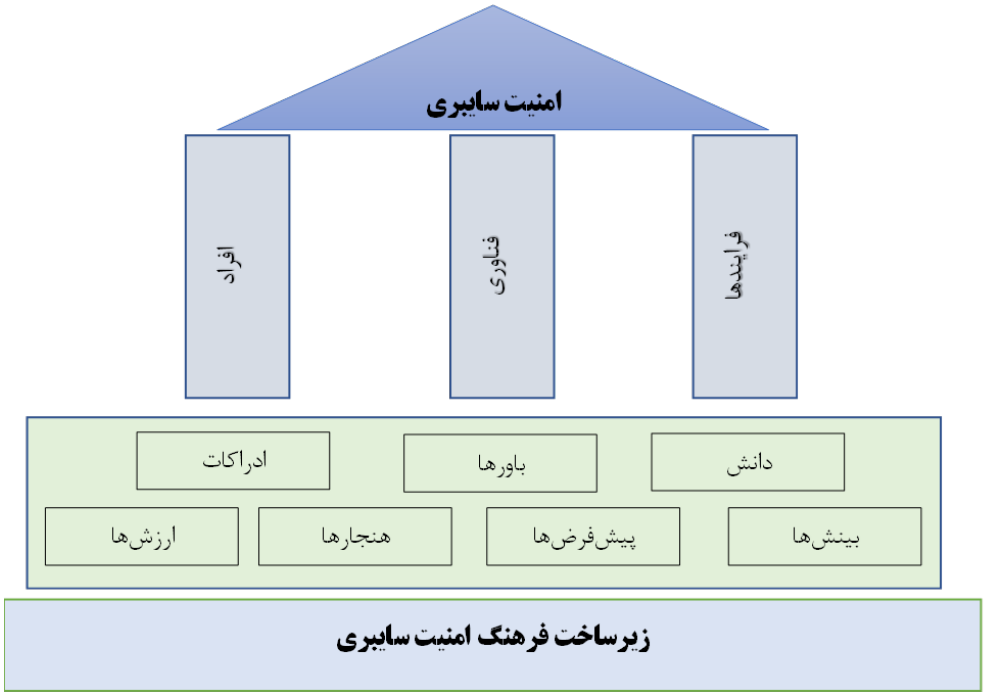
این مدل که در شکل ۱ زیرساخت فرهنگ امنیت سایبری را نشان می‌دهد از افراد، فناوری و فرآیندهای امنیت سایبری پشتیبانی می‌کند. اما ایجاد این مؤلفه‌ها که ستون‌های امنیت سایبری می‌باشند نیازمند زیرساخت‌هایی است. هفت بلوک دانش، باورها، ادراکات، نگرش‌ها، مفروضات، هنجارها و ارزش‌ها، محیط اجتماعی و روانی مناسبی را برای حمایت از امنیت سایبری فراهم می‌کند [۴].

مدل هفت‌بعدی اندازه‌گیری فرهنگ امنیت سایبری مؤسسه ENISA

در این مدل (ENISA)[۴] فرهنگ امنیت سایبری مبتنی بر امنیت اطلاعات به هفت بعد تقسیم شده است که عبارتند از [۶]:

۱. رفتارها: اقدامات ارادی یا آگاهانه کارکنان که مستقیم یا غیرمستقیم بر روی فرهنگ امنیت اثرگذار است.

[4] The European Union Agency for Cybersecurity



شکل ۱: مدل هفت‌بلوک زیرساخت فرهنگ امنیت سایبری [۴]

۲. نگرش‌ها: احساسات و گرایش‌ها در رابطه با اقداماتی که مرتبط با امنیت سازمان است.

۳. شناخت‌ها: دانش، آگاهی و باورهایی از کارکنان که بر اقدامات و کارآمدی آنها در امنیت سازمان مؤثر است.

۴. انطباق: مربوط به داشتن سیاست‌های امنیت سازمانی، آگاهی از آنها و دسترسی به دستورالعمل‌های حاصل از سیاست‌ها است.

۵. ارتباطات: راه‌هایی که کارکنان با دیگران در رابطه با مقوله‌های امنیت، گزارش‌دهی حوادث و احساس تعلق سازمانی ارتباط برقرار می‌کنند.

۶. هنجارها: اینکه کارکنان چه بخشی از اقدامات و عملیات سازمان را به‌طور طبیعی مرتبط با امنیت درک می‌کنند و چه بخشی را خارج از آن می‌دانند.

۷. مسئولیت‌ها: آگاهی از اینکه هریک از کارکنان عنصری حیاتی در پایداری یا از بین رفتن امنیت در سازمان هستند.

مؤسسه ENISA در رابطه با فرهنگ امنیت سایبری فرایندهای اقدام و مدل‌های مختلفی ارائه نموده است. این مؤسسه ابعاد اثرگذار بر فرهنگ امنیت سایبری را در سازمان‌ها به دو بعد اصلی انسانی و بیرونی تقسیم‌بندی نموده است.

۱. مؤلفه‌های انسان‌پایه:

۱-۱) روانشناختی: شامل عوامل و شرایطی است که منجر به تغییر رفتار انسان به‌لحاظ روان‌شناختی و درونی می‌گردد.

۱-۲) شخصیت و انطباق: شامل روش‌ها و فرایندهایی است که کارکنان در آن نسبت به تشخیص و مواجهه با تهدیدات سایبری، ریسک‌ها و حوادث، آگاهی و حساسیت یافته و مسئولیت‌پذیر می‌شوند و به‌عبارتی امنیت سایبری در کارکنان درونی‌سازی می‌گردد.

۱-۳) محیط اجتماعی: با توجه به اینکه انسان موجودی اجتماعی است، بسیاری از رفتارها در محیط اجتماع شکل می‌گیرد. براین اساس این مؤلفه شامل انتظارات و واکنش‌های مدیران و تأییدات و نگرش‌های همکاران پیرامونی در تغییر رفتار کارکنان است.

۲. مؤلفه‌های بیرونی:

فرهنگ ملی: عمده موارد مربوط به این مؤلفه مربوط به تأثیراتی است که فرهنگ یک کشور بر رفتار افراد آن می‌گذارد. اینکه رفتاری توسط فرهنگ ملی مورد تأیید یا رد قرار گیرد می‌تواند موجب رشد یا از بین رفتن آن رفتار در افراد گردد. لذا این مؤلفه شامل مواردی از فرهنگ درونی کشورها یا فرهنگ غالب خارج از سازمان است که بر تغییر رفتار کارکنان تأثیر می‌گذارد.

۳ روش‌شناسی تحقیق

از منظر هدف، این تحقیق کاربردی می‌باشد و روش تحقیق بکارگرفته شده در آن نیز، توصیفی تحلیلی است که با استناد به منابع کتابخانه‌ای و با تحلیل و بررسی اسناد در این حوزه، ابعاد و مؤلفه‌های مربوط به ایجاد و ساختاردهی فرهنگ امنیت سایبری سازمان‌ها را جستجو نموده است.

در فرایند انجام این پژوهش بدواً تعاریف و مفاهیم، مدل‌های فرهنگ سازمانی، فرهنگ امنیت سایبری در سازمان‌ها، از میان اطلاعات کتابخانه‌ای و اسناد معتبر اینترنتی مرتبط با موضوع، مورد مطالعه قرار گرفت. در انتخاب اسناد مورد مطالعه به‌روز و معتبر بودن، دو شاخص کلیدی بود که استخراج داده‌ها براساس این دو شاخص انجام شد. در این راستا ابعاد و مؤلفه‌ها، از میان مدل‌هایی که در منابع کتابخانه‌ای به آنها پرداخته شده بود، استخراج گردید و تطبیق و جمع‌بندی آنها براساس دو شاخص بیان شده؛ به‌روز بودن مطالب و اعتبار منابع انجام شد. نظر خبرگان فرهنگ سازمانی و امنیت سایبری در رابطه با ابعاد و مؤلفه‌های استخراج شده و در ادامه، سطوح سازمانی هریک از آنها، براساس ابزار پرسشنامه و طی فرایندهای مجزا، گردآوری و

مورد تجزیه و تحلیل قرار گرفت و نهایتاً ابعاد و مؤلفه‌های مرتبط با هدف تحقیق براساس سه سطح مدنظر مشخص شد.

۴ یافته‌ها

در ابتدای استخراج و جمع‌بندی ابعاد و مؤلفه‌های تحقیق، مشخص شد که ابعاد فرهنگ امنیت سایبری دارای اثرگذاری برابر نبوده و به‌طور کلی در سه سطح راهبردی، عملیاتی و تکنیکی منشأ اثر هستند. لذا هریک از ابعاد و مؤلفه‌ها بر اساس شدت اثرگذاری در یکی از سه سطح جای گرفت.

براین اساس نظر خبرگان بر روی سه مقوله سطح، بعد و مؤلفه دریافت شد. برای گردآوری داده‌ها ۲ پرسشنامه تدوین شد. در پرسشنامه اول ابعاد و مؤلفه‌ها مورد پرسش قرار گرفت. پس از تجزیه و تحلیل پاسخ‌ها، مواردی که امتیاز بالاتر از نصف یعنی ۲/۵ را کسب نموده بودند، از نظر خبرگان به عنوان ابعاد و مؤلفه‌های فرهنگ امنیت سایبری در نظر گرفته شدند. در ادامه جهت تعیین جایگاه هریک از ابعاد در سطوح سازمانی، پرسشنامه دوم به خبرگان ارائه شد و نظر ایشان در رابطه با جایگاه هریک از ابعاد اخذ شد. پس از تجزیه و تحلیل داده‌های این مرحله بالاترین امتیاز کسب شده برای هر بعد در سطوح مدنظر، به عنوان سطح مناسب خبرگان در نظر گرفته شد. براساس این دو فرایند گردآوری و تجزیه و تحلیل، نهایتا پاسخ به سئوال تحقیق که ابعاد و مؤلفه‌های ساختاردهی فرهنگ امنیت سایبری در سازمان‌ها بود در سه سطح، براساس جدول ۱ مشخص شد.

۵ نتیجه‌گیری

در کنار برنامه‌ها و دستورالعمل‌های صرفاً حقوقی و فنی که تاکنون جهت ارتقاء امنیت سایبری در کشور اجرا شده، نتایج حاصل از این تحقیق روش دیگری را پیشنهاد می‌نماید که در آن امنیت سایبری در جو حاکم برسازمان یا فرهنگ غالب آن جاری می‌شود و رفتار امن در کلیه سطوح سازمانی در کارکنان و مدیران درونی می‌گردد.

جهت پاسخ به مسئله تحقیق که ابعاد و مؤلفه‌های مؤثر بر ایجاد و ساختاردهی فرهنگ امنیت سایبری در سازمان می‌باشد، ادبیات، مدل‌ها و فرایندهای ایجاد فرهنگ امنیت سایبری مدنظر قرار گرفت. در فرایند مطالعه مشخص شد که فرهنگ امنیت سایبری با سه سطح راهبردی، عملیاتی و تکنیکی سازمان‌ها در تعامل است و تصمیمات و اقدامات سازمان در این سه سطح بر ایجاد این نوع فرهنگ در سازمان به نسبت اهمیت و جایگاه آن سطح، تأثیر دارد. بنابراین نمی‌توان سطح تأثیر ابعاد و مؤلفه‌ها را برابر درنظر گرفت.

ابعاد و مؤلفه‌های سطح راهبردی در پی ایجاد و همسوسازی ارزش‌ها، راهبردها، سیاست‌ها و دستورالعمل‌ها و ساختار سازمان با فرهنگ امنیت سایبری است. همچنین در سطح عملیاتی به اقدامات مختلفی در سازمان در حوزه‌های کارکنان و مشاغل آنها و اقدامات سایبری همچون تمرینات، هنجارسازی، اتحادها و اطلاع‌رسانی در میان همه کارکنان تأکید دارد تا امنیت سایبری را به امری روزمره و جدایی‌ناپذیر از فعالیت‌ها و وظایف مدیران و کارکنان سازمان مبدل کند. اما در سطح تکنیکی به فراهم نمودن بسترهای

جدول ۱: سطوح، ابعاد و مؤلفه‌های ساختاردهی فرهنگ امنیت سایبری

سطح سازمانی	ابعاد	مؤلفه‌ها
راهبردی	ارزش‌ها	حفظ و صیانت از سرمایه‌های سایبری- صیانت از کارکنان در مقابل حوادث سایبری
	سبک رهبری	حمایت از امنیت- واکنش به حوادث سایبری- واکنش به رفتار کارکنان در حوادث سایبری- مدیریت سرمایه‌های سایبری
	راهبردها	انطباق راهبردهای موجود با امنیت سایبری- راهبرد امنیت سایبری- ایجاد راهبرد فرهنگ امنیت سایبری- ایجاد راهبردهای کاهش اثرات منفی محیط پیرامونی در فرهنگ امنیت سایبری
	سیاست‌ها	انطباق سیاست‌های موجود با امنیت سایبری- ایجاد سیاست‌های جدید امنیت سایبری
	ساختار	تقویت جایگاه سازمانی امنیت سایبری- تطبیق مشاغل و جایگاه آنها با آسیب‌پذیری‌های سایبری مرتبط- تطبیق سلسله‌مراتب گزارش‌دهی با پاسخ‌گویی حوادث سایبری
عملیاتی	آموزش و آگاه‌سازی	انطباق برنامه‌های آموزشی موجود با امنیت سایبری- تدوین و اجرای برنامه‌های آموزشی امنیت سایبری کارکنان- تدوین و اجرای برنامه‌های آموزشی ویژه متخصصین سایبری
	امور شناختی	بررسی و شخصیت شناسی کارکنان نسبت به امنیت سایبری- تدوین برنامه روانشناختی مدیران و کارکنان در تطبیق و تثبیت رفتار امنیت سایبری - تدوین برنامه‌های شناختی در تقویت مسئولیت‌پذیری و پاسخگویی در قبال امنیت سایبری
	امور خدمات شغلی	تطبیق مشاغل با آسیب‌پذیری‌های سایبری آنها- تدوین برنامه ترغیب و تنبیه کارکنان در قبال رفتارها و واکنش‌های منطبق با امنیت سایبری- ایجاد برنامه چرخش شغلی کارکنان در انطباق شخصیت، شغل و آسیب‌پذیری سایبری
	تمرینات سایبری	تدوین و اجرای برنامه برگزاری تمرینات سایبری دوره‌ای درون سازمانی- تدوین و اجرای برگزاری تمرینات سایبری با سازمان‌های متولی- تدوین و اجرای برگزاری تمرینات سایبری با سازمان‌های همکار
	اتحادهای سایبری	همکاری با سازمان‌های همسو در حوزه امنیت سایبری- ایجاد روش‌ها و دستورالعمل‌های برقراری ارتباط سایبری میان سازمانی
	هنجارسازی امنیت سایبری	استفاده از نمادهای امنیت سایبری- ایجاد گروه‌های رسمی و غیررسمی رصد، مقابله و پاسخ‌گویی امنیت سایبری
	اطلاع‌رسانی امنیت سایبری	استفاده از شبکه‌های اطلاع‌رسانی درون سازمانی- ایجاد کمپین‌های امنیت سایبری- ایجاد شبکه اطلاع‌رسانی واکنش به حوادث سایبری
تکنیکی	تقویت زیرساخت	ایجاد زیرساخت شبیه‌سازی تمرینات سایبری- ایجاد زیرساخت رصد و تشخیص رفتار کارکنان در قبال امنیت سایبری
	اطلاع‌رسانی فنی	تدوین برنامه گزارش‌دهی دوره‌ای آسیب‌پذیری‌ها- شبکه اطلاع‌رسانی و آگاه‌سازی از آسیب‌پذیری‌های جدید
	شبکه ارتباط درون سازمانی	ایجاد شبکه‌های ارتباطی کارکنان در حوزه امنیت سایبری- ایجاد بسترهای امن ارتباط میان کارکنان در حوادث سایبری
	شبکه ارتباط برون سازمانی	ایجاد بستر امن ارتباط کارکنان سایبری سازمان با کارکنان سایبری سازمان‌های همسو- ایجاد بستر تمرینات سایبری میان سازمانی

فنی فرهنگ امنیت سایبری که در سطوح بالاتر مدنظر قرار گرفته شده بود می‌پردازد و علاوه برآن شبکه‌هایی جهت ارتباط برون‌سازمانی فراهم می‌نماید.

برای ایجاد فرهنگ امنیت سایبری در سازمان، بررسی تحقیقات قبلی توسط محقق نمایانگر این موضوع است که موارد انجام شده بر اساس هدفی خاص بوده و باهدف این تحقیق که نگاهی جامع به کلیه ابعاد و سطوح سازمان در ایجاد فرهنگ سایبری است، تفاوت داشته‌اند. نتایج این تحقیق با توجه به عمومیت و جامعیت نسبی آن و توجه به تمام سطوح سازمان، می‌تواند دستورالعمل و راهنمایی برای برنامه‌ریزان سازمانی باشد تا در تدوین برنامه ارتقاء فرهنگ امنیت سایبری به سطوح، ابعاد و مؤلفه‌های مختلف توجه نموده و امنیت سایبری را امری جامع و چندبعدی در نظر گیرند. همچنین نتایج این تحقیق راهنمایی است برای محققینی که در این موضوع اقدام به تحقیق می‌نمایند، تا براساس آن بتوانند به مدل‌های مختلف فرهنگ امنیت سایبری پرداخته و دامنه موضوع را توسعه و تعمیق بخشند.

محققین علاقمند به این موضوع می‌توانند در رابطه با ابعاد و مؤلفه‌های فرهنگ امنیت سایبری در حوزه‌های تخصصی همانند صنایع، امور نظامی و زیرساخت‌های حیاتی به تحقیق بپردازند. همچنین روش‌های ارزیابی و سنجش ارتقاء فرهنگ امنیت سایبری در سازمان‌ها با هدف ایجاد مسیر برای برنامه‌ریزی را به عنوان موضوع تحقیق مدنظر قرار دهند. علاوه بر آن به نظر می‌رسد با توجه به اهمیت بسیار بالای امور شناختی کارکنان و ارتباط آن با فرهنگ امنیت سایبری، می‌توان به این مقوله به صورت ویژه توجه نموده و تحقیقاتی در رابطه با این موضوع صورت پذیرد.

مراجع

[۱] سعیدی، پرویز (۱۳۸۹). شناسایی فرهنگ سازمانی براساس مدل کویین و گارت. فصلنامه روانشناسی تربیتی.

[۲] طوسی، محمدعلی (۱۳۷۲). فرهنگ سازمانی. تهران: مرکز آموزش مدیریت دولتی.

[3] A. Fagerström (2013). Creating, Maintaining and Managing an Information Security Culture.

[4] Alvarez-Dionisi, L., & Urrego-Baquero, N. (2019, March 15). Implementing a Cybersecurity Culture. Retrieved from ISACA: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/implementing-a-cybersecurity-culture

[5] Barker, J., Davis, A., Hallas, B., & Mc Mahon, C. (2021). Cybersecurity ABCs: Delivering awareness, behaviours and culture change. BCS Publishing.

[6] Cyber Security Culture in organisations. (2017). ENISA.

[7] Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. Journal of Computer Information Systems, DOI: 10.1080/08874417.2020.1845583, pp. 452-462.

[8] Henry, Shawn (2017, 11, 17). IABM. Retrieved from The Top 5 Cybersecurity Mistakes Companies Make and How to Avoid Them: https://theiabm.org/top-5-cybersecurity-mistakes-companies-make-avoid/

[9] Kaspersky. Retrieved from https://www.kaspersky.com/blog/the-human-factor-in-it-security/

[10] Leenen, L. v. (2019). Framework for the cultivation of a military cybersecurity culture. 14th International Conference on Cyber Warfare and Security (ICCWS 2019) pp. 212-220.

[11] Mncedisi Willie, M. (2023). The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture. SSRN.

[12] Nasir, A. F. (2023). How to Cultivate Cyber Security Culture? The Evidences from Literature. International Journal of Synergy in Engineering and Technology, pp. 13-19.

[13] Ramluckan, T. (2020). A Change Management Perspective to Implementing a Cyber Security Culture. 19th European Conference on Cyber Warfare and Security. 10.34190/EWS.20.059.

تشخیص وب‌سایت‌های اسپم فارسی با استفاده از پردازش زبان طبیعی

صبا حیدری‌دوست [۱]، امیرحسین کیهانی‌پور [۲]

[۱] کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
saba.heydaridoost@ut.ac.ir
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
keyhanipour@ut.ac.ir

چکیده

تولید صفحات اسپم به عنوان یکی روش‌های جلب توجه کاربر به محتوای غیر مطلوب، یکی از چالش‌های عمده در حوزه بازیابی اطلاعات به ویژه در محیط وب، بشمار می‌رود و طی سالهای گذشته، الگوریتم‌های مختلفی برای تشخیص آنها مطرح شده است. بر این اساس، روش‌های تولید اسپم نیز همزمان با پیشرفت فناوری، تغییر شکل می‌دهند. امروزه، یکی از روش‌های غیرقانونی افزایش رتبه وب‌سایت، استفاده از وب‌سایت‌های اسپم است. در این مقاله، ابتدا انواع اسپم و روش‌های شناسایی وب‌سایت‌های اسپم مورد بررسی قرار گرفته است. سپس یک مجموعه داده شامل وب‌سایت‌های اسپم و غیر اسپم در وب فارسی، معرفی شده و با استفاده از این مجموعه داده، یک مدل Multinomial Naïve Bayes آموزش دیده است. در این مدل، متون این وب‌سایت‌ها با توجه به تکنیک‌های پردازش زبان طبیعی، مورد بررسی قرار گرفته است و نهایتاً هر وب‌سایت، در یکی از دو دسته اسپم و غیر اسپم، دسته‌بندی می‌شود. نتایج ارزیابی روش پیشنهادی روی مجموعه داده متشکل از حدود هزار وب‌سایت در محیط وب فارسی، حاکی از برتری عملکرد آن نسبت به روش مرجع مورد مقایسه، بر اساس شاخص ارزیابی F-Score و به میزان حدود ٪۲۰٫۲۵ می‌باشد.

کلمات کلیدی: وب‌سایت‌های اسپم، مدل Multinomial Naïve Bayes، پردازش زبان طبیعی.

۱ مقدمه

وب‌سایت‌های اسپم، عمدتاً صفحاتی با محتوای غیر مفید را شامل می‌باشند که قادر به تأمین نیازهای اطلاعاتی کاربران نیستند. از این رو، شناسایی این قبیل وب‌سایت‌ها، یکی از پردازش‌های پایه و کلیدی در فرآیند ایجاد سامانه‌های بازیابی اطلاعات وب و به خصوص جویشگرهای وب، بشمار می‌رود. بر این اساس، در این پژوهش، به مقوله شناسایی وب‌سایت‌های اسپم در محیط وب فارسی با بهره‌گیری از تکنیک‌های پردازش زبان طبیعی، پرداخته شده است.

۱.۱ چیستی اسپم

اسپم به هر گونه ارسال پیام به تعداد زیادی از کاربران در فضای آنلاین، بدون کسب اجازه یا توافق قبلی با آنها اطلاق می‌شود (Internet Society, 2014). اسپم می‌تواند به صورت ایمیل، پیامک، پیام در شبکه‌های اجتماعی و سایر وسایل ارتباطی صورت گیرد. برای مثال، ایمیل‌های تبلیغاتی ارسال شده به تعداد زیادی از افراد بدون موافقت قبلی آنها نوعی اسپم هستند. همچنین، پیامک‌های تبلیغاتی یا پیامک‌هایی که وعده‌ی جایزه رایگان را در بردارند نیز به عنوان اسپم شناخته می‌شوند. البته ممکن است یک محتوای اسپم، تبلیغاتی باشد یا نباشد (encyclopedia by Kaspersky, 2019).

به‌طور کلی پنج نوع مرسوم اسپم وجود دارد؛ از جمله نظر اسپم، اسپم trackback، حمله منفی سئو، حملات DDos با استفاده از spiderها و ربات‌ها و در نهایت ایمیل اسپم (Cojocariu, 2018). در این مقاله منظور از وب‌سایت اسپم، بک لینک‌هایی است که در حملات منفی سئو به کار گرفته می‌شوند. انواع مختلفی وب‌سایت اسپم وجود دارد که در ادامه شرح داده خواهند شد.

۱.۱.۱ انواع وب‌سایت اسپم

انواع وب‌سایت اسپم به سه دسته مبنی بر محتوا، مبنی بر لینک و مبنی بر صفحات پنهان تقسیم می‌شوند.

در وب‌سایت‌های اسپم مبنی بر محتوا، محتوای صفحه طوری تغییر داده شده تا وب‌سایت رتبه بالاتری را دریافت کند. بیش‌تر تکنیک‌های شناسایی اسپم مبنی بر محتوا از پردازش زبان طبیعی استفاده می‌کنند. پرکاربردترین تکنیک پردازش زبان طبیعی برای تشخیص وب‌سایت‌های اسپم شده با این روش، TF-IDF است (Danandeh Oskuie and Razavi, 2014). تکنیک دیگر، کوله کلمات[1] می‌باشد که در آن، وقوع کلمات در یک متن به صورت عددی توصیف می‌شود (Brownlee, 2017). بدنه، عنوان، URL و برچسب متا در یک وب‌سایت مبنی بر محتوا می‌توانند اسپم باشند. همچنین، ممکن است اسپم‌کننده از صفحات دیگر در وب برای صفحه اسپم خود، محتوا کپی کند و در قسمت‌های مختلف آن، اصطلاحات اسپم را به صورت رندوم قرار دهد. علاوه بر آن، در برخی صفحات اسپم تکرار یک یا چند کلمه خاص و استفاده بسیار از اصطلاحات نامرتبط، محتمل است (Danandeh Oskuie and Razavi, 2014).

در راستای به دست آوردن رتبه بالاتر در وب‌سایت‌های اسپم مبنی بر لینک، ساختار لینک دست‌کاری می‌شود. برای این کار، روش‌های دست‌کاری متفاوتی از جمله خرید لینک، استفاده از دامنه‌های منقضی‌شده و مزارع لینک[2] وجود دارد (Danandeh Oskuie and Razavi, 2014). وب‌سایت‌های اسپم مبنی بر صفحات پنهان، از طریق نشان دادن محتوای متفاوت به جویشگرهای وب، رتبه خود را بالاتر می‌برند. در این نوع، دو روش پنهان‌کاری محتوا برای جویشگرهای وب و تغییر مسیر هنگام بارگذاری صفحه به کار برده می‌شوند (Danandeh Oskuie and Razavi, 2014).

[1] Bag-of-Words
[2] Link Farms

۲.۱ اهمیت شناسایی وب‌سایت‌های اسپم

یکی از روش‌های قانونی افزایش رتبه سایت در نتایج جویشگرهای وب، بهبود کیفیت صفحات آن سایت می‌باشد. اما این روش بسیار زمان‌بر و دارای هزینه بالایی است. روش دیگر که غیرقانونی و غیر اخلاقی به شمار می‌رود، فریب دادن جویشگرهای وب با استفاده از بک لینک‌های اسپم است. این وب‌سایت‌ها با هدف تغییر رتبه سایت در نتایج جویشگرهای وب به وجود می‌آیند (Danandeh Oskuie and Razavi, 2014). تشخیص بک لینک‌های اسپم، یکی از چالش برانگیزترین مشکلات برای جویشگرهای وب و کاربران وب به حساب می‌آید.

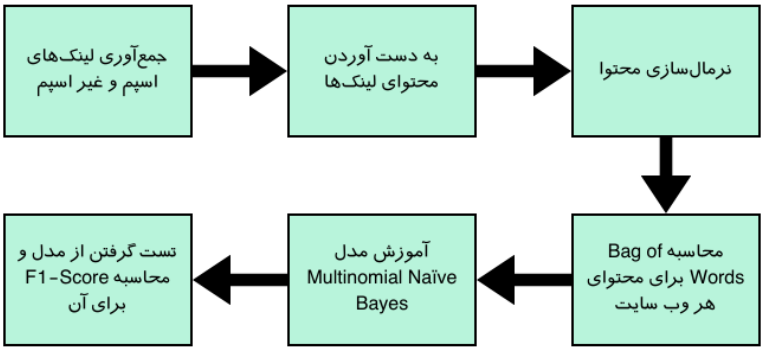
جویشگرهای وب، مانند گوگل، سعی می‌کنند سایت‌ها را بر اساس کیفیت و اعتبار بک لینک‌ها رتبه‌بندی کنند. اما وجود بک لینک‌های اسپم می‌تواند باعث کاهش رتبه وب‌سایت در نتایج جستجو شود (Ntoulas et al., 2006). از طرفی، این لینک‌ها می‌توانند اعتبار یک وب‌سایت را کاهش دهند. وجود بک لینک‌هایی از سایت‌های نامعتبر و مشکوک می‌تواند باعث شود که مخاطبان و جویشگرهای وب، اعتماد کمتری به آن وب‌سایت داشته باشند (Ntoulas et al., 2006). یکی دیگر از آثار مخرب این وب‌سایت‌های اسپم این است که ممکن است باعث کاهش ترافیک وب‌سایت شوند. به این صورت که این بک لینک ها به سایت هدف هدایت شده ولی بازدیدکنندگان به‌سرعت متوجه این موضوع گشته و از سایت خارج می‌شوند. این موضوع باعث کاهش ترافیک و معیارهای مهمی همچون میانگین زمان بازدید و نرخ بازگشت می‌شود.

در نتیجه، برای جلوگیری از خدشه‌دار شدن اعتماد کاربران، هدر رفتن منابع محاسباتی جویشگرهای وب (Najadat & Hmeidi, 2008) و همچنین جلوگیری از کاهش ترافیک وب‌سایت، شناسایی این بک لینک‌ها بسیار حائز اهمیت است و کمک بسیاری به بهبود نتایج جویشگرهای وب کرده و سبب افزایش رضایت کاربران می‌شود.

۳.۱ نوآوری‌ها

- برای ساخت مدل، یک مجموعه داده از لینک وب‌سایت‌های اسپم به همراه محتوای آن‌ها احتیاج بود که برای زبان فارسی، همچین مجموعه داده‌ای وجود نداشت. بنابراین، یک مجموعه داده جدید که شامل لینک وب‌سایت‌های اسپم و همچنین محتوای هر کدام از آنها است، در این مقاله معرفی می‌شود.
- در راستای شناسایی وب‌سایت‌های اسپم، یک مدل یادگیری ماشین که با استفاده از تکنیک‌های پردازش زبان طبیعی این وب‌سایت‌ها را تشخیص می‌دهد، با استفاده از مجموعه داده مذکور، آموزش دیده است.

بر این اساس، ابتدا در بخش دوم این مقاله، مروری بر پژوهش‌های مرتبط صورت خواهد گرفت و سپس در بخش سوم، روش پیشنهادی برای شناسایی وب‌سایت‌های اسپم توضیح داده می‌شود. ارزیابی روش پیشنهادی و نتایج بدست آمده نیز در بخش چهارم ذکر شده است و نهایتاً در بخش پنجم، نتیجه‌گیری این پژوهش، بیان شده است.



شکل ۱: روال به کار رفته در جمع‌آوری داده و آموزش مدل یادگیری ماشین برای شناسایی وب‌سایت‌های اسپم

۲ مروری بر کارهای دیگران

با توجه به اهمیت شناسایی وب‌سایت‌های اسپم، در سال‌های اخیر تلاش‌های بسیاری در این زمینه انجام شده است. در برخی از تلاش‌های انجام‌شده از هوش مصنوعی و یادگیری ماشین برای حل این مسئله استفاده گشته است. (Prieto, Alvarez & Cacheda, 2013) سیستمی به نام SAAD را ارائه دادند که از محتوای وب‌سایت برای تشخیص اسپم بودن یا نبودن آن استفاده می‌کند. (Karmipour, Noroozi & Alizadeh, 2022)، یک روش جدید بر اساس الگوریتم EM با طبقه‌بندی مبنی بر مدل Naïve Bayes برای حل مشکل برچسب‌گذاری پیشنهاد کرده‌اند. این روش، یک مدل طبقه‌بندی را از مجموعه کوچکی از داده‌های برچسب‌دار می‌آموزد تا مجموعه بزرگی از داده‌های بدون برچسب را برچسب‌گذاری کند. (Ntoulas et al., 2006) تعدادی روش مبنی بر محتوا برای شناسایی محتوای اسپم مطرح کرده‌اند. همچنین، (Becchetti et al., 2006) از ویژگی‌های مبنی بر لینک مانند TrustRank و PageRank جهت طبقه‌بندی در دو دسته اسپم و غیر اسپم استفاده کرده‌اند. (Agrawal, 2023) روش TF-IDF را برای ساختاردهی به داده‌ها به کار برده و مدل رگرسیون لجستیک[۳] را برای آموزش داده‌ها انتخاب کرده است.

در این مقاله نیز با به کار گرفتن مدل یادگیری ماشین Multinomial Naïve Bayes و تکنیک‌های پردازش زبان طبیعی، یک مدل برای شناسایی و طبقه‌بندی وب‌سایت‌ها در دو دسته اسپم و غیر اسپم با توجه به محتوای آنها ارائه شده است.

۳ روش پیشنهادی

در پیاده‌سازی مدل شناسایی‌کننده وب‌سایت‌های اسپم، از روال شکل ۱ استفاده شده است.

سه مرحله اول از این روال، مربوط به بخش جمع‌آوری داده بوده و سه مرحله دوم، در بخش مدل یادگیری ماشین، انجام شده‌اند.

[3] Logistic Regression

جدول ۱: آمار مجموعه داده

	اسپم	غیر اسپم	کل
تعداد لینک‌های به دست آمده	۷۳۸	۱۶۹۸	۲۴۳۶
تعداد لینک‌های در دسترس	۶۰۴	۱۳۵۱	۱۹۵۵
تعداد لینک‌ها با محتوای استخراج شده	۳۶۵	۷۵۳	۱۱۱۸
تعداد لینک‌ها پس از تمیز شدن دادگان	۳۶۵	۵۶۰	۹۲۵

۱.۳ جمع‌آوری داده

هدف از آموزش مدل، تشخیص وب‌سایت‌های اسپم و غیر اسپم در محیط وب فارسی است. برای زبان فارسی، چنین مجموعه داده‌ای وجود نداشت. بنابراین، در این مقاله یک مجموعه داده از وب‌سایت‌های اسپم و غیر اسپم فارسی معرفی می‌شود.

در فرآیند جمع‌آوری داده، احتیاج به دو گروه وب‌سایت وجود داشت. گروه اول، شامل وب‌سایت‌های اسپم بوده و گروه دوم از وب‌سایت‌های غیر اسپم تشکیل شده است.

برای گروه اول، ۷۳۸ بک لینک اسپم جمع‌آوری شد. از آن جایی که این لینک‌ها در گذر زمان از دسترس خارج می‌شوند، تمامی این لینک‌ها بررسی شده و در نهایت ۳۶۵ لینک اسپم در دسترس بوده و محتوای موجود در آن‌ها استخراج شده است.

در رابطه با گروه دوم، ابتدا چندین وب‌سایت مانند فارس نیوز، ایسنا، مجله دیجی‌کالا و ... در نظر گرفته شده و سپس تمامی لینک‌های موجود در آن‌ها استخراج گشته و لینک‌هایی که به صفحات دیگر مربوط بودند از میان تمامی لینک‌ها جدا شده‌اند. علت این کار این است که برخی از لینک‌ها، لینک وب‌سایت نبوده و به طور مثال، لینک مربوط به تصاویر بوده‌اند. در ادامه، محتوای لینک‌های جمع‌آوری شده نیز استخراج شد. در نهایت، تعداد ۵۶۰ وب‌سایت به همراه محتوای موجود در آن‌ها، به عنوان وب‌سایت غیر اسپم جمع‌آوری شد.

متون استخراج شده، احتیاج به تمیز شدن به صورت دستی داشتند؛ زیرا برخی از آنها شامل کاراکترهای نامفهوم بودند یا هنگام بارگذاری صفحه تغییر مسیر می‌دادند. تغییر مسیر باعث می‌شود هنگام استخراج متن از وب‌سایت، به جای متن اصلی صفحه، متن موجود در زمان تغییر مسیر استخراج شود. در این فرآیند، وب‌سایت‌هایی که متن استخراج شده از آنها شامل کاراکترهای نامفهوم یا متن غیر از متن اصلی بود، به‌صورت دستی از مجموعه داده حذف شده‌اند. در مجموع ۱۱۱۸ متن اسپم و غیر اسپم استخراج شده بود؛ که این مقدار پس از تمیز کردن دادگان به ۹۲۵ متن رسید.

تمامی محتواهای به دست آمده، با استفاده از کتابخانه Parsivar (Mohtaj et al., 2018)، نرمال‌سازی شده‌اند. علت این کار این است که تمام متون استخراج شده از یک استاندارد یکسان پیروی کنند و یکپارچه شوند. این کار بخشی از فرآیند پیش‌پردازش دادگان قبل از آموزش مدل می‌باشد.

در جدول ۱، آمار مربوط به مجموعه داده قابل مشاهده است.

۲.۳ مدل یادگیری ماشین

یادگیری نظارت‌شده یکی از انواع روش‌های یادگیری ماشین است که خروجی آن واضح یا برچسب‌زده‌شده می‌باشد. یکی از دسته‌های این روش، طبقه‌بندی[۴] نام دارد. طبقه‌بندی در مسائلی که خروجی آنها مقادیر محدودی دارد، قابل استفاده است. در این مقاله، با توجه به این‌که خروجی مدل اسپم بودن یا نبودن یک وب سایت است، تعداد خروجی‌ها محدود به ۲ بوده و مدل مورد نیاز آن در دسته الگوریتم‌های طبقه‌بندی قرار می‌گیرد.

مدل Naïve Bayes یک روش طبقه‌بندی بر اساس تئوری بیز میباشد. تئوری بیز احتمال رخ دادن یک پیشامد را هنگامی که پیشامد دیگر اتفاق افتاده باشد، به دست می‌آورد. مدل Bayes Na ve برمبنای احتمال شرطی است. در این مدل، فرض بر این است که ویژگی‌ها نسبت به یکدیگر مستقل‌اند (Gandhi, 2018).

به‌صورت کلی، سه نوع مدل Naïve Bayes وجود دارد (Saxena, 2021):

- Gaussian Naïve Bayes (GaussianNB): این مدل برای داده‌های پیوسته که از توزیع گاوسی (نرمال) پیروی می‌کنند، بهترین انتخاب است.
- Multinomial Naïve Bayes (MultinomialNB): این مدل هنگام برخورد با داده‌های گسسته، مانند شمارش فرکانس، مفید است. معمولا در موارد استفاده پردازش زبان طبیعی مانند طبقه‌بندی اسپم به کار برده می‌شود.
- Bernoulli Naïve Bayes (BernoulliNB): این مدل با متغیرهای بولی، یعنی متغیرهایی با دو مقدار، مانند True و False یا ۰ و ۱ استفاده می‌شود.

با توجه به موارد بررسی شده، نوع Multinomial Naïve Bayes برای استفاده در تشخیص وب‌سایت‌های اسپم، انتخاب مناسب‌تری است.

برای آموزش مدل، مجموعه داده به دو قسمت آموزش و تست تقسیم شده و سپس برای هر قسمت مقدار کوله کلمات، محاسبه شده است. پس از آن، مدل Multinomial Naïve Bayes با استفاده از مجموعه داده آموزشی، آموزش دیده است.

۴ ارزیابی

برای ارزیابی و مقایسه، احتیاج به مدلی مرتبط که روی زبان فارسی آموزش داده شده باشد، وجود داشت. از مدل‌های ذکر شده در بخش ۲، تنها مدل معرفی شده توسط (Agrawal, 2023) که روی زبان انگلیسی آموزش داده شده، در دسترس بود. در راستای انجام ارزیابی، این مدل بار دیگر روی زبان فارسی با استفاده از مجموعه داده معرفی شده در این مقاله، آموزش داده شد. مجموعه داده تست که شامل ۲۳۲ وب‌سایت

[4] Classification

جدول ۲: ارزیابی مدل با استفاده از مجموعه داده تست

سیستم ارزیابی	مدل (Agrawal, 2023)	مدل پیشنهادی این مقاله
(macro) F۱-score	۶۸۱۷.۰	**۹۶۲۴.۰**
(micro) F۱-score	۸۰۲۹.۰	**۹۶۵۵.۰**
(weighted) F۱-score	۷۶۷۲.۰	**۹۶۵۲.۰**

می‌شود، برای محاسبه F1-score برای هر دو مدل به کار رفته است. نتایج در جدول ۲ قابل بررسی هستند. بهترین نتیجه در هر سیستم، پررنگ شده است.

۵ نتیجه‌گیری

در این مقاله، ابتدا انواع اسپم بررسی شد و سپس یک مجموعه داده، شامل لینک وب‌سایت‌های اسپم و غیر اسپم به همراه برچسب مربوطه و محتوای هر لینک، جهت وب فارسی، معرفی گردید. در نهایت، با استفاده از مجموعه داده، مدل Multinomial Naïve Bayes برای طبقه‌بندی وب‌سایت‌ها به دو دسته اسپم و غیر اسپم، آموزش دیده است. در ارزیابی این مدل، مقدار ۰/۹۶۵۵ برای معیار F1-score ، به دست آمده است؛ که این نتیجه بسیار قابل قبول بوده و مدل می‌تواند در راستای شناسایی وب‌سایت‌های اسپم با استفاده از محتوای آن‌ها و در نتیجه آن، افزایش اعتماد کاربران و جلوگیری از گمراه شدن جویشگرهای وب، به کار رود.

کد منبع این مقاله و همچنین مجموعه داده معرفی‌شده، در گیت‌هاب[5] برای استفاده توسط دیگر محققان در کارهای آینده، منتشر شده است.

سپاس‌گزاری

با تشکر از آقایان محسن محمدی، شایان داودی و عماد نعمتی که در جمع‌آوری بک لینک‌های اسپم ما را یاری کردند.

مراجع

[1] Agrawal, I. (2023, March 29). Spam-Detection-Model. Github. https://github.com/ishitvaagrawal

[2] A. Ntoulas, M. Najork, M. Manasse and D. Fetterly, “Detecting Spam Web Pages through Content Analysis”, The Web Conference, 2006.

[3] Brownlee, J. (2019, August 7). A Gentle Introduction to the Bag-of-Words Model. Machine Learning Mastery. https://machinelearningmastery.com/gentle-introduction-bag-words-model/

[5] https://github.com/Saba-Heydaridoost/spam-detection

[4] Cojocariu, A. (n d). 5 Common Types of Spam & How You Can Protect Yourself Against Them. COGNITIVESEO. https://cognitiveseo.com/blog/18718/5-common-types-spam-can-protect/

[5] encyclopedia by Kaspersky. (n d). What is Spam?. encyclopedia by Kaspersky. https://encyclopedia.kaspersky.com/knowledge/what-is-spam/

[6] Gandhi, R. (2018, May 5). Naïve Bayes Classifier. Towards Data Science. https://towardsdatascience.com/naive-bayes-classifier-81d512f50a7c

[7] H. Najadat and I. Hmeidi, "Web Spam Detection Using Machine Learning in Specific Domain Features", Journal of Information Assurance and Security, vol. 3, pp. 220–229, 2008.

[8] Internet Society. (2014, July 27). What Is Spam. Internet Society. https://www.internetsociety.org/resources/doc/2014/what-is-spam/

[9] J. Karimpour, A. Noroozi, S. Alizadeh, "Web Spam Detection by Learning from Small Labeled Samples", International Journal of Computer Applications, vol. 50–No. 2, 2022.

[10] L. Becchetti, C. Castillo, D. Donato, S. Leonardi, R. Baeza-Yates, "Using Rank Propagation and Probabilistic Counting for Link-Based Spam Detection", 2006.

[11] M. Danandeh Oskuie and N. Rasavi, "A Survey of Web Spam Detection Techniques", International Journal of Computer Applications Technology and Research, vol. 3, pp. 180–185, 2014.

[12] Saxena, S. (2021, April 6). Inroduction to Naïve Bayes Algorithm. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2021/03/introduction-to-naive-bayes-algorithm/

[13] S. Mohtaj, B. Roshanfekr, A. Zafarian, H. Asghari, "Parsivar: A Language Processing Toolkit for Persian", LREC, pp. 1112–1118, 2018.

[14] V. Prieto, M. Alvarez, F. Cacheda, "SAAD, a content based Web Spam Analyzer and Detector", Journal of Systems and Software, vol. 86, pp. 2906–2918, 2013.

ابزارهای جنگ شناختی و راه‌کارهای مقابله با آن در حوزه سایبرنتیک

محمود اعتصامی فر[1]

[1]سطح سه تخصصی مدیریت اسلامی و کارشناس ارشد مدیریت رسانه
mimalef69@mail.ir

چکیده

یکی از تحولات دوران معاصر در عرصه نظام بین الملل، انقلاب اطلاعات و فناوری ارتباطات است. تحت تاثیر این فناوری‌ها، جنگ تغییر و تحولات گسترده‌ای به خود دیده که از آن جمله می‌توان به جنگ نرم و تحول مفاهیمی چون امنیت در فضای سایبرنتیک اشاره کرد. امروزه کشور ایران پس از چهار مرحله جنگ سرد، جنگ سخت، نیمه سخت و نرم، وارد پنجمین جنگ سلطه جویان با عنوان جنگ شناختی-ادراکی شده است. جنگ شناختی به معنای هدف قرار دادن قوه شناخت عموم مردم و نخبگان جامعه هدف با تغییر هنجارها، ارزش‌ها، باورها، نگرش‌ها و رفتارها، از طریق مدیریت ادراک و برداشت است. پژوهش حاضر کاربردی و آینده‌نگرانه است و روش تحقیق آن کیفی و از نوع توصیفی-تحلیلی است. نتایج پژوهش نشان می‌دهد که برای مقابله با جنگ شناختی در حوزه سایبرنتیک نیازمند به استفاده از راهبردهای ویژه در مورد اقوام و اقلیت‌ها، شفافیت، اطلاع‌رسانی دقیق و بصیرت افزایی به جامعه، ارتقای سواد رسانه‌ای مخاطبان با استفاده از تمام وسایل ارتباط جمعی، ایجاد راه‌های مشروع برای ارضاء نیازهای مردم، افزایش محصولات فرهنگی تأثیرگذار بر جامعه و جوانان می‌باشد.

کلمات کلیدی: فضای سایبرنتیک، جنگ شناختی، عصر اطلاعات، عملیات روانی.

۱ مقدمه

در شرایط ژئوپلیتیک فعلی که شناسه و ویژگی آن تضعیف چندجانبه گرایی، بازگشت به «تفکر بلوکی» است و این تصور که قدرت نظامی، برابر با درجه بالاتری از امنیت است، فناوری‌های جدید، لایه دیگری از پیچیدگی را در وضعیت چالش‌برانگیز ایجاد می‌کنند. در سال‌های اخیر، در زمینه‌های یادگیری ماشین، علوم اعصاب، روباتیک یا اقتصاد پیشرفت‌های سریعی انجام شده است. کشورهایی که این فناوری‌های نوین را در اختیار دارند، کاربرد رویکرد سنتی برای کنترل تسلیحات را نیز زیر سؤال می‌برند. این کشورها از این فناوری‌ها برای عملیات سایبری و تأثیر آن‌ها بر بازدارندگی هسته‌ای گرفته تا سیستم‌های تسلیحاتی خودمختار و جنگ شناختی استفاده می‌کنند (پوچوتو و همکارانش، ۲۰۱۸).

جنگ شناختی، به فعالیت‌هایی اشاره دارد که برای کنترل حالات و رفتارهای ذهنی دیگران طراحی شده است. اگرچه این ایده جدید نیست، اما جنگ شناختی با پیشرفت سریع فناوری اطلاعات و ارتباطات، نقش پررنگ‌تری را ایفا کرده است. روسیه نه‌تنها در انتخابات ریاست جمهوری ایالات متحده مداخله کرد، بلکه چین نیز در استرالیا و نیوزلند مداخله کرد (دیت و همکارانش، ۲۰۲۱). جنگ شناختی تهدیدی ویژه برای دموکراسی‌ها است. آزادی بیان توسط اطلاعات نادرست مورد سوءاستفاده و تضعیف قرار می‌گیرد. بدین سبب این یک مسئله نوظهور است که باید به طور جدی با آن برخورد شود (ویتکر و همکارانش، ۲۰۲۲).

درحالی‌که جنگ شناختی یک پدیده مهم است، هنوز توافقی در مورد خود مفهوم وجود ندارد. علاوه بر این، اغلب با مفاهیمی مانند جنگ اطلاعاتی و جنگ فضای سایبری درگیر است. به‌عنوان مثال، لیبیکی استدلال می‌کند که جنگ شناختی شامل هفت جزء (یعنی جنگ فرماندهی و کنترل، جنگ مبتنی بر اطلاعات، جنگ الکترونیک، جنگ روانی، جنگ هکرها، جنگ اطلاعات اقتصادی و جنگ سایبری) است که در آن دست‌کاری در دسته جنگ روانی قرار می‌گیرد (کالویلو و همکارانش، ۲۰۲۰). تاشف، پرسل و مک لافلین استدلال می‌کنند که بعد شناختی بالاترین جنبه فضای اطلاعاتی است. علاوه بر این، طبق مطالعه کانل و ووگلر درباره اطلاعات نادرست کرملین، جنگ سایبری شامل دست‌کاری شناخت به‌عنوان یک عنصر کلیدی است. لوئیس نیز بر تأثیر شناختی در حملات سایبری تأکید می‌کند. راجرز معتقد است که «تلفیق جنگ اطلاعات عملیاتی با جنگ شناختی یک خطای مقوله‌ای است که ابتدا باید به آن پرداخته شود». برنال، جنگ شناختی را از جنگ اطلاعاتی متمایز می‌کند. درحالی‌که دومی بر کنترل جریان اطلاعات تمرکز دارد، هدف اولی کنترل واکنش افراد و گروه‌ها به اطلاعات ارائه شده است (بورک و همکارانش، ۲۰۲۰).

۲ ادبیات پژوهش

دشمن در جنگ شناختی با هدف‌گیری ایده اصلی نظام یعنی اسلام ناب و ولایت مطلقه فقیه، ساختار و کارکرد نظام، تلاش دارد تا مردم را نسبت به آینده ناامید، نسبت به نهادهای رسمی بدبین و نسبت به سرنوشت عمومی جامعه بی‌تفاوت کند. چیستان و همکارانش (۱۳۹۵) در پژوهش خود به بررسی آسیب‌ها و ارائه راهکارهای جنگ شناختی و ادراکی در فضای سایبری پرداختند. یافته‌ها نشانگر آن است که حفظ و تقویت سرمایه‌هایی فرهنگی و اجتماعی و ارزش‌های انقلابی در برابر جنگ شناختی مستلزم ساماندهی شبکه‌ای ظرفیت‌های جبهه انقلاب برای جهاد تبیین و روایت امیدبخش، بازنمایی واقعیت‌های امیدبخش به شکل صادقانه و هنرمندانه برای مردم، اطلاع‌رسانی به‌موقع و حفظ ابتکار عمل در خبررسانی، نوآوری و تنوع‌بخشی به قالب‌های اطلاع‌رسانی، تقویت روح امید و باور به نتیجه‌بخش بودن استقامت و پایداری در ناامیدسازی دشمن می‌باشد. قیامی و همکارانش (۱۳۹۹) در پژوهش خود به معماری سازمانی جنگ شناختی در ارتش جمهوری اسلامی ایران پرداختند. یافته‌ها نشان داد که اهداف جنگ شناختی، تحول در نحوه نگرش انسان به محیط پیرامون است و زمینه را برای انجام کاری خاص که به گستردگی کل کشور و تمام افراد جامعه اعم از نیروهای نظامی، غیرنظامی و حتی زنان و کودکان آن جامعه می‌باشد، مهیا می‌سازد. عراقی و همکارانش (۱۴۰۱) در پژوهش خود به بررسی واکاوی اهداف جنگ شناختی دشمن و راهکارهای

تاب‌آوری مقابله با آن با تأکید بر آموزه‌های قرآن پرداختند. یافته‌ها نشان داد که جنگ شناختی با تحریف واقعیت‌ها، ایجاد یأس و ناامیدی، نادیده‌گرفتن دستاوردها و پیشرفت‌های عظیم انقلاب، خدشه‌دار کردن غیرت دینی و زیر سؤال بردن سنت‌های الهی پرداخته و راهکارهای تاب‌آوری مقابله با آن را شامل افزایش آگاهی و بصیرت، شناخت تکنیک‌های جنگ شناختی، ولایت‌پذیری، جهاد تبیین و ارتقای سواد رسانه‌ای با تأکید بر آموزه‌های قرآن می‌دانند. محبوب و شکوری (۱۴۰۱) در پژوهش خود به بررسی جنگ‌شناختی مدرن از شناخت در رزم تا عرصه جنگ‌شناختی پرداختند. یافته‌های پژوهشی آنها نشان داد که در مفهوم‌سازی جنگ‌شناختی، شش مغالطه منطقی رایج وجود دارد: ۱. تحدید جنگ‌شناختی به سطح روان‌شناختی؛ ۲. تحدید جنگ‌شناختی به عملیات شناختی؛ ۳. تحدید تأثیرشناختی به مداخله‌شناختی؛ ۴. تحدید جنگ‌شناختی به آسیب‌شناختی؛ ۵. تحدید جنگ‌شناختی به عملیات نظامی؛ ۶. تحدید جنگ‌شناختی به شناخت در جنگ. هر یک از مغالطه‌های فوق، نشان‌دهنده یک عنصر ماهیتی از جنگ‌شناختی است که شبکه مفهومی آن را نمایان می‌سازد: علوم و فناوری‌های جنگ‌شناختی، جنگ‌شناختی مبتنی بر تئوری‌شناختی، اثربخشی جنگ‌شناختی، ابعاد جنگ‌شناختی، دامنه جنگ‌شناختی و عرصه جنگ‌شناختی. در نتیجه باید سعی در شناخت و رسیدن به فهم مشترکی از جنگ شناختی نموده و در مرحله بعد پاسخ متناسب را به دشمن بدهد. در وهله اول نیاز به جلسات هم‌اندیشی، بیان نظرات و نظریات گوناگون حول این مفاهیم و رویدادهای در پی آن وجود دارد. به نظر در چنین صحنه جنگی که جنگ‌های مختلف سخت و نرم در ابعاد گوناگون فنی، فرهنگی، سیاسی و ... مطرح‌اند، پاسخی صرفاً فنی یا امنیتی نمی‌تواند اثرگذار باشد؛ حتی ممکن است با چنین تصمیمی، دیگر قوای ما در دیگر ابعاد این جنگ نیز آسیب‌دیده و در مجموع باعث تضعیف نظام در دیگر ابعاد نزاع بین جبهه حق و باطل گردد. رنسانس علوم و فناوری‌های شناختی، برتری آینده را برتری‌شناختی می‌داند و آن را در گرو قدرت‌نمایی در عرصه جنگ‌شناختی ترسیم می‌کند؛ به همین دلیل، ضروری به نظر می‌رسد که با ایجاد پژوهشکده‌های علوم و فناوری‌های جنگ‌شناختی، مراکز دفاع‌شناختی، قرارگاه و فرماندهی رزم‌شناختی و تربیت افسران جنگ‌شناختی، زمینه‌هایی فراهم آورد تا بتوان به سیاست‌گذاری، خط‌مشی‌گذاری، برنامه‌ریزی و اقدام‌های عملی برای انجام عملیاتهای آفندی و پدافندی در عرصه جنگ‌شناختی پرداخت.

۳ مبانی نظری

در بخش مبانی نظری به بررسی تعریفات و اصلاحات مهم در این زمینه از جمله شناخت و دانش شناختی، فضای سایبرنتیک، جنگ‌شناختی، نظریه‌های جنگ‌شناختی، سلاح‌ها و اهداف جنگ‌شناختی و تاکتیک‌های جنگ شناختی پرداخته می‌شود.

شناخت و دانش شناختی: شناخت اصطلاحی است که به فرایندهای ذهنی مربوط به کسب دانش و درک مربوط می‌شود. فرایندهای شناختی شامل تفکر، دانستن، به‌خاطر سپردن، قضاوت و حل مسئله است. این فرایندها عملکردهای سطح بالایی از مغز بوده، و شامل زبان، تخیل، ادراک و برنامه‌ریزی است. فرایندهای

شناختی شامل توجه، زبان، یادگیری، حافظه، ادراک و اندیشه است. فرایندهای شناختی تحت‌تأثیر طیف وسیعی از عوامل از جمله ژنتیک و تجربیات قرار می‌گیرند (گرین و همکارانش، ۲۰۰۸). دانش شناختی پروژه‌ای در حال پیشرفت است که از دهه‌ی ۱۹۵۰ میلادی آغاز شده و نام «علوم شناختی» در سال ۱۹۷۳ به آن داده شده است. دانش شناختی، مطالعه‌ی علمی ذهن است. در این تعریف منظور از ذهن مجموع هر آن چه که نمودهای هوشمندی و آگاهی هستند مانند تفکر، ادراک، حافظه، احساس، استدلال و نیز تمام روندهای ناآگاهانه شناختی است. گاهی دانش شناختی را به‌صورت مطالعه‌ی علمی شناخت نیز تعریف می‌کنند و شناخت را مجموع حالت‌ها و فرآیندهای روانی مانند تفکر، استدلال، درک و تولید زبان، دریافت حواس پنجگانه، آموزش، آگاهی، احساسات و... در نظر می‌گیرند. به طور کلی پرسش‌هایی مانند این که ذهن چگونه کار می‌کند یا مغز چگونه هوشمندی را ایجاد می‌کند، از جمله پرسش‌هایی هستند که در این شاخه‌ی علمی بررسی می‌شوند. هدف از این علم این است که اولا قابلیت‌های شناختی که در موجودات زنده وجود دارد به شکل علمی تعریف و تدوین شود و بعد مکانیسم‌هایی که در مغز باعث به وجود آمدن چنین قابلیت‌هایی بوده‌اند، شناسایی شوند (وولفورث، زوبوک، ۲۰۱۷).

فضای سایبرنتیک: سایبرنتیک ازجمله علومی است که در قرن بیستم پدید آمد و با رشد سریع خود توانست به علوم دیگر راه یابد. موضوع اصلی سایبرنتیک بررسی ماهیت کنترل در انسان، حیوان و ماشین است و لذا با زیست‌شناسی، روان‌شناسی، مکانیک، مهندسی، مدیریت و بسیاری علوم دیگر همبستگی دارد. با دردست‌داشتن طیفی کامل از یافته‌های سایبرنتیک، همیشه امکان تحلیل یک وضعیت از دیدگاه پدیده‌های تنظیم‌کننده آن وجود دارد. بر اساس دیدگاه متخصصان سایبرنتیک، هدف یک سیستم همان کاری است که انجام می‌دهد. این یک قضیه ابتدایی است و ازآنجایی‌که حقیقتی آشکار است؛ لذا نقطه آغاز بهتری برای فهم ویژگی‌هایی معمول نیت‌های خیر، پیش‌داوری نسبت به توقعات، قضاوت‌های اخلاقی یا غفلت محض از عواقب است (روبینسون و همکارانش، ۲۰۱۵).

جنگ شناختی: جنگ شناختی رویکردهای شناخته شده و بدیع در اطلاعات، سایبری و جنگ روانی را نه‌تنها با تلاش برای تغییر طرز تفکر مردم، بلکه همچنین نحوه واکنش آن‌ها به اطلاعات را به سطح جدیدی می‌برد. علاوه بر این، روش‌های جنگ شناختی خطوط بین اهداف غیرنظامی و نظامی را محو می‌کند و احتمالاً اعمال نیرو را از حوزه فیزیکی به حوزه مجازی تغییر می‌دهد (هانک و همکارانش، ۲۰۲۲). در یک تعریف، جنگ شناختی به معنای هدف قراردادن قوه شناخت مردم و نخبگان جامعه هدف با تغییر هنجارها، ارزش‌ها، باورها، نگرش‌ها و رفتارها، از طریق مدیریت ادراک و برداشت است (روبینسون و همکارانش، ۲۰۱۵). هدف از جنگ شناختی ایجاد تغییر در سیاست جامعه هدف، از طریق فرایند شناختی، به نفع دولت مهاجم (بازیگر غیردولتی) است. اگرچه جنگ سایبری، جنگ اطلاعاتی، جنگ شناختی، و جنگ ترکیبی حاوی عنصر عملیات نفوذ هستند و ممکن است بر شناخت انسان تأثیر بگذارند، اما فقط جنگ شناختی به طور خاص به کنترل مغز با گنجاندن علوم اعصاب تسلیحاتی در اعمال مختلف اختصاص دارد (وایتی و همکارانش، ۲۰۲۱).

نظریه‌های جنگ شناختی: جنگ شناختی به‌عنوان اصطلاحی نوین در علوم استراتژیک، محصول نگاهی جامع به جنگ‌هایی است که با عنوان جنگ اطلاعاتی، جنگ سایبری، جنگ الکترونیکی، جنگ نظارت و شناسایی، جنگ روانی، شناسایی می‌گردند. در ادامه نظریه‌های مهم در رابطه با جنگ شناختی مطرح می‌گردد. در نظریه جنگ عقیده شناخت‌ها و بینش‌ها با قطع‌نظر از آکادمیک یا دینی و عرفی بودن، زمانی ساختارهای اجتماعی را نظام می‌بخشد که به عقیده و الگوی باثبات بینشی جامعه و فرد تبدیل شده باشد. بر اساس کاربستی از نظریه قدرت و دانش میشل فوکو، جنگ شناختی همان جنگ عقیده است؛ حاکم مستبدی که از حکمت بهره‌ای ندارد دشمنان خود را با سلاح گرم و سخت شکست می‌دهد و به بند انقیاد می‌کشد (گری، کریس هیبلز، ۱۳۸۱). نظریه جنگ اتاق فکر، به معنای جنگی که در فضایی اتاق فکر برنامه‌ریزی و راهبری می‌گردد. قالب اصلی فضای اندیشکده‌های بر اساس طوفان فکری کنشگران آن سامان می‌یابد. تصمیم‌سازی‌های نظامی در دهه‌های اخیر در اتاق فکر شکل می‌گیرد، کشف پروتکل حاکم بر اتاق‌های فکر که مبتنی بر نوعی بارش نامنظم فکری در عین نظام‌مندی است، امری پیچیده و درخور توجه است. این بارش نامنظم از گزینش ترکیب شرکت‌کنندگان در اتاق فکر با ویژگی‌های شخصی و شخصیتی متفاوت شروع‌شده و تا ایده‌ها و جمع‌بندی و تصمیم‌سازی راهبردی و تاکتیکی ادامه می‌یابد (لیواس و همکارانش، ۲۰۱۸).

در نظریه ممتیک قواعد ناظر بر ژن‌ها در میم‌ها جاری هستند. ماندگاری، مانایی و امانت در نسخه‌برداری، ویژگی مشترک ژن‌ها در انسان و میم‌ها در اجتماع جانوران است. اساس ممتیک بر تقلید انسان‌ها در عرصه فرهنگ استوار است. با فهم دقیق میم‌ها می‌توان یک جامعه و نهادهای اجتماعی آن را فهم کرد و با خلق میم‌های جدید یا تغییر و مداخله ممتیک می‌توان جامعه و نهادها و روابط اجتماعی و ازجمله جنگ را مدیریت کرد (هامز، ۲۰۰۲). در نظریه جنگ، جنگ شناختی به سه دسته خط مقدم فرمان، عوامل استرس‌زای دشمن و فریب طبقه‌بندی می‌شوند. خط پایه فرمان، ویژگی‌های تصمیم‌گیری موجود دشمن را نشان می‌دهد. این شامل انتظارات، ادراکات، ترتیبات فرماندهی، رویه‌های تصمیم‌گیری، تجربه، آموزش، سنت، فرهنگ و هر عامل مهم دیگری است که تصمیم‌گیری او را تشکیل می‌دهد (کالویلو و همکارانش، ۲۰۲۰). عوامل استرس‌زای فیزیکی اقداماتی هستند که با تحت‌فشار قراردادن توانایی‌ها و منابع زمانی دشمن، تصمیم‌گیری را پیچیده و تضعیف می‌کنند (لیواس و همکارانش، ۲۰۱۸). زبان نقش اصلی در معنادهی به واقعیت‌ها و ایجاد شناخت دارد؛ بنابراین جنگ‌شناختی را می‌توان جنگ در عرصه زبان و معنا تفسیر کرد که طی آن روابط سازمان و سامان‌یافته انسان‌ها مضمحل می‌گردد (وولفورث، زوبوک، ۲۰۱۷). در دانش رتوریک، انواع اقناع و مغالطه تعریف و مراحل و شیوه‌های عملیاتی کردن آن تبیین می‌شود. ابزار و قواعد رتوریک در شکل سنتی آن عموماً ناظر بر مقولات گفتاری و نوشتاری و شنیداری بوده و مرتبط با دانش منطق است. برخی رویکردهای دانش منطق که قابلیت بهره‌برداری در جنگ شناختی دارند (گری، کریس هیبلز، ۱۳۸۱).

عملیات جنگ شناختی: عملیات‌های جنگ شناختی چین بر علیه تایوان را می‌توان به چهار دسته اصلی ۱- ارعاب نظامی، ۲- نفوذ از طریق تبادل دوجانبه، ۳- مداخله مذهبی، و ۴- اطلاعات نادرست محتوا در اینترنت دسته‌بندی کرد. تهدیدات نظامی ممکن است مستقیم‌ترین راه برای تأثیرگذاری روانی روی مردم تایوان در مورد موضوع اتحاد باشد. چین سابقه طولانی در تهدید تایوان به‌زور در صورت تعقیب استقلال

تایوان دارد (دیموند و همکارانش،۲۰۱۹). استراتژی آن ساده است: شهروندان تایوانی را با مزایای اقتصادی و اجتماعی فرهنگی فریب می‌دهد تا نیازها و وابستگی را برای اعمال کنترل بیشتر ایجاد کنند. ثالثاً دین، کانال دیگری از عملیات شناختی است. مازوئیسم که منشأ آن در چین است (ارنکس و همکارانش، ۲۰۲۰). در ماه‌های قبل از انتخابات ریاست‌جمهوری آمریکا در سال ۲۰۱۶، دولت ایالات متحده به طور فزاینده‌ای از قصد دولت روسیه برای مداخله در روند انتخابات ایالات متحده آگاه شد. در ماه ژوئیه، جامعه اطلاعاتی ایالات متحده به کاخ سفید گزارش داد که به قضاوت خود در مورد دخالت روسیه در هک علیه کمیته ملی دموکرات اعتماد زیادی دارد (هانسن و همکارانش، ۲۰۲۱).

۴ روش تحقیق

پژوهش حاضر کاربردی و آینده‌نگرانه است و روش تحقیق آن کیفی و از نوع توصیفی-تحلیلی است. برای جمع‌آوری اطلاعات، روش اسنادی و مبتنی بر تفسیر متن مورداستفاده قرار گرفته است. روش‌های اسنادی در زمرهٔ روش‌ها یا سنجه‌های غیر مزاحم و غیر واکنشی به شمار می‌آید.

۵ نتایج و یافته‌ها

در ادامه در این قسمت به بررسی نتایج و یافته‌های پژوهش در این زمینه پرداخته می‌شود.

سلاح‌ها و اهداف جنگ شناختی: یکی از انواع عملیات روانی ایجاد اخلال در قوه شناخت مردم با استفاده از خطاهای شناختی مغز انسان است. در این نوع عملیات روانی که به آن جنگ شناختی نیز گفته می‌شود، دشمن به دنبال هدف قراردادن قوه شناخت عموم مردم و نخبگان جامعه هدف با تغییر هنجارها، ارزش‌ها، باورها، نگرش‌ها و رفتارها از طریق مدیریت ادراک و برداشت است. در جنگ شناختی، دشمن از چند سلاح اعتماد زدایی، ناامیدسازی جامعه، ناکارآمد نشان‌دادن حاکمیت، از بین بردن مشروعیت‌های جامعه و زیر سؤال بردن اعتبار نظام و حاکمیت در رأس یک کشور استفاده می‌کند. جنگ شناختی، سبب می‌شود پیش از آن که جنگ اقتصادی ساختار و کارکردهای اقتصاد ملی را به چالش بکشاند، جامعه را در مسیر هموارسازی سناریوی دشمن و آسیب‌رسانی درون‌زا قرار دهد (دیاموند و همکارانش، ۲۰۱۹). نتیجه اجرای راهبردهای دشمن در این جنگ آن است که درحالی‌که هنوز تحریم‌های آمریکا بازنگشته بود که بازار داخلی در حوزه‌های مختلف دچار نوسان و نابسامانی شده و یا آنکه کالاهایی با منشأ کاملاً داخلی دچار کمبود یا افزایش افسارگسیخته قیمت شدند (ویتکر و همکارانش، ۲۰۲۲).

تاکتیک‌های جنگ شناختی: یکی از تاکتیک‌های جنگ شناختی، برچسب‌زدن است. بر اساس این تاکتیک، رسانه‌ها، واژه‌های مختلف را به صفات مثبت و منفی تبدیل کرده و آن‌ها را به آحاد یا نهادهای مختلف نسبت می‌دهند. یکی دیگر از تاکتیک‌های جنگ شناختی، شایع پراکنی در جامعه است. مطالب کلی شایعه باید حول محورهای اساسی و مهمی باشد که مخاطب نسبت به آن حساسیت بالایی دارد. یکی دیگر از

تاکتیک‌ها دروغ‌گویی است. این تاکتیک قدیمی که هنوز هم مورداستفاده فراوان است، عمدتاً برای مرعوب کردن و فریب ذهن حریف مورداستفاده قرار می‌گیرد. از تکنیک‌های معروف جنگ شناختی، ترور شخصیت است (باسکو و همکارانش، ۲۰۲۰). در جنگ شناختی برخلاف جنگ سخت، ترور فیزیکی جای خود را به ترور شخصیت داده است. در زمانی که نمی‌توان و یا نباید فردی مورد ترور فیزیکی قرار گیرد با استفاده از نظام رسانه‌ای و انواع تاکتیک‌ها از جمله بزرگ‌نمایی، انسانیت‌زدایی و اهریمن‌سازی، پاره حقیقت‌گویی وی را ترور شخصیت می‌کنند و از این طریق باعث افزایش نفرت عمومی و کاهش محبوبیت وی می‌شوند. یکی دیگر از تکنیک‌ها، استفاده از رعب و ترس بین مردم است. در این تاکتیک از حربه تهدید و ایجاد رعب و وحشت میان نیروهای دشمن، به‌منظور تضعیف روحیه و سست کردن اراده آنها استفاده می‌شود (ارنکس و همکارانش، ۲۰۲۰).

مکانیزم‌هایی برای مقابله با جنگ‌های شناختی در حوزه سایبرنتیک از نگاه محققان: اقلیت‌های جامعه اغلب به سبب داشتن احساس نابرابری، مستعد مخالفت‌ورزی علیه نظام حاکم هستند و دشمنان فرامنطقه‌ای یکی از میدان‌های فعالیت خود را در کشورهایی که دارای تنوع قومیت‌هاست، قرار می‌دهند. اما زمانی که نظام مستقر با انجام راهبردهای مناسب در مناطق محروم و دور از مرکز و اختصاص بودجه‌های لازم در قالب طرح‌های توسعه همه‌جانبه خصوصاً طرح‌های اشتغال‌زا و به‌کارگیری مدیریت‌های توانمند در این مناطق و با روحیه جهادی و بسیجی مشغول خدمت به مردم شدند، می‌توانند آن احساس را کم کنند یا از میان بردارند. در مقابله با جنگ شناختی نبایستی منفعلانه عملکرد. عاملان تهدید جنگ شناختی از انواع تبلیغات، فنون مجاب سازی روش‌های نفوذ اجتماعی و عملیات روانی به منزله روش‌های تغییر نگرش‌ها، باورها و ارزش‌های جامعه هدف استفاده می‌کنند. انجام تبلیغات هوشمندانه، سریع باقدرت منطق و اندیشه و احاطه ذهنی بر مخاطبان جنگ شناختی می‌تواند یکی از روش‌های مقابله باشد (گرین و همکارانش، ۲۰۰۸). مهم‌ترین راه مقابله با عملیات روانی و جنگ شناختی-ادراکی عبارت است از: شفافیت، اطلاع‌رسانی دقیق و بصیرت‌افزایی به جامعه، هرچه فضای جامعه، شفاف‌تر و مردم آگاه‌تر شوند، فرصت برای دروغ‌گویی و جولان دشمن در افکار عمومی و مدیریت آن کاسته می‌شود. یکی دیگر از راه‌های مقابله، ارتقای سواد رسانه‌ای مخاطبان با استفاده از تمام وسایل ارتباط‌جمعی و عبور از شعارزدگی و درک ضرورت فراگیری سواد رسانه‌ای می‌باشد. همچنین نخبگان جامعه اعم از مسئولان و گروه‌های مرجع اجتماعی با هر وسیله و گرایش، تهاجم شناختی دشمن و مخاطرات ناشی از هرگونه رفتار هیجانی مبتنی بر منفعت فردی را برای جامعه تبیین کرده و مراقب باشند که خود نیز در این پازل دشمن بازی نکنند (زو و همکارانش، ۲۰۱۸).

مکانیزم‌هایی برای مقابله با جنگ‌های شناختی در حوزه سایبرنتیک از نگاه مقام معظم رهبری: رهبر انقلاب برای مقابله با جنگ‌های شناختی، بحث تبیین را مطرح کردند. تبیین در لغت‌نامه دهخدا به معنای هویدا شدن؛ پیداشدن و آشکارشدن و نیز هویدا کردن، پیداکردن، بیان‌کردن و آشکارا ساختن است. در فلسفه علم تبیین علمی به سه معنا آمده است از نظر برخی تبیین علمی یک پدیده عبارت است از بیان علت و سببیت آن پدیده و رویداد، گروهی دیگر به دلیل و چرایی پدیده‌ها می‌پردازند. یعنی بیان و توضیح

دلیل و هدف از یک امر که عموماً به پدیده‌های انسانی معطوف است؛ یعنی تبیین آن پدیده انسانی، و برخی دیگر به بیان معنا و مفهوم یک پدیده اطلاق تبیین می‌کنند. گروه نخست معتقد است، وقتی موفق به توضیح علمی پدیده‌ای می‌شویم که علت عینی و بیرونی تحقق آن را مشخص کنیم. گروه دوم بر این نظر است که توضیح علمی امر اجتماعی عبارت است از تعیین دلیل معقولی که فاعلان در پی آن بوده‌اند. گروه سوم به دنبال فهم چارچوب‌های معنایی و فرهنگی عمل انسان‌ها هستند و تبیین از نظر آن‌ها چیزی نیست جز کشف معنای افعال جمعی در پرتو فرهنگ خاص فاعلان.

رهبر انقلاب می‌فرمایند ما باید بحث تبیین را نسبت به حقایق انجام بدهیم و خیلی از حقایق باید تبیین شوند. این جمله به معنای این است که هنوز بسیاری از حقایق هستند که تبیین نشده‌اند و یا به‌خوبی این کار انجام نشده است. در مقابل تبیین، حرکت گمراه‌کننده و تحریف‌کننده دشمن وجود دارد که از جوانب مختلف و از صدها طرف به‌سوی جمهوری اسلامی ایران سرازیر شده و می‌خواهد افکار مردم را مورد اثرپذیری سم‌آلود قرار دهد. ازاین‌جهت، یکی از موضوعات خوبی که رهبر انقلاب ذکر می‌کنند این است که افکار عمومی را به سمت راه درست و منطقی و راهی که در آن عقلانیت انقلابی هست، هدایت کنیم. جهاد تبیین، خنثی‌کننده توطئه دشمن است. با جهاد تبیین می‌توان حرکات صحیح را منتشر کرد و به سؤالات پاسخ داد. همچنین با جهاد تبیین می‌توان ابهام‌آفرینی‌های موجود در فضای سایبری را به‌نوعی مورد خدشه قرارداد و با آن مقابله کرد. جهاد تبیین، مقوله و شاکله مهم از قدرت نرم است که البته لوازم بسیار جدی دارد. مهم‌ترین لوازم قدرت جنگ‌های شناختی در قالب جهاد تبیین، سخن متین، عقلانیت کامل، بصیرت و استدلال است؛ اما آنچه باید به آن توجه کرد و رهبر معظم انقلاب آن را موردتوجه قرار دادند این است که باید به معنای واقعی کلمه جهاد را در «جهاد تبیین» به کاربرد. در جهاد تبیین، اخلاق‌مداری از جمله موضوعات مهمی است که رهبر انقلاب بر آن تأکید دارند. در واقع، اخلاق‌مداری دعوت به رسیدگی به عمل و رفتار، دعوت بر اساس انصاف، صداقت و به‌نوعی دل‌سوزی و دعوت بر اساس پرهیز از حرص و امل و سخن‌چینی است. باید از شیوه‌های اخلاقی در جهاد تبیین پیروی کرد و از روش‌های دشنام، تهمت، فریب و دروغ عده‌ای در فضای مجازی، مطبوعات، رسانه‌ها و مقالات که افکار عمومی را ملتهب می‌کنند، اجتناب کرد. رهبر انقلاب می‌فرمایند: جهاد تبیین باید مبتنی بر سخن متین، مبتنی بر زینت عاطفه و عواطف انسانی و مبتنی بر نگاه و رویکرد اخلاقی باشد. نکته بسیار مهمی که ایشان ذکر می‌کنند این است که همه ما در فضای جهاد تبیین سهم و مسئولیتی داریم و همه باید در این مسیر و میدان جدی حرکت کنیم. از این بابت، جهاد تبیین در قالب جنگ‌های شناختی می‌تواند موضوع اساسی و جدی مطرح شود، به شرطی که از لوازم و منابع آن استفاده جدی شود. بصیرت در جهاد تبیین نیز بسیار مهم است. بصیرت، یعنی ظلم‌ستیزی، دشمن‌شناسی، هوشیاری و جریان‌شناسی؛ لذا باید تصمیم‌گیری‌ها بر اساس خِرد باشد. در جهاد تبیین تصمیم‌گیری‌های اقناعی موردتوجه قرار می‌گیرد. تجزیه و تحلیل محیطی هم بسیار مهم است. فرابخشی و منطقه‌ای بودن و سرعت در تصمیم‌گیری از موضوعات بسیار مهمی هستند که در جهاد تبیین می‌توان اشاره کرد. یکی از موضوعات بسیار مهم دیگری که در بحث جهاد تبیین می‌توان به آن توجه کرد ارتباطات مؤثر با مردم است. در جهاد تبیین باید در درون مردم بود؛ یعنی مشارکت و مشاهده میدانی داشت، از بدزبانی به مردم و مردم‌گریزی پرهیز کرد. باید روحیه خدمتگزاری و کار جهادی را در جهاد تبیین موردتوجه ویژه قرارداد. از نکات مهم دیگر در جهاد تبیین، انقلابی‌گری است.

انقلابی‌گری، یعنی اتکا بر عزم ملی برای محرومیت‌زدایی، توجه به ریزش‌ها و رویش‌های انقلاب، توجه به اصل بسیار مهم اعتقاد به نظام و وفاداری به ارزش‌های انقلابی، اعتقاد به استقلال و لزوم خودکفایی و ولایت محوری و آرمان‌خواهی که می‌تواند در فضای جهاد خودش را نشان دهد. از این جهت، می‌توان انقلابی‌گری را به‌عنوان یکی از موضوعات جدی در فرایند خرد، تصمیم‌گیری انقلابی و اخلاقی و عمل‌کردن در جهاد تبیین یک شاکله اصلی مطرح کرد.

مخاطب ویژه جهاد تبیین بر اساس فرمایشات مقام معظم رهبری جوانان هستند؛ زیرا آنها نسبت به گذشته آگاهی، اطلاعات و دانش لازم را نداشته و قرار است جوانان در آینده برای پاسداری از انقلاب اسلامی شمشیر بزنند، بنابراین لازم است اقدامات سایبری و رسانه‌ای و تبیینی را برای بیانیه گام دوم انجام داد، محتوای بیانیه گام دوم به طور عمده گزاره‌ای خبری است که به نظر می‌رسد بسته‌ای تبیینی از گذشته، حال و آینده انقلاب اسلامی در آن ترسیم شده است. در اوج تهاجم‌ها و فشارهای اقتصادی و رسانه‌ای سال ۹۷ و ادعاهایی که معتقد بودند جمهوری اسلامی ۴۰ سالگی خود را نخواهد دید و در فضای شدید سیاه‌نمایی، فضای اقتصادی در آن سال و عملیات روانی پیرامون آن قرار داشتیم که سهم فشارهای اقتصادی اگر کمتر از فشارهای روانی و اجتماعی در بازه زمانی سال‌های ۹۷ و ۹۸ نباشد، قطعاً هم وزن آن خواهد بود که بر افکار عمومی در کشور وارد شد و هم زمانی آن با ۴۰ سالگی انقلاب اسلامی بود. مقام معظم رهبری در بیانیه گام دوم در مورد جنگ شناختی اشاره می‌کند، اینکه تمام اتفاقات نسبت به گذشته، حال، آینده، تحریف‌ها و سیاه‌نمایی رخ می‌دهد تا مردم راه‌حل مشکلات و رشد آن را در بوسه بر پنجه گرگ ببینید؛ آحاد مردم به‌ویژه فعالان رسانه‌ای مخاطب فرمایشات مقام معظم رهبری هستند و سواد و تاکتیک‌های رسانه‌ای باید ارتقا یابد تا بتوان با بینش و دانش کافی وارد جنگ شد و از پس این کارزار برآمد و دچار آسیب نشد. جهاد تبیین که تمام اقشار مردم در جایگاه‌های خود مخاطب آن هستند، مقدمه‌ای دارد و بیانیه گام دوم انقلاب اسلامی، راهبردها و سواد رسانه‌ای به‌عنوان آموزش‌های پیش از اعزام است که افراد باید آن را فراگرفته و وارد جهاد تبیین شوند. وظیفه خود رسانه و فعالان رسانه‌ای برای مشارکت در جهاد تبیین و تعریف عرصه‌هایی که آحاد جامعه می‌تواند به این موضوع ورود کند، دو بخش مهم است که باید به آن پرداخته شود و به‌عنوان رسانه و فعال رسانه‌ای آموزش آحاد مردم برای حضور در عرصه جهاد تبیین و نقش‌آفرینی مؤثر در فضای سایبرنتیک را باید در برنامه‌ها داشته باشیم، همچنین گلوگاه‌هایی از جمله مقابله با دشمن، جنگ علیه افکار عمومی و ادراک مردم که نیاز به تبیین دارد نیز باید بر اساس گام دوم مشخص شود و هر رسانه متناسب با کارکرد خود به این موضوع ورود کند.

۶ نتیجه‌گیری و کارهای آینده

هدف اصلی و اولیهٔ جنگ شناختی، تسلط بر تفکر و رفتار جمعیت هدف است. برای رسیدن به این مهم، باید اطلاعاتی را که جمعیت هدف دریافت می‌کند، ماهرانه کنترل و دست‌کاری شود. در وجود انسان، مغز نقش داده‌پردازی را برعهده دارد پس باید گفت ازآنجایی‌که مغز نه دیوار آتش دارد و نه سیستم محافظت از ویروس تا آن را در مقابل شیوه‌های فریب یا امواج الکترومغناطیس مصون بدارد، هدف بسیار ارزشمندی

محسوب می‌شود. در نتیجه فکر یک سرباز در میدان جنگ یا یک رهبر استراتژیک به‌صورت بالقوه بی‌دفاع‌ترین و باصرفه‌ترین هدف در عملیات روانی برای ارسال اطلاعات پردازش شده، به‌حساب می‌آید. آگاهی از روش‌ها و شیوه‌های عملیات روانی به افزایش آمادگی افراد منجر خواهد شد، به‌نحوی‌که افراد بتوانند با کسب دانش و مهارت‌های لازم در صحنه عملیات روانی مقهور عملیات روانی دشمن نشده، ابتکار عمل را به دست بگیرند و دشمن را وادار به عکس‌العمل نمایند. جهاد تبیین صرف بیان و گفتگو بین دو طرف جنگ و یا نیروهای خودی نیست. باید بر اساس جنگ ترکیبی که وجود دارد پاسخ متناسب را داد. به‌عنوان مثال در غائله پاییز ۱۴۰۱، دشمن با استفاده از فضای سایبرنتیک سعی در تغییر ذهنیت کاربران، دامن زدن به اغتشاشات و به‌تبع تخریب اموال عمومی در سطح جامعه داشت. حال در پاسخ به این برنامه که فقط یکی از حربه‌های دشمن در کنار دیپلماسی اقتصادی غرب حول مرزهای ایران، جنگ اوکراین و تأثیر آن در نظم نوین جهانی، حرکت گروه‌های تجزیه‌طلب در استان‌ها و نزدیک مرزهای ایران، اعتراض ناآگاهانه به اصل حجاب و سرلوحه قراردادن شعار آزادی بدون فهم معنای آن چه در اسلام و چه در غرب، شناخت برتری غرب در مسائل فنی و سکوهای مجازی و سوءاستفاده از آن‌ها و دیگر مسائل مطرح امروز جهان است، اگر تنها سیاست جمهوری اسلامی فیلترکردن این شبکه‌ها بدون پیش‌زمینه‌های آگاهی‌بخش و مدنظر قرارندادن دیگر ابعاد جنگ ترکیبی و تأثیر فیلترینگ در آن‌ها باشد قطعاً جهاد کبیر رخ نداده و ضررهای بیشتری را متأثر خواهیم شد. در نتیجه برای مقابله با جنگ شناختی نیازمند به استفاده از راهبردهای ویژه در مورد اقوام و اقلیت‌ها، شفافیت، اطلاع‌رسانی دقیق و بصیرت‌افزایی به جامعه، ارتقای سواد رسانه‌ای مخاطبان با استفاده از تمام وسایل ارتباط‌جمعی، ایجاد راه‌های مشروع برای ارضای نیازهای مردم، افزایش محصولات فرهنگی تأثیرگذار بر جامعه و جوانان می‌باشد. به‌عنوان کارهای آینده می‌توان به بررسی جنگ شناختی و راهکارهای مقابله با آن در صنعت فیلم‌سازی و انیمیشن پرداخت.

مراجع

[۱] چیستان، ذبیح الله، پور اسد، یعقوب، چیستان، حسین، بغدادی، حمیده (۱۳۹۵). بررسی آسیب‌ها و ارائه راه‌کارهای جنگ شناختی و ادراکی در فضای سایبری، نخستین کنفرانس ملی تحقیقات بین‌رشته‌ای در مهندسی کامپیوتر، برق، مکانیک و مکاترونیک.

[۲] قیامی، سید برات، سجادی اصیل، وحید، مصدق، مسعود (۱۳۹۹). معماری سازمانی جنگ شناختی در ارتش جمهوری اسلامی ایران، ۳(۷)، صص ۱۳۳-۱۵۲.

[۳] عراقی، عبدالله، بیدگلی، محمد، رجبی ده برزوئی، اصغر (۱۴۰۱). بررسی واکاوی اهداف جنگ شناختی دشمن و راهکارهای تاب‌آوری مقابله با آن با تأکید بر آموزه‌های قرآن، ۸(۲)، صص ۱۴۱-۱۶۰.

[۴] گری، کریس هیبلز (۱۳۸۱). جنگ پست مدرن، سیاست نوین درگیری، مترجم، احمدرضا تقاء، انتشارت دانشکده فرماندهی و ستاد، معاونت و تحقیق و پژوهش.

[۵] محبوب، حسن، شکوری، سعید (۱۴۰۱). بررسی جنگ‌شناختی مدرن: از شناخت در رزم تا عرصه جنگ‌شناختی، ۱۲(۲)، صص ۱۵۶-۱۸۰.

[6] Pocheptsov, G. (2018). Cognitive attacks in Russian hybrid warfare. Information Security, 41, 37-43.

[7] dit Avocat, A. B. (2021). Cognitive Warfare: The Battlefield of Tomorrow?. New Technologies, Future Conflicts, and Arms Control, pp. 60-64.

[8] Whiteaker, J., Valkonen, S. (2022). Cognitive Warfare: Complexity and simplicity.

[9] Calvillo, D. P., Smelter, T. J. (2020). An initial accuracy focus reduces the effect of prior exposure on perceived accuracy of news headlines. Cognitive research: principles and implications, 5(1), pp. 1-11.

[10] Burke, E. J., Gunness, K. A., Cooper, C. A., Cozad, M. R. (2020). People's Liberation Army operational concepts (p. 32). Santa Monica, CA: RAND.

[11] Hung, T. C., Hung, T. W. (2022). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. Journal of Global Security Studies, 7(4).

[12] Hammes, L. T. X. (1994). The evolution of war: The fourth generation. Marine Corps Gazette.

[13] Robinson, M., Jones, K., Janicke, H. (2015). Cyber warfare: Issues and challenges. Computers security, 49, pp. 70-94.

[14] Whyte, C., Thrall, A. T., Mazanec, B. M. (Eds.). (2020). Information warfare in the age of cyber conflict. Routledge.

[15] Wohlforth, W. C., & Zubok, V. M. (2017). An abiding antagonism: realism, idealism and the mirage of western–Russian partnership after the Cold War. International Politics, 54, pp. 405-419.

[16] Lewis, J. A. (2018). Cognitive effect and state conflict in cyberspace. Center for Strategic and International Studies (CSIS).

[17] Diamond, L., & Schell, O. (Eds.). (2019). China's influence and American interests: Promoting constructive vigilance. Hoover Press.

[18] Beskow, D. M., & Carley, K. M. (2020). Characterization and comparison of Russian and Chinese disinformation campaigns. Disinformation, misinformation, and fake news in social media: emerging research challenges and opportunities, pp. 63-81.

[19] Orinx, K., & de Swielande, T. S. (2022). China and Cognitive Warfare: Why Is the West Losing?.

[20] Splidsboel Hansen, F. (2021). When Russia wages war in the cognitive domain. The Journal of Slavic Military Studies, 34(2), pp. 181-201.

[21] Scales Jr, R. H. (2000). Adaptive enemies: Achieving victory by avoiding defeat. Joint Force Quarterly, 23, pp. 7-14.

[22] Green, S. A. (2008). Cognitive warfare. The Augean Stables.

[23] Zhou, H. (2020). An introduction of cognitive electronic warfare system. In Communications, Signal Processing, and Systems: Proceedings of the 2018 CSPS Volume III: Systems 7th (pp. 1202-1210). Springer Singapore.

شناسایی مالکِ داده‌ها در «هوش مصنوعی» و «اینترنت اشیاء»

محمد امینی[۱]، محمود رستگاری[۲]، سعید نصر[۲]

[۱] دانشجوی دکتری حقوق خصوصی، دانشگاه اصفهان، ایران
m.aminiphdlaw74@ase.ui.ac.ir
[۲] دانش‌آموخته کارشناسی ارشد حقوق خصوصی، دانشگاه اصفهان، ایران
{m.rastegari1994,saeednasr11}@gmail.com

چکیده

مالکیت از مفاهیم فقهی - حقوقی با سابقه‌ای است که مردم با آن آشنا بوده و متعلق آن را بیشتر اشیاء مادی تصور می‌کنند و وقتی با لفظ مالک مواجه می‌شوند، بی‌درنگ این لفظ را برای انسان معتبر می‌دانند. ولی به مرور زمان و فرض یا اعطای شخصیت به بعضی از عناوین یا نهادها، وصف ملکیت و مالک شدن برای آن‌ها نیز معقول شناخته شد. امروزه با پیشرفت تکنولوژی و فناوری‌های ارتباطات، برنامه‌ها و ابزارهای نوینی ظهور یافته که از جمله‌ی آنها، هوش مصنوعی (AI) و اینترنت اشیا (IOT) می‌باشد. براین‌اساس پرسش اصلی در تحقیق حاضر آن است که آیا می‌توان هوش مصنوعی و اینترنت اشیا را مالک داده‌هایشان دانست؟ در این خصوص آیا میان این دو تفاوت وجود دارد؟ نگارندگان با روش توصیفی - تحلیل و تدقیق در پژوهش‌های انجام شده و قوانین موجود به این مهم دست یافتند که در هوش مصنوعی با وجود وصف خودمختاری و امکان اعطای شخصیت، می‌توان آن را مالک آفرینه‌های ایجادی‌اش دانست، ولی در اینترنت اشیا، مالک داده‌های ارسالی از سوی شیئ، همان برنامه‌نویس، طراح و کنترل‌کننده‌ای است که این اطلاعات مستقیماً برای او فرستاده می‌شود.

کلمات کلیدی: اینترنت اشیا، شخصیت، مالک (مالکیت)، وصف خودمختاری، هوش مصنوعی.

۱ مقدمه

اقتضای تکنولوژی، فضای سایبر و فناوری ارتباطات، ایجاد برنامه‌ها و موضوعات نوظهوری است که به دنبال آن، مسائل حقوقی نوینی نیز مطرح می‌شود و لازم است به منظور حل ابهامات و چالش‌های مربوط به چنین فناوری‌های بدیع، حقوقدانان بدان پاسخ داده و متناسب با شرایط عصر و زمان خود، راه‌حل‌های صحیح و کاربردی ارائه دهند.

از جمله‌ی این موضوعات نوظهور و جذاب، هوش مصنوعی[۱] و اینترنت اشیا[۲] می‌باشد که در مقایسه با سایر

[1] Artificial Intelligence (AI)
[2] Internet of Things (IOT)

تکنولوژی‌های جدید، با شتاب شگفت‌انگیزی در حال توسعه‌اند. همین پیشرفت اعجاب‌انگیز، موجب طرح مسائل حقوقی بیشتری می‌شود که ضروری است حقوقدانان و پژوهشگران حقوقی به آن بپردازد. هوش مصنوعی که به اختصار آن را AI می‌نامند، یک پدیدهٔ نسبتاً نوینِ علومِ شناختی و علوم کامپیوتری است که برای برطرف کردنِ نیازهای جهانی، درحال تکمیل و توسعه است [۱].

اگر سابقاً تکنولوژی، صرفاً در بخش‌هایی مانند صنعت، کشاورزی، آموزش و غیره، به کار گرفته می‌شد و تنها متخصصین مربوطه توان کار با آن را داشتند، ظهور هوش مصنوعی و اینترنت اشیا این رسم را دگرگون ساخت و موجب شد انسان به طور مستقیم و غیرمستقیم در بخش‌های مختلف زندگی‌اش با آن‌ها مواجه باشد و حتی در مواردی، ادامه‌ی حیات او، منوط به استفاده از این برنامه‌ها و ابزار باشد. این انسان بود که قبلاً بر تکنولوژی و برنامه‌های آن مسلط بود[۳]، اما جهان امروزه شاهد یک اتفاق نادر و در مواردی دلهره‌آور است و آن، امکان تسلط هوش مصنوعی بر انسان و رفتارهای انسانی است و چنانچه متخصصان علم و دانش، اصول اخلاقی را در این زمینه رعایت نکنند و سرلوحه‌ی اقدامات خود قرار ندهند و بدون التفات به گزاره‌های وجدانی، صرفاً بر بُعد پیشرفت تکنولوژی چشم دوزند، چه بسا به همان سرعت، شرایطی پیش آید که هیچ‌گاه جبران آن ممکن نباشد و دیگر کاری از دست انسان برنیاید. به همین مناسبت، برخی از سازمان‌ها و موسسات، اسنادی در این زمینه تنظیم کرده‌اند[۴]. عمده اصول و قواعد مشترکی که در اسناد موجود در زمینه‌ی رعایت گزاره‌های اخلاقی در هوش مصنوعی، به چشم می‌خورد، عبارتند از: رعایت حریم خصوصی، مسئولیت پذیری، امنیت، شفافیت و قابلیت توضیح دادن، عدالت و دوری از تبعیض، کنترل انسان بر تکنولوژی، مسئولیت حرفه‌ای و ارتقای اصول انسانی [۱۷].

آنچه در این مقاله به عنوان یکی از مسائل حقوقی مطرح در حوزه‌ی هوش مصنوعی و اینترنت اشیا، مورد تحلیل و بررسی قرار می‌گیرد، موضوع مالکیت آثار و داده‌های ناشی از هوش مصنوعی و اینترنت اشیا است که مالک این داده‌ها و اطلاعات را چه کس یا چه چیزی باید دانست؟ آیا همان طراح، برنامه‌نویس و یا مالک و خریدار برنامه‌ی هوش مصنوعی و اینترنت اشیا، مالک آثار ایجادی AI یا IOT می‌شود یا آنکه مالک چنین داده‌هایی را باید همان هوش مصنوعی و شیئی که متصل به برنامه‌ی اینترنت است، دانست؟ به عنوان یک پرسش اساسی‌تر، آیا می‌توان هوش مصنوعی را به مثابه‌ی انسان، مالک آثار و آفرینه‌های ایجادی‌اش دانست و آیا چنین فرضی امکان‌پذیر است؟ آیا در این زمینه و راجع به موضوع مالک داده‌ها، تفاوتی میان هوش مصنوعی و اینترنت اشیا وجود دارد؟

روش تحقیق حاضر به صورت توصیفی - تحلیلی می‌باشد و شیوه‌ی گردآوری داده‌ها، به شکل کتابخانه‌ای و اسنادی است.

---

[3] human control of technology

[4] Ethics Guidelines for Trustworthy AI (2019) P 36. (available at https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai); Google, 'AI at google: our principles' (2018) https://www.blog.google/technology/ai/ai-principles/

۲ مروری بر کارهای دیگران

آقایی طوق و ناصر (۱۳۹۹) در تحقیقی با عنوان «چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایران و اتحادیه اروپا» با تبیین وظایف و اقدامات کنترل‌کننده، پردازنده و کاربر در اینترنت اشیا، بیان می‌دارند که دارنده‌ی ابزاری که با اینترنت اشیا فعالیت می‌کند، بدون اجازه کنترل‌کننده (باتوجه به حق معنوی طراح نسبت به داده‌های برنامه‌ی مورد ساخت و طراحی‌اش) نمی‌تواند داده‌های دریافتی ابزار متصل به اینترنت اشیا را به دیگری منتقل نماید. به عبارتی، هرچند دارنده‌ی شیئ، مالک آن وسیله است ولی داده‌های دریافتی توسط آن وسیله، برای کنترل کننده و طراح برنامه ارسال می‌شود و شخص اخیر، نسبت به داده‌های دریافتی، حق دارد. نگارندگان مقاله مزبور راجع به مالکیت آثار هوش مصنوعی، مطلبی ذکر نکرده و تفاوت هوش مصنوعی و اینترنت اشیا را در این خصوص، متذکر نشده‌اند.

کچوئی (۱۳۹۹) در پژوهشی با موضوع «وضعیت مالکیت آثار حاصل از هوش مصنوعی» پیشنهاد می‌دهد تا با پیش گرفتن رویه‌ای مانند حقوق انگلستان، آثار حاصل از هوش مصنوعی را منتسب به برنامه نویس آن دانست. درحالی‌که در مقاله‌ی حاضر، مستند به قوانین موجود و ظرفیت موجود در آنها، نتیجه‌ی دیگری بیان خواهد شد.

احمدیِ مرادی (۱۴۰۰) در پژوهشی (پایان‌نامه) با عنوان «اینترنت اشیا در فقه امامیه و حقوق ایران» به موضوع‌شناسی و بررسی ابعاد حقوقی – فقهی اینترنت اشیا پرداخته است. ایشان ذیل عنوان «حق مالکیت داده‌های شخصی» معتقد است که افراد نسبت به داده‌های خود در بستر اینترنت اشیا حق مالکیت دارند و دیگران اعم از دولت و افراد جامعه نمی‌توانند به حق او در این زمینه تجاوز کنند. اما چنانکه مشخص است این پژوهشگر صرفاً به موضوع اینترنت اشیا پرداخته و در خصوص هوش مصنوعی و مالکیت آفرینه‌های آن، سخنی نگفته است.

براین‌اساس نویسندگان تحقیق حاضر، مالک آفرینه‌ها و داده‌های هوش مصنوعی و اینترنت اشیاء را به صورت تطبیقی مورد تحلیل و شناسایی قرار می‌دهند.

۳ معرفی «هوش مصنوعی»

واژه هوش مصنوعی اولین بار در سال ۱۹۵۶ میلادی توسط جان مکارتی، ماروین مینیسکی و سایر همکارانشان در کنفرانس دارتموث ذکر شد [۱۸] و مطالعات آن به شکل رسمی از سال ۱۹۵۹م توسط آلن تورینگ، آغاز شد [۱۷].

تعریف واحدی برای هوش مصنوعی ذکر نشده است بلکه دارای تعاریف متعددی می‌باشد [۲۴]. در یک تعریف کلی، هوش مصنوعی به هر برنامه‌ی سخت افزاری یا نرم‌افزاری گفته می‌شود که از خود رفتاری نشان می‌دهد که هوشمندانه به نظر می‌رسد [۲۵]. باتوجه به شبکه‌های عصبی مصنوعی[۵] که در برنامه‌های فعال

[۵] Artificial Neural Networks؛ شبکه‌های عصبی مصنوعی مجموعه پردازشگرهای کوچکی هستند که همگی به یکدیگر متصل‌اند و برای حل یک مسئله، تقسیم وظایف می‌کنند. این مدل ریاضی به‌صورت یک الگوریتمِ کامپیوتری، برنامه‌نویسی شده است. این شبکه‌های عصبی (دارای ورودی و خروجی) بر روی اطلاعات ورودی پردازش انجام می‌دهند و چون حافظه‌ای مجزا

با تکنولوژی هوش مصنوعی وجود دارد، ویژگی‌هایی را برای هوش مصنوعی می‌توان برشمرد: مانند توانایی در تطبیق با شرایط جدید، آموختن، استدلال کردن، حل کردن مشکلات، ادراک و استفاده از زبان [۲۱].

هوش مصنوعی دارای سه ویژگی است: ۱. دنیای اطراف را فهم می‌کند، ۲. اطلاعات دریافتی را تحلیل کرده و ۳. سپس بر مبنای آن عمل می‌کند [۱۸]. مزیت هوش مصنوعی بر انسان، حضور همیشگی اطلاعات و فراموش نکردن امور است؛ اما از طرف دیگر فاقد احساس است و ممکن است باعث خساراتی شود؛ این دو ویژگی، آن را از خصایص انسانی متمایز و در احکام آن تغییرات ایجاد می‌کند [۱۸].

مطابق با نوع عملکرد هوش مصنوعی، دو رویکرد نسبت به آن وجود دارد [۲۴]:

الف. رویکرد ضعیف: در رویکرد ضعیف نسبت به هوش مصنوعی، محققان و پژوهشگران مربوطه، نه به دنبال ساخت انسانی مصنوعی بلکه به دنبال ساختن ماشینی هستند که در برخی از زمینه‌ها، کارکردی شبیه به انسان داشته باشد.

ب. رویکرد قوی: این رویکرد در پی آن است ماشینی بسازد که تمامی قابلیت‌های ذهن انسانی را داشته باشد [۲۴].

باتوجه به تعریفی که از هوش مصنوعی به عمل آمد، مشخص می‌شود که آفرینه‌های ناشی از این‌گونه برنامه‌ها مانند ChatGPT[۶] دارای وصف خودمختاری[۷] اند. به‌عبارتی، سیستم‌ها و برنامه‌های هوش مصنوعی، با داده‌ها و اطلاعاتی که در اختیار آن‌ها گذاشته می‌شود و یا خود دریافت می‌کنند، مستقلاً تصمیم‌گیری کرده و تابع محض نمی‌باشند. برخلافِ سیستم‌های اتوماتیک[۸] که فرایند کارشان مشخص و قابل پیش‌بینی[۹] است ، در هوش مصنوعی، تأمین کننده و سازنده‌ی آن، از تصمیم و پاسخ برنامه ناآگاه است و حتی غالباً امکان پیش‌بینی آن نیز وجود ندارد. برای مثال امروزه یکی از انواع گسترده‌ی استفاده از یادگیری ماشین نرم‌افزاری است که با استفاده از یادگیری عمیق می‌تواند چهرهٔ انسان را تشخیص دهد. در این برنامه، طراح نمی‌داند به طور دقیق چه مراحلی طی می‌شود تا ماشین به نتیجهٔ اشاره شده برسد. برنامه‌نویس داده‌ها را به ماشین می‌دهد، هدف را برای آن مشخص می‌کند، و وقتی در مسیر درست تشخیص است به آن بازخورد مثبت می‌دهد. اما اینکه ماشین سپس چه مراحلی را طی می‌کند تا به نتیجه برسد نامعلوم است [۲۵]. این دستگاه‌ها (دستگاه‌های هوشمند و متصل به هوش مصنوعی) دیگر ابزار ساده‌ای برای تسریع ارتباطات در دست کاربر خود و انتقال اراده او نیستند؛ بلکه خودشان شروع کننده یک ارتباط بوده و در تشکیل عقد و قرارداد نقش سازنده دارند و برای مثال اعمال حقوقی مانند عقد بیع، دیگر نه از طریق آنها بلکه توسط آنان تشکیل می‌شود [۳۰].

برای خود دارند، اطلاعات را در خود ذخیره می‌کنند و به‌طور هوشمندانه‌ای، اطلاعات دریافتی، به‌روزرسانی می‌شوند و الگوی جدیدی را در پیش می‌گیرند [۱].

[۶] هوش مصنوعی ممکن است حالت مادی داشته باشد که ربات (Robot) خطاب می‌گردد یا صرفاً نرم‌افزاری باشد که مصطلح به بات (Bot) است [۳۲].

[7] Autonomous

[8] Automatic Systems

[۹] هوشمندی سامانه‌ی اتوماتیک محدود به انعقاد معامله و انجام کارهای خواسته شده، طبق دستور است، نه تشخیص مصلحت مالک [۲۱].

۴ معرفی «اینترنت اشیاء»

اصطلاح اینترنت اشیاء را اولین بار شخصی به نام کوین اشتون[10] در سال ۱۹۹۹م به کار برد و برای نخستین بار آن را انتشارات مؤسسه فناوری ماساچوست به دنیا معرفی نمود و جهانی را توصیف کرد که در آن هر چیزی از جمله اشیای بی‌جان، برای خود هویت دیجیتال داشته باشند و به کامپیوترها اجازه دهند آنها را سازماندهی و مدیریت کنند [۱۶]. این فناوری در سال ۲۰۰۵ طبق گزارش اتحادیه مخابرات بین المللی (ITU) صورت رسمی معرفی شد [۴].

اینترنت اشیا باعث ارتباط اشیا به اشیا می‌شود و پیدایش آن موجب گردید یک اکوسیستم جدیدی برای زندگی انسان به وجود آید. منظور از اینترنت اشیا، سناریوی کاربردی متنوعی است که در آنها اتصالات درون شبکه و قابلیت‌های محاسباتی به حسّ‌گرها، اشیا و تمامی تجهیزات روزمره تعمیم داده شده و به آنها اجازه می‌دهند تا اشیا با کمترین دخالت انسان، اطلاعات و داده‌ها را تهیه، مبادله و استفاده کنند [۸].

در اینترنت اشیا، واقعیت آن ناظر است به اینکه اشیاء از طریق اینترنت به هم مرتبط می‌شوند. برای مثال به موجب سیستم GPS خودرو که در زمان سرقت رفتن آن، می‌توان مکان آن را شناسایی کرد، شکلی ساده از اینترنت اشیا است. به عنوان یک نمونه ساده، وقتی از طریق گوشی همراه با تلویزیون ارتباط برقرار می‌کنید و به کمک یک نرم‌افزار، گوشی تبدیل به کنترل تلویزیون می‌شود، نوعی اینترنت اشیاء ایجاد شده است؛ لکن اگر در همین مثال دقت شود، خود ساختمان فیزیکی موبایل با قالب فیزیکی تلویزیون ارتباط برقرار نمی‌کند، بلکه نرم‌افزاری که در آن نصب شده است با حس‌گرهای تلویزیون که قابلیت ارتباط‌گیری را دارند، ارتباط برقرار می‌کند. در واقع موجودیت‌های مجازی که در داخل موجودیت‌های فیزیکی قرار دارند، با هم ارتباط می‌گیرند و در ظاهر ارتباط بین دو چیز فیزیکی تصور می‌شود [۹].

ماده ۲۹ اعلامیه مرکز نظارت بر داده پیام‌های اتحادیه اروپا مصوب ۲۰۱۰ با الحاقات و اصلاحات، در تعریف اینترنت اشیا بیان می‌دارد: «اینترنت اشیا، زیرساخت‌هایی هستند که در آن، میلیاردها حس‌گر تعبیه شده در دستگاه‌های کاربردی روزمره برای ضبط، پردازش، ذخیره و انتقال داده‌ها طراحی شده است و همانطور که از قابلیت ارتباط با عامل انسانی برخوردار هستند، با بهره‌مندی از شناسه‌های منحصر به فرد، با دستگاه‌ها یا سیستمهای دیگر با استفاده از قابلیت‌های شبکه، تعامل برقرار می‌کنند». به عبارت دیگر، ابزارهای اینترنت اشیا، نوعی ابزارهای هوشمندند که با تعبیه پروتکل‌های منحصر به فرد به پردازنده آنها، همانند انسان، قابلیت دریافت و پردازش داده پیام‌ها برای انجام وظایف از پیش تعیین شده را دارند.

بنابراین، اینترنت اشیا سیستمی است که بدون دخالت انسان، دستگاه‌ها قادر به برقراری ارتباط با یکدیگر هستند و منجر به خروجی سریع‌تر و به موقع می‌شوند و باعث بالا رفتن اطلاعات بیشتر می‌گردد و به تصمیم گیری بهتر کمک می‌کند و باعث صرفه جویی در زمان و هزینه می‌شود. در واقع هدف اینترنت اشیا، اتصال در هر زمان و مکان با هر چیزی و هر شخصی است که از هر مسیری، از آن شبکه و خدمت استفاده می‌کند [۱۱].

ابزارهای اینترنت اشیا با برخورداری از پروتکل‌های از پیش طراحی شده، نسبت به جمع‌آوری اطلاعات

[10] Kevin Ashton

محیط پیرامون خود، پردازش و ارسال اطلاعات به کنترل‌کنندگان یا پردازندگان اقدام می‌کنند [۳۰]. پس در اینترنت اشیا اشخاصی به نام کنترل کننده و پردازش‌گر نقش ایفا می‌کنند. بند ۷ ماده ۴ دستورالعمل مصوب ۲۰۱۶ اتحادیه اروپا در تعریف کنترل کننده بیان می‌دارد: «کنترل کننده، شخص حقیقی یا حقوقی، مرجع عمومی، نمایندگی یا هر نهاد دیگری است که به تنهایی یا به طور مشترک با دیگران، اهداف و وسایل پردازش داده‌های شخصی را تعیین می‌کند». دسترسی کنترل کننده به اطلاعات پردازش شده، هرچند تحت خط مشی تعیین شده توسط وی صورت می‌پذیرد اما نمی‌توان عنوان پردازنده را بر این اشخاص بار کرد. این امر در شماره ۱۱ از بند ۸ ماده ۲۹ اعلامیه و دستورالعمل مذکور نیز مورد تاکید قرار گرفته شده است [۳۰]. به موجب بند ۸ ماده ۴ دستورالعمل «پردازنده؛ شخصی حقیقی یا حقوقی، مقامات دولتی یا هر نهاد دیگری است که داده‌های شخصی را از طرف کنترلکننده پردازش می‌کند» به عبارتی، عنوان پردازنده داده پیام از کنترل کننده جدا است. عملکرد پردازشگر، تحت خط مشیی است که توسط کنترل کننده تعیین می‌گردد. ازاین‌رو در صورتی که خط مشی و چگونگی پردازش داده پیام‌ها توسط پردازشگر تعیین گردد وی دارای عنوان کنترل کننده است و مسئولیت‌های قانونی پیش‌بینی شده برای کنترل کننده برای وی نیز قابل اعمال خواهد بود [۳۰]. مطابق بند ۲ ماده ۴ دستورالعمل مصوب ۲۰۱۶ در ارتباط با عملیات پردازشگر: «پردازش به مجموعه‌ای از عملیات اطلاق می‌گردد که بر روی داده‌های شخصی از طریق اعمالی مانند جمع آوری، ضبط، سازماندهی، ذخیره سازی، سازگاری یا تغییر، بازیابی، مشاوره، استفاده، افشای از طریق انتقال، انتشار یا استفاده دیگر، تراز یا ترکیب، مسدود کردن، محدودیت، پاک کردن یا تخریب صورت پذیرد».

از آنجا که فناوری اینترنت اشیا، واجد زوایای گوناگونی است که مدنظر دستورالعمل حفاظت از داده پیام‌های الکترونیکی اتحادیه اروپا در سال ۱۹۹۵ قرار نگرفته بود، سیاست‌گذاران در این اتحادیه مبادرت به تصویب مقرراتی جدید با عنوان دستورالعمل عمومی حفاظت از اطلاعات اتحادیه اروپا در سال ۲۰۱۶ نمودند و این مهم در ماه مِی سال ۲۰۱۸ لازم الاجرا گردیده است [۳۰].

۵ امکانِ فرض یا اعتبارِ «شخصیت» برای هوش مصنوعی

مالک شدن، منوط به وجودِ «شخص» و لحاظ «شخصیت» است و ازاین‌رو مالک شناختن هوش مصنوعی نسبت به آفرینه‌هایش، نیازمند بررسی این مهم است که آیا امکان اعطای شخصیت به هوش مصنوعی وجود دارد؟ راجع به این امر، چه نظراتی وجود دارد؟

شخصیت، مقوّم شخص حقوقی است و شخص حقوقی قبل از دارا بودن شخصیت نمی‌تواند وجود داشته باشد و با داشتن شخصیت است که شخص حقوقی ایجاد می‌گردد و شخص حقوقی بدون شخصیت قابل پذیرش نیست. از طرفی نیز شخصیت یک صفت وجودی است و نمی‌تواند به معدوم تعلق گیرد و ابتدا باید چیزی وجود داشته باشد تا به آن شخصیت داده شود و به عنوان شخص شناخته گردد. راجع به امکان اعطای شخصیت به هوش مصنوعی، نظریاتی مانند هوش مصنوعی به مثابه‌ی «نهنگ»[۱۱] [۱۸ و ۱۹]، نظریه واقعی

[۱۱] بر مبنای این تئوری، کسانی هوش مصنوعی را به دلیل هوشمند بودن آن و اینکه به نوعی دارای شعور و ادراک است، به حیواناتی مانند نهنگ که دارای درجه‌ای از خودآگاهی و هوشمندی است قیاس کرده و مدعی صلاحیت اخلاقی سامانههای

بودن شخص حقوقی [۵ و ۲۱]، نظریه اعتبار حقوقی [۳۰] و غیره مطرح شده است. به نظر می‌رسد هر دو نظریه‌ی واقعیت و اعتباری بودن شخصیت حقوقی با تعدیلاتی قابل پذیرش بوده و بر سامانه‌های هوشمند نیز قابل تطبیق است [۲۴].

هوش مصنوعی دارای یک واقعیت است؛ اطلاعات را پردازش کرده و کارهای محوله را انجام میدهد. مثلاً اقدام به انعقاد عقد می‌کند یا در کنار پزشکان فعالیت کرده یا ماشینی می‌شود خودران. در صورت داشتن شخصیت حقوقی، شخصیت به این واقعیت است که داده می‌شود و پس از دارا شدن این شخصیت، دارای وجودی اعتباری به صورت شخص حقوقی نیز می‌گردد که می‌تواند صاحب حق و تکلیف شود. اعطای شخصیت، مصلحتی است که قانونگذار به هرچه تشخیص دهد با رعایت شرایط و ضوابط می‌تواند اعطا کند؛ حال این مصلحت می‌تواند سهولت و توجیه معاملات منعقده باشد یا مسئولیت مدنی و مسائل دیگر. پس باید بر این نظر بود که از جهت مبنای علمی و تئوری، داشتن شخصیت حقوقی برای سامانه‌های هوشمند امکان‌پذیر است [۲۴].

در آمریکا، قوانینی مانند قانون امضاهای الکترونیکی در تجارت ملی و جهانی[۱۲]، قانون یکنواخت معاملات الکترونیکی[۱۳] و قانون یکنواخت معاملات مبتنی بر اطلاعات رایانه‌ای[۱۴]، از سامانه‌های الکترونیکی به «ابزار» تعبیر کرده است که به صورت ضمنی، داشتن شخصیت حقوقی سامانه‌های خودکار را نفی می‌کند. آنچه از آراء قضایی در محاکم آمریکایی نیز بر می‌آید[۱۵]، مبین گرایش محاکم بر تلقی نماینده الکترونیکی به مثابه ابزاری صرف در اختیار استفاده کننده است که مسئولیت را همواره معطوفِ شخص به کار گیرنده سامانه الکترونیکی کرده و در این میان اشاره‌ای به قواعد نمایندگی یا وجود شخصیت مستقل برای سامانه‌ها نشده است [۳۲]. ظاهراً تا کنون نظام حقوقی وجود ندارد که به طور رسمی شخصیت حقوقی را برای سامانه‌های هوشمند به رسمیت شناخته باشد[۱۶] [۲۴].

در حقوق ایران که مبتنی بر نظام شرعی و فقهی است، امکان تفویض شخصیت به هوش مصنوعی نیازمند دلیل است. با بررسی در فقه، می‌توان رگه‌هایی از اعطای شخصیت به غیر انسان را یافت. مثلا در بحث وقف و یا وصیت اگر موقوف‌علیهم یا موصی‌لهم محصور نباشند و وقف و وصیت بر عناوین کلی همانند نمازگزاران، فقرا، مصالح عامه، جهات و غیره انجام پذیرد، این بحث پیش می‌آید که مالکیت مال موقوفه یا موصی‌به متعلق

هوشمند برای اعطای شخصیت حقوقی شده‌اند. البته به این نظریه ایراد وارد شده است.

[12] Electronic Signatures in Global and National Commerce Act. E- sign

[13] Uniform Electronic Transactions Act. UETA

[14] Uniform Computer Information Transactions Act, UCITA

[15] Register.com, Inc., Plaintiff-appellee, v. Verio, Inc, US Court of Appeals for the Second Circuit - 356 F.3d 393 (2d Cir. 2004) Argued: January 21, 2001 Decided: January 23, 2004. Other case: Corinthian Pharmaceutical v. Lederle Laboratories, 724 F. Supp. 605 (S.D. Ind. 1989) US District Court for the Southern District of Indiana - 724. see on: https://law.justia.com/cases/federal/appellate-courts/F3/356/393/539823/

[۱۶] مطالبی که در مقاله حاضر راجع به شخصیت و وضعیت مالکیت داده‌های اینترنت اشیاء و آفرینه‌های هوش مصنوعی از برخی از حقوق کشورها بیان می‌شود، برگرفته از تحقیقات و قوانینی است که تا زمان نگارش این پژوهش وجود داشته و چه بسا به مرور زمان، قوانین کشورهای مذکور در این مورد تغییر یابد. لذا به پژوهشگران و خوانندگان این مقاله توصیه می‌شود برای به روزرسانی اطلاعات و آگاهی خود، آثار، تحقیقات و مقررات تدوینی جدیدتر را که بعد پژوهش حاضر انجام می‌شود را، مشاهده نمایند.

به چه کسی است؟ آیا مالک کنونی، مفاهیم کلی نمازگزاران، فقها، فقرا و غیره هستند یا مصادیقشان به حمل شایع؟

برخی قائل بر این نظر هستند که هرجا فقها از همان زمان‌های قدیم خواسته‌اند اهلیت و صلاحیت موضوعی غیر انسانی را مطرح سازند، از عنوان «جهت» استفاده کرده‌اند [۳۲]. با پذیرش کنونی اصل شخصیت حقوقی در فقه، به نظر نمی‌رسد مشکلی برای پذیرش آن برای سامانه‌های هوشمند وجود داشته باشد [۲۴]؛ زیرا این شخصیت با استناد به ارتکاز و سیره عقلا و ظهور اطلاقات و عمومات ادله به مسائل مستحدثه‌ای تسری داده شده است که سابقه‌ای در گذشته ندارند [۱۴].

به موجب بند م ماده ۲ قانون تجارت الکترونیکی (مصوب ۱۳۸۲): «شخص[17] اعم است از شخص حقیقی و حقوقی و یا سیستم‌های رایانهای تحت کنترل آنان». چنانکه مشخص است بند اخیر در یک نوآوری و با نظر به مقتضیات زمانه، سیستم‌های رایانه‌ای تحت کنترل را نیز شخص محسوب کرده است. برای تطبیق هوش مصنوعی بر این ماده، باید بیان داشت که داده‌ها و آفرینه‌های حاصل از هوش مصنوعی، تحت کنترل سازنده و برنامه نویس آن نیست (کنترل جزئی)، زیرا با عنایت به ویژگی خودمختاری هوش مصنوعی در تولید اطلاعات، امکان پیش بینی پاسخ و یافته‌ی تولیدی هوش مصنوعی از سوی سازنده‌ی آن، وجود ندارد. البته چنانچه تعبیر «تحت کنترل» موسع معنا شود و هریک از اقسام کنترل کلی و جزئی را داخل آن قرار داد، براین‌اساس می‌توان هوش مصنوعی را نیز طبق ماده مذکور، شخص قلمداد نمود؛ زیرا درهرحال کنترل کلی برنامه‌ای که با هوش مصنوعی فعالیت می‌کند، در اختیار سازنده و طراح آن می‌باشد.

یکی از دلایلی که حقوقدانان را متمایل یا مجاب به پذیرش شخصیت حقوقی برای سامانه‌های هوشمند می‌گرداند، توانایی این سامانه‌ها در مذاکره و انعقاد قرارداد است. وقتی سامانه‌های هوشمند، برخلاف سایر اشخاص حقوقی قادر به انعقاد عقد به صورت مستقل باشند، دیگر نیازی به شخص حقیقی برای نمایندگی آنها وجود نخواهد داشت؛ اما صرف اعطای شخصیت حقوقی یا شناسائی آن از جانب قانونگذار، مشکل عدم وجود اراده برای آنها و فقدان اهلیت استیفا را حل نخواهد کرد [۲۵]. مگر اینکه قانونگذار امکان انشای اعمال حقوقی از جانب هوش مصنوعی را به رسمیت بشناسد؛ پس حداقل سامانه‌های هوشمندی که به نمایندگی معامله می‌کنند در صورت داشتن شخصیت حقوقی، دارای اهلیت انعقاد عقد نیز خواهند بود و از این حیث نیازمند نماینده نخواهند بود [۲۴].

۶ وضعیت مالکیت آثار و داده‌های حاصل از هوش مصنوعی و اینترنت اشیاء

قانونگذاران انگلیسی، در مورد پدیدآورندگی آثار حاصل از هوش مصنوعی، براین نظر هستند که این عنوان را به شخصی که کارها و عملکردهای لازم برای خلق اثر را انجام داده است، اعطا شود. به عبارتی برنامه‌نویس هوش مصنوعی را مستحق چنین عنوانی می‌دانند، به دلیل آنکه او آگاهی کامل نسبت به نحوه‌ی عملکرد الگوریتم‌ها و چگونگی انجام فرآیند خلاقانه را دارد [۳۰].

[17] Person

به نظر می رسد که این موضوع در مورد هوش مصنوعی قوی صادق نباشد. درست است که برنامه نویس ابتدا الگوریتم‌هایی را طراحی می‌کند اما پس از آن، نمی‌توان رابطه ی سببیتی بین اثر ایجاد شده و عمل برنامه نویس برقرار ساخت. به عبارتی به نظر می‌رسد، نظریه‌ی بیان شده در مورد پدیدآورندگی برنامه نویس، زمانی قابل اعمال باشد که ارتباط منطقی بین برنامه نویس و خروجی خلاق وجود داشته و قابل مشاهده باشد [۳۰].

در اتحادیه اروپا، اعطای عنوان مالکیت و پدیدآورندگی آثار، مبتنی براین نظر است که اثر، بیانگر اصالت و شخصیت پدیدآورنده باشد؛ اما امروزه با توجه به پیشرفت‌های هوش مصنوعی، برنامه‌نویس، هیچ دخالتی در روند خلاق شبکه‌های نورونی و الگوریتمی ندارد و تأثیر وی در فرآیندهای خلاق، حذف می‌شود؛ لذا بعید به نظر می‌رسد که آثار حاصل از هوش مصنوعی، بازتابی از شخصیت پدیدآورنده‌ی هوش مصنوعی (یعنی برنامه‌نویس و سازنده) باشد [۳۰].

در اتحادیه اروپا، راهنمای EC/24/2009 بیان می‌دارد که برنامه نویس هوش مصنوعی است که می‌تواند حمایت‌های کپی رایتی را دریافت کند، نه خود هوش مصنوعی. علاوه بر آن ماده‌ی (۱) ۷ کنوانسیون بِرن و ماده‌ی ۹ اصلاحات EC/116/2014، مدت حمایت را براساس فوت پدیدآورنده تعیین کرده است، لذا این مفاد بر فرضی است که پدیدآورندگان، انسان باشند؛ بنابراین نمی‌توان یک موجود مصنوعی را به عنوان یک پدیدآورنده در اتحادیه اروپا، دانست [۳۲].

در قوانین اتحادیه اروپا، از جمله ماده‌ی ۹۱ قانون ثبت اختراعات تصریح می‌کند، تقاضانامه‌ی ثبتِ اختراع باید شامل نام و نام خانوادگی مخترع باشد. چنین قاعده‌ای در قوانین حقوق اختراعات آمریکا نیز مشاهده می‌شود، علاوه‌بر آن، دادگاه‌های فدرال نیز بارها تاکید کرده اند که تنها شخص حقیقی است که استحقاق برخورداری از عنوان مخترع و حقوق مالکانه‌ی ناشی از آن را دارد و در تازه ترین رای خود که مربوط به پرونده‌ی DABUS بود نیز براین موضوع مجدداً تاکید داشت[۱۸].

در حقوق ایران برای امکان مالک شناختن هوش مصنوعی، باید بین دو رویکرد حقوق اختراعات و رویکرد حقوق کپی رایت قائل به تفصیل شد.

وفق رویکرد حقوق اختراعات و مستند به مواد و مقرراتی از جمله ماده ۱ قانون ثبت اختراعات و طرح‌های صنعتی و علائم تجاری مصوب ۱۳۸۶: «اختراع نتیجه فکر فرد یا افراد است که برای اولین بار فرآیند یا

[۱۸] در پرونده DABUS، مالک و متصرف ماشین (DABUS) مدعی بود که ماشین، اختراعی را به وجود آورده و بیان می‌کرد برای حل مسئله‌ی خاصی به وجود نیامده است و هیچ داده‌ی به خصوصی که مرتبط با اختراع حاصله باشد، به آن تعلیم نداده است. همچنین اظهار داشت که مخترع نباید منحصر به اشخاص طبیعی باشد، لذا در تقاضانامه‌ی تقدیمی، نام ماشین را به عنوان مخترع درج کرد و معتقد بود اخطار ۸ آگوست ۲۰۱۹ مبنی بر اصلاح تقاضانامه و مشخص کردن شخص طبیعی به عنوان مخترع ، فاقد اعتبار و باطل است (In re Application of Application No,; 16/524,350). نتیجه گیری کلی که از پرونده‌ی ارائه شده، چنین است: به دلیل آن که تقاضانامه مذکور ماشین را مخترع می‌داند، به دلیل قواعد موجود و پرونده‌ها و قواعد اداره‌ی ثبت اختراعات و علائم تجاری و قوانینی که مخترع را محدود به شخص طبیعی می‌داند، تقاضانامه‌ی مذکور منطبق با بخش a 115، کد ۳۵ نمی باشد. بنابراین اداره ی ثبت اختراعات و علائم تجاری، در ۸ آگوست ۲۰۱۹ به درستی اطلاعیه داد که شناخت مخترع مستلزم نام قانونی فرد است بنابراین قانون اختراعات آمریکا اجازه نمی‌دهد که ماشین‌ها به عنوان مخترع در تقاضانامه حق اختراع آورده شود و هنوز نقش انسان به عنوان مخترع اهمیت دارد [۳۲]. استدلال ارائه شده در پرونده DABUS، باتوجه به قوانین موضوعه ی آمریکا صحیح می باشد و نشان دهنده‌ی عدم تمایل و پذیرش هوش مصنوعی به عنوان مخترع در نظام اختراعات این کشور است [۱۷].

فرآورده‌ای خاص را ارائه می‌کند و مشکلی را دریک حرفه، فن، فناوری، صنعت و مانند آنها حل می‌نماید»؛ بند ب و ج ماده‌ی ۵ قانون مزبور: «... –ب اگر افرادی به صورت مشترک اختراعی کرده باشند، حقوق ناشی از اختراع مشترکاً به آنان تعلق می‌گیرد. ج– هرگاه دو یا چند نفر، مستقل از دیگری اختراع واحدی کرده باشند ...» و نیز بند ۱ فصل ۱ از بخش ۲ ماده ۵ آیین نامه اجرایی قانون ثبت اختراعات ، طرح های صنعتی و علائم تجاری سال ۱۳۸۷ می‌توان چنین اظهار داشت که حقوق ایران، تنها فرد انسان (شخص حقیقی یا طبیعی) را به عنوان مخترع به رسمیت می‌شناسند؛ چرا که سیاق بیان و کلمات به کار گرفته شده در نگارش مواد قانونی به شیوه‌ای است که چنین برداشتی را موجب می‌شود. در نتیجه، اگرچه در صورت وجود شرایط، حقوق اختراعات ایران از مخترع هوش مصنوعی -که انسان است– حمایت به عمل می‌آورد اما هوش مصنوعی را به عنوان مخترع و مالک اختراعش به رسمیت نمی‌شناسد [۱۷].

اما رویکرد حقوق کپی رایت، با توجه به قسمت ابتدایی ماده‌ی ۱ قانون حمایت از حقوق مولفان و مصنفان و هنرمندان مصوب ۱۳۴۸ که بیان می‌دارد: «از نظر این قانون به مؤلف و مصنف و هنرمند «پدیدآورنده» و به آنچه از راه دانش یا هنر و یا ابتکار آنان پدید می‌آید بدون در نظر گرفتن طریقه یا روشی که در بیان و یا ظهور و یا ایجاد آن به کار رفته «اثر» اطلاق می‌شود»؛ شاید بتوان چنین تفسیر کرد که هوش مصنوعی نیز می‌تواند به عنوان پدیدآورنده شناخته شود و حتی به نظر می‌رسد که بتوان مفهوم هوش مصنوعی را به قسمت‌های اخیر ماده نیز تطبیق داد. بدین نحو که هوش مصنوعی با توجه به توسعه و پیشرفت‌هایی که در چند سال اخیر داشته است، واجد ابتکار و خلاقیت می‌باشد و می‌تواند با تکیه بر داده‌های دریافتی دانشی که به آن تعلیم داده شده است، اثری را مستقلاً ایجاد نماید. هم‌چنین با توجه به قسمت اخیر بند الف ماده اول آیین نامه اجرایی ماده ۲۱ قانون سال ۱۳۴۸[۱۹] که بیان می‌کند: «... و هرگاه درخواست کننده شخص حقوقی باشد نام و شماره ثبت واقامتگاه قانونی شخص حقوقی» و به کار بردن لفظ (شخص)[۲۰] در تعریف پدیدآورنده نرم‌افزار ذیل ماده ۳ آیین نامه‌ی اجرایی ماده ۲ و ۱۷ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای[۲۱]؛ می‌توان چنین برداشت نمود که پدیدآورنده می‌تواند شخص حقوقی نیز باشد. بنابراین چنانچه بتوان برای هوش مصنوعی شخصیت مستقل قانونی قائل شد (همانطور که در قسمت قبل، ممکن دانسته شد)، به نظر می‌رسد که امکان تطبیق آن با همین قوانین موجود در نظام کپی رایت سنتی حاکم در حقوق کپی رایت ایران، وجود داشته باشد. البته از قانون اصلاح ماده ۱۲ قانون سال ۱۳۴۸، فناپذیر بودن پدیدآورنده برداشت می‌شود. در این مورد، شاید بتوان گفت زمانی که استهلاک و مخارج هوش مصنوعی افزایش یابد و کارکرد اولیه‌ی خود را از دست دهد و و ارتقاء سیستم به نحوی ناممکن یا بسیار هزینه‌بر باشد، شاید بتوان آن زمان را پایان عمر سیستم یاد شده دانست. لذا به طور کلی در صورت پذیرش موارد یاد شده به نظر می‌رسد که در

[۱۹] ماده اول – ثبت اثر طبق درخواست نامه چاپی که از طرف وزارت فرهنگ و هنر تهیه ودر اختیار درخواست کننده ثبت اثرگذارده می شود به عمل می آید و باید در دو نسخه به زبان فارسی نوشته وامضاءشده و حاوی نکات زیر باشد: الف – نام و نام خانوادگی و تابعیت واقامتگاه وشماره محل صدور شناسنامه و تاریخ تولد پدید آورنده و یا شخصی که به اعتبار قانون فوق الذکر قائم مقام پدید آورنده اصلی اثر می باشد و هرگاه درخواست کننده شخص حقوقی باشد نام و شماره ثبت واقامتگاه قانونی شخص حقوقی. ...

[۲۰] لفظ شخص، اعم است از انسان و غیرانسان (در موردی که برای آن، شخصیت، فرض یا اعتبار شده است).

[۲۱] – پدیدآورنده نرم‌افزار شخص یا اشخاصی هستند که بر اساس دانش و ابتکار خود کلیه مراحل مربوط اعم از تحلیل، طراحی، ساخت و پیاده سازی نرم‌افزار را انجام دهند.

نظام کپی رایت ایران بتوان مالکیت آثار کپی رایتی را به هوش مصنوعی نسبت داد [۱۷].

علاوه بر دو رویکرد مزبور و قوانین مربوط به آن، می توان از قانون تجارت الکترونیکی (مصوب ۱۳۸۲) هم استمداد جست.

ازاینرو و باتوجه به مسائل شخصیت که بیان گشت و ارتباط مالک شدن با شخص، می‌توان اظهار داشت که با چنین تفسیری، هوش مصنوعی را طبق بند م ماده ۲ از قانون مزبور، ممکن است هم شخص قلمداد کرد و هم مالک آفرینه‌هایش.

البته امکان طرح این ایراد وجود دارد که چون آفرینه‌های هوش مصنوعی، اثر فکری است و آثار فکری متعلق به موجودی صاحب فکر می‌باشد (باتوجه به قانون ثبت اختراعات ۱۳۸۶)، لذا هوش مصنوعی را نمی‌توان مالک بُعد معنوی (حقوق معنوی[۲۲]) آثارش دانست و هوش مصنوعی از حیث مالکیت فکری، با خلاء مالک روبه‌رو است. مگر آنکه مفهوم فکر را توسعه داد و بیان شود بُعد معنوی اثر هم از آنِ هوش مصنوعی است.

همچنین در سال ۱۳۹۳ لایحه ای تحت عنوان حمایت از مالکیت فکری به پیشنهاد وزارت فرهنگ و ارشاد به تصویب هیئت دولت رسید. اگرچه تا به امروز این لایحه به تصویب مجلس شورای اسلامی نرسیده است لکن در بخش اول از کتاب اول این لایحه که در مورد مالکیت ادبی و هنری و حقوق مرتبط است، نکات جالبی قابل مشاهده است؛ از جمله آنکه در بند ۸ از ماده ۱، اثر پدید آمده‌ی خودکار چنین تعریف شده است: «اثری که بدون دخالت مستقیم انسان به طور خودکار توسط رایانه یا ابزارهای وابسته و مشابه آن ایجاد شده است از قبیل نقشه هوایی» و در ادامه در تبصره‌ی ماده ۷۸، مدت حمایت در اثر پدید آمده خودکار را، تا ۵۰ سال پس از خلق اثر شناسایی می‌کند.

به نظر می‌رسد که بتوان تعریف اثر خودکار در لایحه را نسبت به آثار حاصل از هوش مصنوعی نیز تعمیم داد و براین اساس می توان چنین نتیجه گرفت که در صورت تصویب لایحه، آثار حاصل از هوش مصنوعی می‌توانند طبق تبصره‌ی ماده‌ی ۷۸ تا ۵۰ سال مورد حمایت قانون قرار گیرد [۱۷].

اما در اینترنت اشیا به نظر نمی‌رسد چنین باشد. توضیح آنکه باتوجه به اهمیت مالکیت داده‌های شخصی اینترنت، می‌توان مالکیت داده پیام‌ها را به دو صورت مطرح کرد:

۱. حقیقی: این مورد در ارتباط با انسان‌ها است. به عنوان مثال افرادی که لباس هوشمند به تن دارند و با توجه به آن، هرروز سلامتی خود را ارزیابی می‌کنند.

۲. حقوقی: در این مورد می‌توان کارخانه‌ها را مثال زد که با سیستم هوشمند اداره می‌شوند و به عنوان

[۲۲] حقوق معنوی بخشی از حقوق پدیدآورندگان آثار فکری است که اساساً جنبه‌ی مالی و اقتصادی ندارد و وابسته به شخصیت پدیدآورنده است. بدین معنی، حقوق معنوی در مقابل حقوق مادی قرار دارد (صفایی، ۱۳۸۵، ص ۲۰). حقوق معنوی از منافع مادی پدیدآورنده دفاع نمی‌کند بلکه صرفاً از شخصیت او در صورتی که در قالب یک اثر تجلی یافته باشد، حمایت خواهد کرد [۳۰ و ۳۱]. حق معنوی ماهیتی مختلط از حق مالی و با ارزش و حق غیرمالی و مربوط به شخصیت است. این اختلاط، به ویژه در فرضی که مولفی حق انتشار اثر خود را به دیگران واگذار می کند، دیده می‌شود؛ آنچه انتقال یافته چهره مالی حق تألیف و بهره برداری از انتشار اثر است. ولی حق شخصی او درباره دفاع از اثر خود و تجدیدنظر در آن همچنان باقی است و مانند سایر حقوق غیرمالی به دیگران انتقال نمی‌یابد [۱۰].

مثال، مشخص می‌کند که با چه مقدار مواد اولیه، چه مقدار خروجی کالای تولیدشده داشته باشند (احمدی مرادی، ۱۴۰۰: ۴۸).

طرح مثالی راجع به چیستی داده‌های ابزار و ماشین‌های فعال با اینترنت اشیا، به تفهیم مطلب کمک می‌کند. به عنوان نمونه در یک زمین کشاورزی به وسیله ابزاری یا تراکتوری که در آنجا به کار گرفته می‌شود، هر چند روز، از رطوبت خاک، کیفیت رشد گیاه، دمای هوا و غیره اطلاعاتی بدست می‌آید. پرسش این است که آیا مالک داده‌هایی که از طریق آن وسیله، تحصیل می‌شود، از آنِ پردازنده‌ای است که مرتبط با اینترنت اشیا می‌باشد یا افراد و اشخاص حقیقی و حقوقی که عنوان کنترل‌کننده را دارا می‌باشند و یا برای خود آن شیئ و برنامه‌ای که با تکنولوژی اینترنت اشیاء کار می‌کند؟

مالکیت به رابطه مستقیمی گفته می شود که بین شخص با شیء (اعم از مادی و غیرمادی) وجود دارد. درصورتیکه شخصی این رابطه را از راه صحیح به دست آورده باشد، قانون آن را معتبر می‌شناسد و مورد حمایت قرار می‌دهد. طبق ماده ۲۹ قانون مدنی ممکن است اشخاص نسبت به اموال علاقه‌هایی مانند مالکیت (اعم از عین یا منفعت) داشته باشند. طبق این علقه، علاوه‌بر حق کنترل داده که می‌تواند ناشی از همین مالکیت باشد، افراد نسبت به داده‌های خود در بستر اینترنت اشیا حق مالکیت دارند. ضمن اینکه در اینترنت اشیاء به دلیل آنکه پردازشگر دارای وصف خود مختاری نیست و این کنترل کننده است که نسبت به داده‌های اینترنت اشیا آگاهی دارد، لذا نمی‌توان خودِ شیئ و برنامه‌ی اینترنت اشیاء و بطور دقیق‌تر پردازش‌گر داده پیام‌ها را مالک داده‌ها قلمداد کرد. در واقع در اینترنت اشیا طبق خط مشی نوشته شده توسط کنترل کننده، آن برنامه دارای کارکردی مشخص است و غیر از آن، فعالیت مازاد و غیرقابل پیش‌بینی دیگری ندارد.

در ابزارهایی که متصل به اینرنت اشیا می‌باشند، آن وسیله و شیئ صرفا داده‌هایی که طبق برنامه‌ی نوشته شده، از او خواسته شده است را دریافت کرده و به کنترل‌کننده انتقال می‌دهد و اصولاً اقدامی افزون بر مورد یا موارد پیش‌بینی شده انجام نمی‌دهد و مانند هوش مصنوعی، واجد وصف خودمختاری در تولید داده‌ها نیست و تنها گزارشی از واقعیتی که از محیط پیرامون خود دارد، به کنترل کننده ارسال می‌دارد و کنترل کننده نیز به فرایندی که طی می‌شود، واقف است و با واکنش بدیع و خلاف انتظاری مواجه نمی‌شود. ازاین‌رو به نظر می‌رسد در ابزارهای متصل به اینترنت اشیاء، مالک داده‌های ارسالی از سوی شیئ، همان برنامه نویس، طراح و کنترل کننده‌ای است که این اطلاعات مستقیماً برای او فرستاده می‌شود. بله، مالکیت خودِ شیئ برای متصرف (خریدار) و دارنده‌ی آن است، مثل یک ماشین کشاورزی متصل به اینترنت اشیاء که شخص کشاورز آن را خریداری نموده ولی داده‌هایی که به موجب برنامه‌ی نصب شده بر روی ماشین به کنترل کننده ارسال می‌گردد، از آنِ همان برنامه نویس و کنترل کننده‌ای است که با دریافت این داده‌ها و اطلاعات، کشاورز و مالک ماشین را در چگونگی ادامه‌ی فعالیت‌های مربوط به زراعت و به منظور تحقق برآیندی مطلوب و با منفعتی بیشتر، راهنمایی می‌کند. البته چنانچه همان وسیله، هم زمان متصل به اینترنت اشیا و هوش مصنوعی باشد، باید برای شناسایی مالک داده‌ی ایجادی، دست به تفکیک زد و پاسخ این تفکیک با توجه به آنچه ذکر شد، برای خواننده ارجمند روشن است.

در پایان ذکر این نکته ضروری است که کنترل‌کننده و پردازش‌گر هنگام دریافت و پردازش داده‌های

دریافتی، باید اطلاعات شخصی اشخاص را حفظ کرده و مفاد مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی را رعایت نمایند.

۷ نتیجه‌گیری

دانسته شد از آنجا که هوش مصنوعی (هم در رویکرد ضعیف و هم در رویکرد قوی) دارای وصف خودمختاری است و داده‌های حاصل از آن، کاملاً غیرقابل پیش‌بینی و خارج از کنترل سازنده‌اش است، چنانچه برای آن قائل به وجود شخصیتی مستقل شد (شخصیت اعتباری یا واقعی)، براین‌اساس به نظر می‌رسد بتوان هوش مصنوعی را مالک آفرینه‌هایش دانست. این نتیجه با تفسیری که از بند «م» ماده ۲ قانون تجارت الکترونیکی به عمل آمد و نیز باتوجه به قسمت اخیر بند «الف» ماده اول آیین نامه اجرایی ماده ۲۱ قانون سال ۱۳۴۸ و به کاربردن لفظ «شخص» در تعریف پدیدآورنده نرم‌افزار ذیل ماده ۳ آیین نامه‌ی اجرایی ماده ۲ و ۱۷ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای، تقویت می‌شود.

ولی در اینترنت اشیا، چون داده‌های ارسالی، اصولاً همان مواردی است که برنامه نویس آنها را پیش‌بینی کرده است و کنترل کننده نیز به فرایندی که طی می‌شود، واقف است و با واکنش خلاف انتظاری مواجه نمی‌شود، ازاین‌رو به نظر می‌رسد در این‌گونه از وسایل و ابزارهایی که متصل به اینترنت اشیاء می‌باشند، مالک داده‌های ارسالی از سوی شیئ، همان برنامه نویس، طراح و کنترل کننده‌ای است که این اطلاعات مستقیماً برای او فرستاده می‌شود.

با اینحال قوانین فعلی ایران در این زمینه صراحتی ندارند و ضروری است باتوجه به پیشرفت روزافزون این فناوری‌ها و گسترش استفاده از آنها، مقنن در موضوعات مزبور با کمک از حقوقدانان و کارشناسان ذی‌ربط، اقدام به قانونگذاری نماید و خلاءهای موجود را از طریق تقنین بر طرف کند.

مراجع

[۱] ولی‌پور، علی؛ اسماعیلی، محسن، امکان‌سنجی مسئولیت مدنی هوش مصنوعی عمومی ناشی از ایجاد ضرر در حقوق مدنی، اندیشه حقوقی، ۲(۶)، ۱-۱۶، ۱۴۰۰.

[۲] کچوئی، پریسا، وضعیت مالکیت آثار حاصل از هوش مصنوعی (پایان نامه ارشد؛ به راهنمایی، انصاری، باقر)، تهران: دانشگاه شهید بهشتی، ۱۳۹۹، صص ۶۹، ۵۷، ۲۳، ۷۰، ۷۱ و ۲۵.

[۳] رجبی، عبداله. «ضمان در هوش مصنوعی» مطالعات حقوق تطبیقی، ۱۰(۲)، ۱۳۹۸، صص ۴۵۵، ۴۶۲.

[۴] ایرانشاهی، علیرضا؛ محمودی، اصغر؛ ملکی، حسین. «مبنای مسئولیت مدنی اینترنت اشیاء»، فصلنامه تحقیقات حقوقی، ۲۵ (ویژه‌نامه حقوق و فناوری)، ۱۴۰۱، ص ۲۲۲.

[۵] گندمکار، رضا حسین؛ صالحی مازندرانی، محمد؛ حمیدی، محمد مهدی. بررسی تطبیقی امکان وجود شخصیت حقوقی برای سامانه‌های هوشمند در فقه امامیه، حقوق ایران و حقوق غرب. پژوهش تطبیقی حقوق اسلام و غرب، ۸(۴)، ۱۴۰۰، صص ۲۴۰، ۲۴۶، ۲۴۷، ۲۴۸، ۲۴۹، ۲۵۱ و ۲۶۱.

[۶] تخشید، زهرا، «مقدمه‌ای بر چالش‌های هوش مصنوعی در حوزه مسئولیت مدنی»، مجله علمی «حقوق خصوصی»، ۱۸(۱)، ۱۴۰۰، ص ۲۳۴.

[۷] السان، مصطفی، حقوق تجارت الکترونیکی، چ ۱، تهران: انتشارات سمت، ۱۳۹۱، ص ۳۷.

[۸] زرکلام، ستار؛ نظام‌الملکی، جعفر؛ طلوع، سید محسن، «تحلیل و ارزیابی حمایت از نرم‌افزار در نظام حقوق مالکیت فکری و نظام متن‌باز»، دوفصلنامهٔ علمی حقوق تطبیقی، ۳(۲)، ۱۳۹۵، صص ۳-۲۸.

[۹] حبیب‌زاده، طاهر، «چالش‌های حقوقی اینترنت اشیاء (Internet of Thing) و اینترنت همه چیز (Internet of Every things)»، قابل دسترسی در وب‌سایت: http://drhabibzadeh.com، ۱۳۹۹.

[۱۰] کاتوزیان، ناصر، حقوق مدنی – اموال و مالکیت، چاپ اول، تهران: نشر یلدا، ۱۳۷۴، صص ۲۹، ۳۰، ۲۶.

[۱۱] قاسمی، روح الله و دیگران، «اولویت‌بندی کاربردهای فناوری اینترنت اشیا در بخش بهداشت و درمان ایران: محرکی برای توسعه پایدار»، تهران: مدیریت فناوری اطلاعات - شماره ۲۶، ۱۳۹۵.

[۱۲] آقایی طوق مسلم، ناصر مهدی. چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایران و اتحادیه اروپا. حقوق اداری. ۱۳۹۹؛ ۷ (۲۳)، صص ۳۳-۵۵.

[۱۳] صفار،محمد جواد، شخصیت حقوقی، چاپ اول، تهران، انتشارات دانا، ۱۳۷۳.

[۱۴] مرتضوی، سیدضیاء، «مبانی و ادله اعتبار شرعی شخصیت حقوقی»، فقه و اصول، ش۲، ۱۳۹۳، ص ۱۷.

[۱۵] زرکلام، ستار؛ محوری، حمایت های حقوقی از پدیدآورندگان نرم‌افزار، چاپ اول، تهران: سمت، ۱۳۹۴.

[۱۶] وحدت، داود، اینترنت اشیاء، تهران: انتشارات آتی‌نگر، ۱۳۹۶، ص ۸.

[17] Fjeld, J., Achten N., Hilligoss, H., Nagy, A., & Srikumar, M. “Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI”, Berkman Klein Center for Internet & Society, 2020.

[18] Gary Yang, “The History of Artificial Intelligence, History of Computing CSEP 590A”, University of Washington, 2006, p 17.

[19] Cerka, Paulius, Jurgita Grigiene & Gintare Sirbikyte, “Is it possible to grant legal personality to artificial intelligence software systems?”, Computer Law & Security Review, 33, 2017.

[20] Kelnar, D. The fourth industrial revolution: a primer on Artificial Intelligence, 2017. https://medium.com/mmc-writes/the-fourth-industrial-revolution-a-primer-on-artificial-intelligence-ai-ff5e7fffcae1

[21] Copeland, B.J., Britannica, Artificial Intelligence, 2020. https://www.britannica.com/technology/artificial-intelligence

[22] Tom allen and robin widdison, “can computer make contracts?”, Harward journal of law and technology, vol.9, no 1, 1996, P 26.

[23] Wildhaber, Isabelle & Melinda Florina Müller, “Roboterrecht – eine Einleitung”, PJA 2, 2017, p 13.

[24] Lawrence B. Solum, “legal personhood for artificial intelligence”, north Carolina law review, volume70,article 4, 1992.

[25] Kerr I, «Providing for autonomous electronic devices in the Uniform Electronic Commerce Act». In: Proceedings of the uniform law conference of Canada, 1999, https://www.ulcc.ca/en/1999-winnipeg-mb/359-civil-section-documents/362-providing-for-autonomous-electronic-devices-in-the-electronic-commerce-act-1999

[26] Filipe Maia Alexandre, "The Legal Status of Artificially Intelligent Robots Personhood, Taxation and Control", Degree of Master of Laws, under the supervision of Prof. Erik Vermeulen, Tilburg University, 2017, p 20.

[27] Weitzenböck, Emily M, Electronic Agents and Contract Performance: Good Faith and Fair Dealing, 2003, p 4-5: http://www.cirsfid.unibo.it/~agsw/lea02/pp/pdf

[28] Haristov, Kalin, Artificial Intelligence and Copyright Dilemma, 2017, 38-32.

[29] Morgrethe, Helen, Bohler, EU Copyright Protection of Works Created by Artificial Intelligence, University of Bergen, June 2017, p 22.

[30] Jenna Lindqvist, New challenges to personal data processing agreements: is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things?, International Journal of Law and Information Technology, 2017, Downloaded from https://academic.oup.com/ijlit/advancearticleabstract/doi/10.1093/ijlit/eax024/4769343

[31] Chimuka, Garikai, Impact of Artificial Intelligence on Patent Law. Towards an analytical framework – [the multi-level model], 2019.

[32] Pollaud - Dulian Frederic, Le droit d'auteur, (corpus pour droit prive). Economica, 2005.

فراسوی GPS: موقعیت‌یابی بصری، سیستم مسیریابی مقاوم به تغییرات جغراسیاسی

عارف برهانی [۱]، کاظم فولادی قلعه [۲]، احسان رزاقی‌زاده [۳]

[۱] دانش‌آموخته مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
rf.borhani@gmail.com
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
kfouladi@ut.ac.ir
[۳] متخصص حوزه یادگیری ماشینی و بینایی ماشین، تهران
ehsanrazaghizade22@gmail.com

چکیده

وابستگی فزاینده به سیستم موقعیت یاب جهانی (GPS) برای مسیریابی، یک آسیب‌پذیری بحرانی را در کاربردهای مختلف نشان داده است، به خصوص زمانی که سیستم‌های مسیریابی سنتی، مانند GPS، به‌دلیل عوامل مختلفی از جمله دستکاری سیگنال، سیگنال‌دهی ضعیف و موارد دیگر در دسترس نیستند. در پاسخ به این چالش، این مقاله پتانسیل «موقعیت‌یابی بصری» را به عنوان یک راه‌حل مسیریابی جایگزین بررسی می‌کند که در برابر محدودیت‌های جغراسیاسی و دستکاری سیگنال قابل اتکا است. هدف این مقاله ارائه یک مرور جامع از تحقیقات موقعیت‌یابی بصری و بررسی قابلیت‌های آن در استفاده به‌عنوان یک راهکار مسیریابی قابل اعتماد است. این مقاله چالش‌ها و محدودیت‌های سیستم‌های کنونی مبتنی بر GPS، اصول و تکنیک‌های زیربنایی اودومتری بصری، و پیشرفت‌های اخیر در این زمینه را مورد بحث قرار می‌دهد. علاوه بر آن، این مقاله نتایج شبیه‌سازی‌های نشان‌دهنده اثربخشی موقعیت‌یابی بصری در سناریوهای مختلف دنیای واقعی را ارائه و ظرفیت آن را به‌عنوان یک جایگزین مناسب برای سیستم‌های مسیریابی مبتنی بر GPS برجسته می‌کند.

کلمات کلیدی: بینایی ماشین، مسیریابی، موقعیت‌یابی بصری (VO)، سیستم موقعیت‌یاب جهانی (GPS).

۱ مقدمه

در دنیای به سرعت در حال تحول امروزی، فن‌آوری مسیریابی نه تنها در زندگی روزمره ما، بلکه در کاربردهای حیاتی مانند عملیات‌های نظامی، پاسخ به بلایای طبیعی و خودروهای خودران نیز نقش محوری ایفا می‌کند.

در حالی که GPS (سیستم موقعیت‌یابی جهانی[1]) فناوری پیشگام برای مسیریابی دقیق بوده است، اما این سیستم بدون آسیب‌پذیری نیست [۱]. این مقاله به یک راه‌حل مسیریابی نوظهور به نام موقعیت‌یابی بصری می‌پردازد و بررسی می‌کند که چگونه این فناوری می‌تواند نسبت به اتفاقات جغراسیاسی[2] مقاومت و قابلیت اطمینان فراهم کند و یک بازیگر مهم در زمینه فناوری مسیریابی باشد.

اودومتری بصری[3]، که اغلب به آن VO گفته می‌شود، فناوری‌ای است که خودروها را قادر می‌سازد تا موقعیت و جهت خود را از طریق تجزیه و تحلیل داده‌های بصری دوربین‌های متصل تعیین کنند [۱]. برخلاف سیستم‌های GPS سنتی که به سیگنال‌های ماهواره‌ای متکی هستند، VO از الگوریتم‌های بینایی کامپیوتری برای ردیابی و تفسیر نشانه‌های بصری از محیط اطراف استفاده می‌کند. این نشانه‌ها ممکن است شامل ویژگی‌هایی مانند علائم جاده، ساختمان‌ها و دیگر وسایل نقلیه در جاده باشند [۷].

در حالی که GPS برای سال‌ها یک ابزار قابل اعتماد برای مسیریابی بوده است، محدودیت‌های خاصی دارد که موقعیت‌یابی بصری به دنبال رفع آن‌ها است. در ادامه مزایای استفاده از موقعیت‌یابی بصری در سیستم‌های مسیریابی خودرو بررسی می‌شود:

- **تاب‌آوری جغراسیاسی:** یکی از مهم‌ترین مزایای موقعیت‌یابی بصری انعطاف‌پذیری آن است. برخلاف GPS که به شبکه‌ای از ماهواره‌ها متکی است که می‌توانند توسط دولت‌های محلی مختل یا کنترل شوند، موقعیت‌یابی بصری به‌طور مستقل عمل می‌کند. این استقلال آن را در برابر مناقشات جغراسیاسی و کشمکش‌های قدرت مصون می‌کند و عملکرد پایدار آن را حتی در زمان‌های پرتلاطم تضمین می‌کند.

- **ثبات در محیط‌های چالش‌برانگیز:** اتکای موقعیت‌یابی بصری به داده‌های بصری، آن را در محیط‌های چالش برانگیز بسیار قوی می‌کند. این سیستم می‌تواند در داخل خانه، زیرِ زمین یا در مناطقی که دسترسی به سیگنال‌های ماهواره‌ای ممکن نیست، عمل کند. این برتری موقعیت‌یابی بصری را برای کاربردهایی مانند ناوبری داخلی، ربات‌های خودمختار و عملیات استخراج زیرزمینی ایده‌آل می‌کند [۲۷].

- **حفظ بهتر حریم خصوصی:** نگرانی‌های حریم خصوصی مرتبط با ردیابی GPS به‌طور قابل توجهی با موقعیت‌یابی بصری کاهش می‌یابد. از آنجایی که این سیستم به سنسورها و دوربین‌ها متکی است، نیازی به انتقال داده‌های موقعیت به سرورهای خارجی نیست و کنترل بیشتری بر روی حریم خصوصی کاربران فراهم می‌کند [۲۷].

همچنان که در دنیا به جلو حرکت می‌کنیم، محدودیت‌های GPS آشکارتر می‌شوند. موقعیت‌یابی بصری به عنوان یک جایگزین قابل اعتماد ظاهر می‌شود که نه‌تنها این محدودیت‌ها را مورد توجه قرار می‌دهد بلکه مزایای بیشتری از نظر انعطاف پذیری جغراسیاسی، قابلیت اطمینان و حریم خصوصی ارائه می‌دهد.

[1] Global Positioning System
[2] Geopolitical
[3] Visual Odometry

بخش اول مقاله (مقدمه)، نگرانی‌های رو به رشد مربوط به وابستگی به GPS در حوزه‌های مختلف را برجسته می‌کند و بر نیاز به راه‌حل‌های مسیریابی مستقل تاکید می‌کند. بخش دوم (مرور ادبیات) به‌طور منتقدانه پژوهش‌های اخیر در حوزه موقعیت‌یابی بصری را بررسی می‌کند و بینش‌هایی را در مورد پیشرفت در الگوریتم‌های VO، فناوری‌های حسگر و کاربردهای آنها ارائه می‌دهد. بخش سوم (سیستم پیشنهادی) یک مدل نوآورانه VO را معرفی می‌کند و اصول آن و نحوه یکپارچه‌سازی حسگرها را توضیح می‌دهد. در بخش چهارم (تحلیل و ارزیابی)، به جزئیات روش‌های استفاده شده برای ارزیابی عملکرد مدل می‌پردازیم و با استفاده از دو مجموعه داده متفاوت، عملکرد آن در سناریوهای دنیای واقعی را نشان می‌دهیم. درنهایت در بخش آخر (نتیجه‌گیری)، یافته‌های کلیدی را خلاصه می‌کنیم، بر پتانسیل موقعیت‌یابی بصری به‌عنوان یک راه‌حل مسیریابی انعطاف‌پذیر تاکید می‌کنیم و حوزه‌هایی را برای تحقیقات آینده پیشنهاد می‌دهیم.

۲ کارهای مشابه

ژان و ویراسکرا [۱۸] در پژوهش خود در مورد ترکیب یادگیری عمیق با هندسه اپیپولار در موقعیت‌یابی بصری بحث می‌کنند. آنها دو شبکه عصبی کانوولوشنال را برای تخمین عمق‌های تک-نما و جریان‌های نوری دو-نما آموزش دادند. تحقیقات آنها منجر به توسعه یک الگوریتم قدرتمند اودمتری بصری فریم به فریم به نام DF-VO می‌شود که عملکرد بهتری نسبت به روش‌های دیگر دارد و از مسائل شناوری مقیاس جلوگیری می‌کند.

لایدار فناوری‌ای است که از لیزر برای اندازه‌گیری فواصل و ایجاد نقشه‌های سه‌بعدی دقیق از اشیا و محیط استفاده می‌کند [۲۸]. هانگ و ما [۱۹] در مقاله‌ی خود یک روش جدید با ترکیب موقعیت‌یابی بصری و لیدار معرفی می‌کنند که ویژگی‌های نقطه و خط را برای بهبود تخمین جایگاه دوربین ترکیب می‌کند. این روش شامل یک رویکرد قدرتمند برای استخراج عمق نقطه‌ای و خطی و افزایش دقت می‌باشد. موقعیت‌یابی بصری داده محور در صنایع مختلفی کاربرد دارد اما اغلب فاقد اطلاعات عدم قطعیت حیاتی برای اطمینان‌پذیری کامل است. در این مقاله کوستانت و مانیچی [۲۰] شبکه عصبی عمیق جدیدی به نام UA-VO طراحی می‌کند که جایگاه فعلی دوربین را تخمین می‌زند و برای هر تخمین معیارهای عدم قطعیت را محاسبه می‌کند.

دوربین‌های مبتنی بر رویداد به سرعت تغییرات روشنایی سطح پیکسل در یک صحنه را ثبت می‌کنند که شبیه به نحوه تشخیص حرکت چشم انسان است و پردازش اطلاعات بصری با سرعت بالا و دقیق را ممکن می‌کند [۲۸]. ژو و گالگو [۲۱] در مقاله خود یک راه‌حل برای موقعیت‌یابی بصری بلادرنگ با استفاده از دوربین‌های مبتنی بر رویداد استریو معرفی می‌کنند. رویکرد پیشنهادی این مقاله، سازگاری مکانی - زمانی را در داده‌های رویداد به حداکثر می‌رساند و بازسازی کارآمد صحنه سه‌بعدی و تخمین جایگاه دوربین را ممکن می‌سازد. این سیستم در شرایط نوری چالش‌برانگیز به‌خوبی کار می‌کند و به صورت متن‌باز برای تحقیق در حوزه مکان‌یابی و نقشه‌برداری همزمان مبتنی بر رویداد در دسترس است.

۳ روش پیشنهادی

۱.۳ اودومتری بصری

موقعیت‌یابی بصری فرایند تخمین حرکت ربات (جابجایی و چرخش نسبت به یک محور مرجع) با مشاهده توالی تصاویر محیط آن است [۷]. در واقع موقعیت‌یابی بصری یک مورد خاص از تکنیکی به نام ساختار از حرکت (SFM) است که مسئله بازسازی سه‌بعدی ساختار محیط و جایگاه دوربین در تصاویر متوالی یا بدون ترتیب را حل می‌کند [۱]. مرحله بهبود نهایی و بهینه‌سازی سراسری جایگاه دوربین و ساختار در SFM هزینه محاسباتی بالایی دارد و معمولاً به‌صورت آفلاین انجام می‌شود. با این حال، تخمین جایگاه دوربین در موقعیت‌یابی بصری باید در لحظه انجام شود.

در سال‌های اخیر، روش‌های VO بسیاری پیشنهاد شده‌اند که می‌توان آنها را به روش‌های دوربین یک چشمی [۲] و دو چشمی [۳] تقسیم کرد. همچنین این روش‌ها به تطبیق ویژگی (تطبیق ویژگی‌ها در تعدادی از فریم‌ها) [۴]، ردیابی ویژگی [۵] (تطبیق ویژگی‌ها در فریم‌های مجاور)، و تکنیک‌های جریان نوری [۶] (براساس شدت تمام پیکسل‌ها یا مناطق خاص در تصاویر متوالی) تقسیم می‌شوند. موقعیت‌یابی بصری پس از استفاده موفقیت‌آمیز در عملیات اکتشاف مریخ توسط ناسا شناخت عمومی به‌دست آورد [۹]. این دستاورد بر کاربرد عملی قابل توجه آن در حوزه‌های مختلف از جمله امنیت عمومی [۸]، واقعیت مجازی [۱۰] و واقعیت افزوده [۱۱] تأکید کرد.

برای اطمینان از عملکرد مناسب اودومتری بصری، روشنایی کافی و یک محیط ایستا و دارای بافت کافی مورد نیاز هستند [۱۳]. در مناطقی با سطوح صاف و کم بافت، نور جهت دار و شرایط روشنایی خاص منجر به نورپردازی غیریکنواخت صحنه می‌شوند [۱۲]. علاوه بر این، سایه‌های اشیا ساکن یا متحرک، از جمله خود وسیله نقلیه، می‌توانند محاسبات جابجایی پیکسل را مختل کرده و به تخمین‌های نادرستی منجر شوند [۱۴،۱۵].

۲.۳ مدل پیشنهادی

در این مقاله، ما یک مدل موقعیت‌یابی بصری را پیشنهاد می‌کنیم که ORB، FLANN و LSH بهره می‌گیرد تا جایگزینی برای سیستم‌های مبتنی بر GPS در ناوبری خودرو ارائه دهد. این مدل شامل سه بخش اصلی است: استخراج ویژگی، تطبیق ویژگی، و مثلث‌بندی.

بخش استخراج ویژگی این مدل از الگوریتم ORB برای استخراج حداکثر ۳۰۰۰ ویژگی از تصاویر ورودی استفاده می‌کند. ORB یک الگوریتم سریع و کاربردی است که یابنده نقاط کلیدی FAST و استخراج‌گر توصیف‌گر BRIEF را ترکیب می‌کند و روشی قوی و کارآمد برای شناسایی ویژگی‌ها در تصاویر فراهم می‌کند [۱۶].

پس از استخراج ویژگی‌ها از تصاویر ورودی، مدل ما از الگوریتم FLANN برای تطبیق ویژگی‌های استخراج شده بین فریم‌های مجاور استفاده می‌کند. FLANN یک الگوریتم کارآمد برای جستجوی تقریبی نزدیک‌ترین همسایه است، که به‌ویژه برای فضاهای ویژگی با ابعاد بالا مناسب است [۱۶]. در این مدل، ما

از LSH برای بهبود کارایی فرآیند تطبیق ویژگی استفاده می‌کنیم. LSH یک تکنیک هش‌کردن است که با نگاشت ویژگی‌های مشابه به یک سطل هش مشترک، به جستجوی تقریبی نزدیک‌ترین همسایگان کمک می‌کند [۱۷].

هنگامی که ویژگی‌ها بین فریم‌های مجاور تطبیق داده شدند، مدل ما از مثلث‌بندی برای تخمین ژست دوربین استفاده می‌کند. مثلث‌بندی تکنیکی است که شامل تخمین موقعیت سه‌بعدی یک نقطه با اندازه‌گیری افکنش[۴] آن بر روی دو یا چند تصویر گرفته شده از دیدگاه‌های مختلف است [۱۶]. با مثلث‌بندی ویژگی‌های منطبق، مدل ما می‌تواند حرکت نسبی دوربین بین فریم‌ها را بازیابی کند و نقشه‌ای از محیط بسازد.

۴ تحلیل و ارزیابی

ارزیابی مناسب پروژه در موقعیت‌یابی بصری مزایای متعددی دارد، مانند بهبود دقت، افزایش ثبات و سازگاری. ارزیابی و بررسی الگوریتم‌ها می‌تواند منجر به تخمین جایگاه دقیق‌تر شود که برای کاربرد مد نظر ما حیاتی است [۱۲، ۲۵]. ارزیابی مناسب همچنین می‌تواند به شناسایی نقاط قوت و ضعف روش‌های مختلف موقعیت‌یابی بصری کمک کند، که منجر به توسعه الگوریتم‌های قابل اعتمادتر می‌شود که می‌تواند از پس محیط‌های چالش برانگیز، مانند روشنایی‌های متغیر، اشیا پویا، و هم‌پوشانی‌ها برآید [۲۶]. جذر میانگین مربعات خطا (RMSE) یک معیار پرکاربرد برای ارزیابی دقت پیش‌بینی‌های یک مدل است که با محاسبه‌ی ریشه دوم میانگین مربعات اختلاف بین مقادیر پیش بینی شده و مقادیر حقیقی به‌دست می‌آید. مقدار پایین‌تر RMSE به معنی دقت بهتر است اما این معیار نسبت به داده‌های پرت حساس بوده و ممکن است جهت خطا را مشخص نکند [۲۲].

مجموعه داده KITTI یک شاخص ارزیابی پرکاربرد برای مسائل بینایی ماشین و رانندگی خودکار است [۲۳]. یکی از مزیت‌های اصلی این مجموعه داده، داده‌های متنوع و واقع گرایانه آن است که به محققان کمک می‌کند تا الگوریتم‌هایی که توسعه داده‌اند را آزمایش کنند و می‌تواند به‌خوبی سناریوهای دنیای واقعی را تعمیم دهد [۲۴].

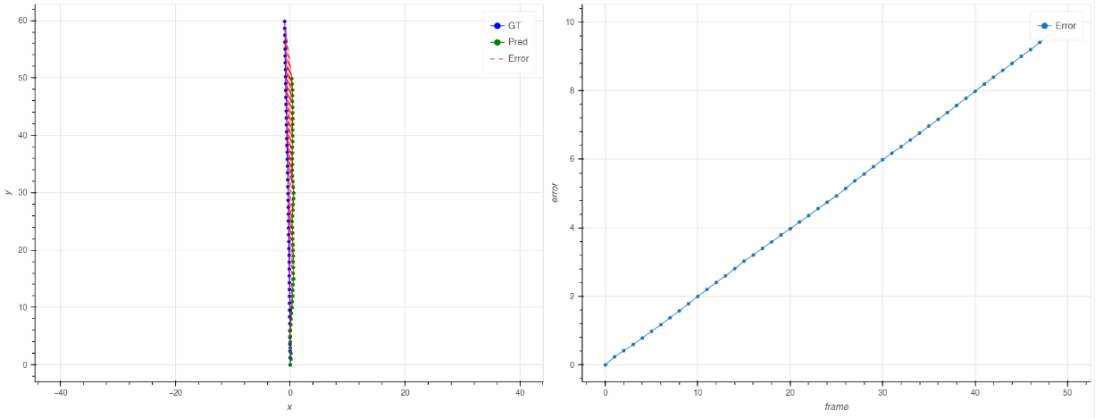
هدف اصلی ما انتخاب دقیق توالی‌های خاصی از مجموعه داده KITTI بود که شامل هر دو مسیر مستقیم و منحنی باشد. این توالی‌ها براساس شباهت آن‌ها با سناریوهای دنیای واقعی انتخاب شدند که تا تمرکز خود را روی سناریوهایی که با شرایط رانندگی واقعی مطابقت دارند قرار دهیم و اعتبار و کاربرد این پژوهش را افزایش دهیم.

۱.۴ عملکرد در مسیر صاف

در توالی اول، مدل در تخمین موقعیت دوربین سطح قابل قبولی از دقت نشان می‌دهد و محاسبات آن نتایجی را به‌دست می‌دهد که بسیار نزدیک به مقادیر واقعی هستند. با این حال، همان‌طور که عملکرد مدل در طول زمان بررسی می‌شود، یک روند نگران‌کننده پدیدار می‌شود: دقت تخمین‌های این مدل به‌تدریج کاهش

[4] projection

شکل ۱: نمونه‌ای از تصاویر موجود در مجموعه داده KITTI، تصویر مربوط به توالی اول این مجموعه داده است.



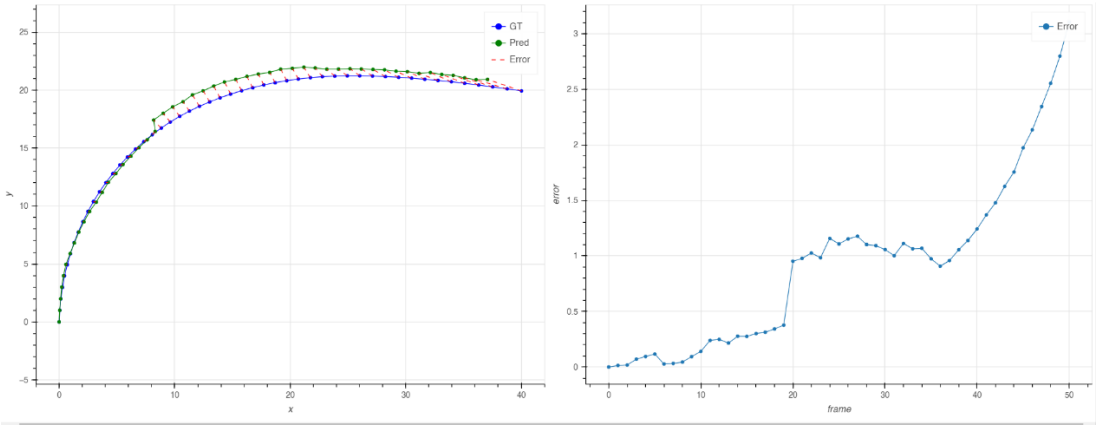
ب) الف)

شکل ۲: الف) نمودار تغییر مقدار RMSE در فریم‌های توالی اول. ب) مقایسه مسیر پیش‌بینی شده توسط مدل(سبز) و مسیر حقیقی (آبی)

می‌یابد و منجر به خطای قابل توجهی می‌شود.

وقتی در نهایت به انتهای مسیر می‌رسیم، متوجه می‌شویم که خطای عمودی (انحراف دوربین در جهت جانبی) نسبتاً کوچک است و اندازه آن کمتر از یک متر است. این نتیجه یک دستاورد قابل توجه است که نشان‌دهنده توانایی مدل برای حفظ دقت در بعد عمودی است. با این حال، وضعیت وقتی که خطای افقی (انحراف دوربین در جهت حرکت) مورد بررسی قرار می‌گیرد متفاوت است. در اینجا، عملکرد مدل پایین‌تر است و خطا از ۱۰ متر فراتر می‌رود (شکل ۲).

مدل‌های موقعیت‌یابی بصری به نشانه‌های بصری از محیط برای تخمین حرکت دوربین متکی هستند. اگر محیط بسیار پویا باشد، با تغییر سریع شرایط نوری، اشیا در حال حرکت، یا همپوشانی، ممکن است مدل برای ردیابی دقیق ویژگی‌ها به مشکل برخورد کند. این تغییرپذیری محیطی می‌تواند خطاهایی را در



الف)　　ب)

شکل ۳: الف) نمودار تغییر مقدار RMSE در توالی دوم. ب) مقایسه مسیر پیش‌بینی شده توسط مدل(سبز) و مسیر حقیقی (آبی)

تخمین‌های مدل ایجاد کند، زیرا تلاش می‌کند تا ورودی‌های بصری همیشه در حال تغییر را درک کند.

۲.۴ عملکرد در مسیر خمیده

در توالی دوم، دوربین روی ماشینی قرار می‌گیرد که مسیر منحنی مشخصی را دنبال می‌کند. در این توالی، مدل سطح بالایی از دقت را در تخمین مختصات فضایی و جهت گیری دوربین از خود نشان می‌دهد (شکل ۳).

زمانی که دوربین مسیر خود را کامل می‌کند، این مدل موفق شده خطای عمودی را به کمتر از یک متر کاهش دهد که دستاوردی با دقت چشمگیر است. علاوه بر این، خطای افقی نیز به طور قابل ملاحظه‌ای کاهش داده شده و کمتر از ۳ متر اندازه‌گیری شده است. این موقعیت‌یابی دقیق دوربین با این حد از خطا، یک دستاورد چشمگیر در زمینه مدل‌سازی محاسباتی و موقعیت‌یابی را نشان می‌دهد.

با این حال، بررسی علل عملکرد بهتر مدل در مسیرهای منحنی نسبت به مسیرهای مستقیم، بسیار مهم است. مسیرهای منحنی ذاتا پیچیدگی بیشتری را در مقایسه با مسیرهای مستقیم ایجاد می‌کنند. ممکن است مدل برای مدیریت این پیچیدگیِ بیشتر، مناسب‌تر باشد که به بهبود دقت منجر شود.

۵ نتیجه‌گیری

هدف اولیه ما در این مقاله نه تنها به چالش کشیدن وابستگی مرسوم به GPS با بررسی قابلیت‌های ساختارشکنانه موقعیت‌یابی بصری بلکه بررسی قابلیت اعتماد این سیستم در برابر چالش‌های جغراسیاسی که ممکن است سیستم‌های سنتی GPS را مختل کنند نیز بود.

ما در طول مقاله تکامل الگوریتم‌های VO را به نمایش گذاشته و پتانسیل آن‌ها برای ارائه اطلاعات موقعیت‌یابی قابل اعتماد و دقیق نشان داده‌ایم. در ادامه، ما یک مدل جدید موقعیت‌یابی بصری را معرفی کردیم، اصول آن را توضیح دادیم و از طریق ارزیابی در مقابل دو مجموعه داده متفاوت، عملکرد آن را ارزیابی کردیم.

در حالی که مدل نوآورانه ما در آزمایش‌ها به دقت نسبتاً خوبی دست یافت، لازم به ذکر است که در برخی صنایع خاص، دقت به‌دست آمده ممکن است الزامات سخت‌گیرانه را برآورده نکند. برای رفع این چالش، استفاده از دوربین‌های استریو پیشنهاد می‌شود که می‌تواند دقت سیستم را به میزان قابل توجهی افزایش دهد. با این حال، این بهبود به قیمت بار محاسباتی بالاتر تمام می‌شود، که مستلزم استفاده از سخت‌افزار پیشرفته‌تر و در نتیجه، افزایش هزینه‌ها است.

علاوه بر این، پیشنهاد می‌شود تکنولوژی‌های جایگزین مانند LiDAR، واحدهای اندازه‌گیری اینرسی (IMUs) و دوربین‌های RGB - D برای تحقیقات بیشتر در نظر گرفته شود. این فناوری‌ها برای تکمیل یا افزایش دقت موقعیت‌یابی بصری به طرق مختلفی کاربرد دارند و راهکارهای جدیدی برای توسعه سیستم مسیریابی ارائه می‌دهند.

در نهایت، زمانی که ما دنیایی را تصور می‌کنیم که تنها به GPS وابسته نیست، تحقیقات ما راه را برای راه‌حل‌های مسیریابی انعطاف پذیرتر و سازگارتر هموار می‌کند. با استفاده از بینایی ماشین و فناوری موقعیت‌یابی بصری ما یک گام به سوی دستیابی به سیستم مسیریابی با قابل تحمل چالش‌های جغراسیاسی نزدیک‌تر می‌شویم.

مراجع

[1] Fraundorfer, F., & Scaramuzza, D. (2011). Visual odometry: Part i: The first 30 years and fundamentals. IEEE Robotics and Automation Magazine, 18(4), 80-92.

[2] Campbell, J., Sukthankar, R., Nourbakhsh, I., & Pahwa, A. (2005, April). A robust visual odometry and precipice detection system using consumer-grade monocular vision. In Proceedings of the 2005 IEEE International Conference on robotics and automation (pp. 3421-3427). IEEE.

[3] Matthies, L., & Shafer, S. T. E. V. E. N. A. (1987). Error modeling in stereo navigation. IEEE Journal on Robotics and Automation, 3(3), 239-248.

[4] Talukder, A., Goldberg, S., Matthies, L., & Ansar, A. (2003, October). Real-time detection of moving objects in a dynamic scene from moving robotic vehicles. In Proceedings 2003 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2003)(Cat. No. 03CH37453) (Vol. 2, pp. 1308-1313). IEEE.

[5] Dornhege, C., & Kleiner, A. (2006). Visual odometry for tracked vehicles. In: Proceedings of the IEEE International Workshop on Safety, Security and Rescue Robotics (SSRR). IEEE.

[6] Zhang, T., Liu, X., Kühnlenz, K., & Buss, M. (2009, October). Visual odometry for the autonomous city explorer. In 2009 IEEE/RSJ International Conference on Intelligent Robots and Systems (pp. 3513-3518). IEEE.

[7] Yousif, K., Bab-Hadiashar, A., & Hoseinnezhad, R. (2015). An overview to visual odometry and visual SLAM: Applications to mobile robotics. Intelligent Industrial Systems, 1(4), 289-311.

[8] He, M., Zhu, C., Huang, Q., Ren, B., & Liu, J. (2020). A review of monocular visual odometry. The Visual Computer, 36(5), 1053-1065.

[9] Zhu, C., He, M., Yang, S., Wu, C., & Liu, B. (2018). Survey of monocular visual odometry. Comput. Eng. Appl, 54, 20-28. (in Chinese with English abstract)

[10] Lin, S., Chen, Y., Lai, Y. K., Martin, R. R., & Cheng, Z. Q. (2016). Fast capture of textured full-body avatar with rgb-d cameras. The Visual Computer, 32, 681-691.

[11] Sharma, O., Pandey, J., Akhtar, H., & Rathee, G. (2018). Navigation in AR based on digital replicas. The Visual Computer, 34, 925-936.

[12] Aqel, M. O., Marhaban, M. H., Saripan, M. I., & Ismail, N. B. (2016). Review of visual odometry: types, approaches, challenges, and applications. SpringerPlus, 5, 1-26.

[13] Scaramuzza, D., & Fraundorfer, F. (2011). Tutorial: visual odometry. IEEE Robotics and Automation Magazine, 18(4), 80-92.

[14] Gonzalez, R., Rodriguez, F., Guzman, J. L., Pradalier, C., & Siegwart, R. (2012). Combined visual odometry and visual compass for off-road mobile robots localization. Robotica, 30(6), 865-878.

[15] Nourani-Vatani, N., & Borges, P. V. K. (2011). Correlation-based visual odometry for ground vehicles. Journal of Field Robotics, 28(5), 742-768.

[16] Lin, Y., Yang, Y., & Lin, L. (2019, December). A Device Pose Estimation Method Based on Monocular Visual Odometer. In 2019 Photonics & Electromagnetics Research Symposium-Fall (PIERS-Fall) (pp. 2109-2113). IEEE.

[17] Klüssendorff, J. H., Hartmann, J., Forouher, D., & Maehle, E. (2013, July). Graph-based visual SLAM and visual odometry using an RGB-D camera. In 9th International Workshop on Robot Motion and Control (pp. 288-293). IEEE.

[18] Zhan, H., Weerasekera, C. S., Bian, J. W., & Reid, I. (2020, May). Visual odometry revisited: What should be learnt?. In 2020 IEEE international conference on robotics and automation (ICRA) (pp. 4203-4210). IEEE.

[19] Huang, S. S., Ma, Z. Y., Mu, T. J., Fu, H., & Hu, S. M. (2020, May). Lidar-monocular visual odometry using point and line features. In 2020 IEEE International Conference on Robotics and Automation (ICRA) (pp. 1091-1097). IEEE.

[20] Costante, G., & Mancini, M. (2020). Uncertainty estimation for data-driven visual odometry. IEEE Transactions on Robotics, 36(6), 1738-1757.

[21] Zhou, Y., Gallego, G., & Shen, S. (2021). Event-based stereo visual odometry. IEEE Transactions on Robotics, 37(5), 1433-1450.

[22] Ahmad, M., Al-Mansob, R. A., Kashyzadeh, K. R., Keawsawasvong, S., Sabri Sabri, M. M., Jamil, I., & Alguno, A. C. (2022). Extreme gradient boosting algorithm for predicting shear strengths of rockfill materials. Complexity, 2022.

[23] Li, R., Wang, S., Long, Z., & Gu, D. (2018, May). Undeepvo: Monocular visual odometry through unsupervised deep learning. In 2018 IEEE international conference on robotics and automation (ICRA) (pp. 7286-7291). IEEE.

[24] Cabon, Y., Murray, N., & Humenberger, M. (2020). Virtual kitti 2. arXiv preprint arXiv:2001.10773.

[25] [25] Lim, K. L., & Bräunl, T. (2020). A review of visual odometry methods and its applications for autonomous driving. arXiv preprint arXiv:2009.09193.

[26] Zhou, S., Yang, Z., Zhu, M., Li, H., Serikawa, S., Mizumachi, M., & Zhang, L. (2022). Higher accuracy self-supervised visual odometry with reliable projection. Artificial Life and Robotics, 27(3), 568-575.

[27] Amami, M.M. (2022). The Advantages and Limitations of Low-Cost Single Frequency GPS/MEMS-Based INS Integration. Global Journal of Engineering and Technology Advances.

[28] Ibrahim, M., Akhtar, N., Jalwana, M.A., Wise, M., & Mian, A.S. (2021). High Definition LiDAR mapping of Perth CBD. 2021 Digital Image Computing: Techniques and Applications (DICTA), 01-08.

بررسی مسئولیت کاربران در فضای مجازی بر اساس قاعده اقدام

سیدرضا چوگان سنبل [۱]، مهدی طالبی چاهوکی [۲]

[۱] طلبه سطح ۲ حوزه علمیه و کارشناسی ارشد مهندسی فناوری اطلاعات و ارتباطات
chogan65@gmail.com
[۲] طلبه سطح ۲ حوزه علمیه، کارشناسی ارشد مهندسی مکانیک
mehditalebich@gmail.com

چکیده

هرگاه شخصی با آگاهی و اختیار، مالش را در معرض تلف قرار دهد، طبق قاعده فقهی اقدام، مسئولیت این کار به عهده وی خواهد بود. پس از توسعه اینترنت و گسترش فناوری‌های نوین ارتباطی، فضای مجازی به بستری برای فعالیت‌های جدید و متنوع تبدیل شده است. با توجه به اینکه در موارد متعددی، کاربران با آگاهی و اختیارخود فعالیت‌هایی در این فضا انجام می‌دهند که امکان بهره‌برداری و سوء استفاده دیگران را فراهم می‌آورد، پاسخ به این مسئله ضروری است که اگر کاربران، آگاهانه اقدام به فعالیتی نمایند که منجر به ورود زیان به ایشان گردد، آیا این اقدام می‌تواند مسئولیت زیان‌زننده را سلب نماید یا خیر. در این پژوهش با روش کتابخانه‌ای، در ابتدا به بررسی قاعده فقهی اقدام و مفاهیم مال و مالکیت در فضای مجازی به‌عنوان دو مفهوم کلیدی در قاعده مزبور پرداخته شد و سپس برخی اقدامات آگاهانه کاربران در فضای مجازی مورد بررسی قرار گرفت و در نهایت بیان گردید که هرگاه شخصی در بستر فضای مجازی اقدامی در جهت اتلاف مالش انجام دهد، مسئولیت آن به عهده خودش است و هرگاه اقدامی غیر مالی انجام دهد که مورد سوء استفاده دیگران واقع شود، نمی‌توان سوءاستفاده‌گر را از مسئولیت مبرا دانست.

کلمات کلیدی: قاعده اقدام، فضای مجازی، اقدام در فضای مجازی، مال و مالکیت در فضای مجازی، مسئولیت زیان در فضای مجازی.

۱ مقدمه

امروزه با توسعه فضای مجازی، بسیاری از فعالیت‌های روزمره مردم از فضای حقیقی به آن منتقل شده است. فضای مجازی میتواند نیازهای متنوع جامعه بشری از جمله ارتباطات، آموزش، بهداشت، خرید و فروش، سرگرمی و... را مرتفع سازد. حتی برخی از نیازهایی که در فضای حقیقی، امکان پاسخ به آنها وجود نداشته، در فضای مجازی به‌راحتی پاسخ داده می‌شوند. با توجه به حضور و فعالیت متعدد کاربرانی از اقشار مختلف جامعه، مسائل فقهی و حقوقی جدیدی ایجاد شده است که پاسخ مستدل و صحیح به این مسائل ضروری به نظر می‌رسد. یکی از این مسائل، بررسی حیطه مسئولیت کاربران در مقابل اقدامات انجام شده توسط خود در

فضای مجازی است. اگر کاربری به‌صورت آگاهانه و با اختیار اقدامی را انجام دهد که به موجب آن، از طرف دیگران ضرری به او وارد آید، آیا مسئولیت این ضرر به عهده خود کاربر است و یا ضمان متوجه افراد دیگر می‌باشد. برای پاسخ به این مسئله بایستی ابتدا قاعده فقهی اقدام، مفاهیم، ادله و حیطه اثر آن مورد توجه قرار گیرد. در فضای حقیقی، هرگاه شخصی با آگاهی و اختیار، مالش را در معرض تلف قرار دهد، طبق قاعده فقهی اقدام، مسئولیت این کار به‌عهده وی خواهد بود. اصل قاعده مزبور همواره مورد توجه فقها و حقوقدانان بوده و ادله و شرایط آن به صورت مبسوط بررسی شده است. به‌عنوان مثال می‌توان به کتب «قواعد فقه» سید مصطفی محقق داماد و «قواعد فقهیه» محمد موسوی بجنوردی اشاره نمود. همچنین مقالات متعددی در رابطه با ابعاد مختلف قاعده مزبور به رشته تحریر در آمده است که برای نمونه می‌توان به مقاله «اقدام به‌عنوان یکی از منابع مسئولیت مدنی در حقوق اسلام» نوشته محمود کاظمی و مقاله «مقایسه قاعده اقدام در فقه با قاعده رضایت زیان‌دیده در حقوق مدنی ایران» نوشته محمد شکاری و عباس تقوایی اشاره کرد. تشخیص مسئول زیان وارده به یک شخص در جایی که اقدام او در کنار عمل زیان‌زننده، در ایجاد ضرر مؤثر بوده است، در فضای مجازی نیز مبتلابه بوده و جزء مسائل مستحدثه و جدید می‌باشد. ذکر این نکته ضروری است که هرچند مال و مالکیت دو مفهوم و مؤلفه اصلی در قاعده اقدام به حساب می‌آیند و درباره موضوعاتی از قبیل مفهوم مال در فضای مجازی و مصادیق مالکیت در آن فضا تحقیقات اندکی انجام شده است که می‌توان از مقاله «بررسی فقهی حقوقی مال بودن داده‌های رایانه‌ای» نوشته عبداله بهمن پوری و همکارانش و همچنین مقاله «مالکیت در فضای مجازی از منظر فقهی» نوشته ابوالحسن حسنی نام برد، لیکن درباره تعیین مسئولیت کاربران فضای مجازی با استناد به قاعده اقدام تحقیق و پژوهش مستقل و جامعی انجام نگرفته است. لذا در پژوهش حاضر با مراجعه به کتب و مقالات مرتبط و معتبر، ماهیت قاعده اقدام در بخش اول بیان شده است. در این بخش با استفاده از ادله فقهی اثبات می‌شود، دایره شمول قاعده، بر مالی است که فرد مالکیت آن را در اختیار دارد؛ فلذا قاعده اقدام، محدود به امور مالی و مالکیتی است. در بخش دوم، بحث مال و مالکیت از منظر فقه و حقوق بررسی شده و در بخش سوم، پس از بیان مفاهیم مال و مالکیت در فضای مجازی، به طرح مصادیق اقدام در فضای مجازی و تعیین مسئولیت کاربران بر اساس قاعده اقدام، پرداخته شده است. یکی از موارد نشان‌دهنده اهمیت موضوع این است که درصورت عدم توجه به آن، ممکن است در تشخیص شخص ضامن در برخی از زیان‌های وارد شده به افراد در فضای مجازی، اشتباه رخ دهد. پژوهش حاضر برای کاربران فضای مجازی، پژوهشگران حوزه فقه و حقوق در فضای مجازی و ... قابل بهره‌برداری می‌باشد.

۲ ماهیت قاعده اقدام

در این بخش قاعده فقهیه اقدام از نظر مفهوم، ادله و شرایط مورد بحث قرار گرفته است.

۱.۲ مفهوم اقدام

برای بررسی مفهوم قاعده اقدام ابتدا الزم است معنای لغوی آن بررسی گردد و سپس معنای اصطلاحی آن که اعم از اقدام به زیان و اقدام به ضمان است، پیگیری می‌شود.

۱.۱.۲ معنای لغوی اقدام

اقدام در لغت به معنای پیش رفتن درکاری، به کاری دست زدن (معین، ۱۳۸۶، ذیل واژه اقدام)، گام برداشتن و پا پیش گذاشتن در امری (عمید، ۱۳۹۰، ذیل واژه اقدام) است. همچنین در لغت‌نامه دهخدا معانی شروع کردن، پرداختن، شجاعت کردن و دلیری کردن برای آن بیان شده است (دهخدا، ۱۳۷۷، ذیل واژه اقدام).

۲.۱.۲ معنای اصلاحی اقدام

اقدام قاعده‌ای فقهی است؛ با این بیان که هر کس در جهت ضرر مالی خود اقدامی کند، کسی به نفع او ضمان قهری یا مسئولیت مدنی نداشته و قانون از چنین کسی حمایت نمی‌کند (موسوی بجنوردی، ۱۴۰۱ق، ج ۱، ص ۹۲). استاد محقق داماد برای قاعده اقدام دو معنا را به شرح ذیل بیان نموده است:

اقدام به زیان. هرگاه شخصی با توجه و آگاهی، عملی را انجام دهد که موجب ورود زیان توسط دیگران به او گردد، واردکننده زیان، که شخص دیگری است، مسئول خسارت نخواهد بود. به این دلیل که شخص با اقدام خود موجب از بین رفتن حرمت مالش شده است. در حقیقت «اقدام» در این معنا مانعی است برای اجرای قواعد ضمان قهری از جمله قاعده احترام که قبلاً گفته شد؛ چرا که «قاعده احترام»، قاعده‌ای است برای حمایت شرع از صاحبان اموال و تردید نیست که اگر صاحب مال خودش حرمت مال خویش را ضایع سازد، مورد حمایت شرع قرار نخواهد گرفت (محقق داماد، ۱۴۰۶ق، ج ۱، ۲۲۱).

اقدام به ضمان طبق این معنا، اقدام یکی از موجبات اثبات ضمان است. در عقود معاوضی، شخص گیرنده ملتزم می‌شود در مقابل نفعی که عایدش می‌گردد، عوض بپردازد. بنابراین در عقود و معاملات صحیح، بی‌گمان التزام و تعهد به پرداخت عوض المسمی برای طرفین به موجب عقد الزام‌آور است، ولی اگر عقد فاسد باشد و طرفین یا یکی از آن دو، مال را از طرف دیگر تحویل گرفته باشد، به دلیل آن که قرارداد، مورد حمایت شرع و قانون نیست، عوض المسمی به عهده آنان نخواهد بود و اگر مال تحویل گرفته شده در ید آنان تلف شود، ضمان به مثل و قیمت مطرح می‌گردد. مستند فقهی ضمان در این حالت، اقدام بر ضمان است؛ بدین معنا که شخص گیرنده در هنگام تحویل مال قصد نداشته آن را مجاناً تحویل بگیرد، بلکه در قبال پرداخت عوض اراده تسلم کرده و اراده‌اش بر این بوده که مال در ضمان او باشد. این اراده را «اقدام بر ضمان» می‌گوییم (همان، صص ۲۲۳ و ۲۲۴).

۲.۲ ادله قاعده اقدام

ادله قاعده اقدام شامل روایات، اجماع و سیره عقلا می‌باشد که به تفصیل بیان می‌گردد:

۱) سید محمد کاظم مصطفوی یکی از ادله اعتبار قاعده اقدام را تمسک به ادله مشروعیت ضمان دانسته و بیان می‌دارد، از آنجایی که ضمان به واسطه اقدام محقق می‌شود، ادله ضمان مدرک اعتبار و مشروعیت اقدام است. این دلیل از نظر ایشان قوی‌ترین دلیل بر قاعده اقدام می‌باشد. مشروعیت ضمان نیز از ضروریات فقهی می‌باشد، تا جایی که شیخ الطائفه (رحمه الله) ضمان را بر طبق کتاب و سنت و اجماع جایز می‌داند (شیخ طوسی، ۱۳۸۷ق، ج ۲، ص ۳۲۲). واضح است که مسئولیت ضامن نسبت به مال و مسئولیت کفیل نسبت به نفس بر اساس اقدام اختیاری ضامن و کفیل و مبادرت آنها به مسئولیت مذکور محقق می‌شود. پس اقدام نقش مبدأی در تحقق ضمان و کفالت داشته و بنابراین صحت ضمان و کفالت و مشروعیت آنها کاشف قطعی از صحت اقدام و مشروعیت آن می‌باشد (مصطفوی، ۱۴۲۱ق، ج ۱، صص ۵۷ و ۵۸).

۲) طبق روایت نبوی مال مسلمان بر کسی حلال نمی‌باشد، مگر آنکه رضایت به تصرف در آن داشته باشد.[۱] مال هر مسلمانی محترم است ولی به واسطه اقدام مالک مال در جهت از بین رفتن مال توسط شخص دیگر، احترام مال از بین می‌رود. رضایت و طیب نفس مالک در راستای تصرف دیگران در مال وی بدون عوض است و به همین دلیل دلیلی برای ضمان وجود ندارد (حسینی، ۱۴۱۷ق، ج ۲، ص ۴۴۸).

۳) طبق حدیثی که در باب صلح مطرح شده است[۲] (کلینی، ۱۳۸۷، ج ۱۰، ص ۳۶۸)؛ از امام صادق (ع) درباره شخصی سؤال شد که ضامن بدهکاری شخص دیگری شده بود، سپس آن دو با هم بر مقداری مصالحه کردند. حضرت فرمود بر آن شخص چیزی نیست، جز مقداری که بر آن مصالحه شده است. بنابر روایت فوق، مضمون علیه فقط به مقدار تعیین شده در صلح، ضامن مضمون له است و ضامن بقیه آن نیست، زیرا به ضرر خود اقدام کرده است (مصطفوی، ۱۴۲۱ق، ج ۱، ص ۵۸).

۴) سیره عقلا: طبق بنای عقلا، فردی که بالغ و رشید باشد و با علم و اراده بر علیه خود اقدام و موجب ورود زیان بر مال خود را فراهم کند، در واقع اقدام مجانی بر ضرر خود کرده و احترام مال خود را از حیث ارزش ساقط نموده است. در چنین مواردی که خود شخص اقدام بر ورود ضرر بر مال خود بکند، عقلا بما هم عقلا هیچ‌گونه مسئولیتی برای شخصی که این عمل را انجام داده است، قائل نیستند و قهراً شرع هم به مقتضای قاعده ملازمه مسئولیتی را در نظر نمی‌گیرد (موسوی بجنوردی، ۱۴۰۱، ج ۱، صص ۹۶ و ۹۷).

۵) اجماع: به طور مسلم فقهای شیعه بلکه کل مسلمین در مواردی که فرد اقدام بر ضرر خویش می‌کند، قائل به ضمان نیستند و او را از ضمان قهری و مسئولیت مدنی معاف می‌دارند (همان، ج ۱، ص ۹۷).

۳.۲ موارد استناد فقها به قاعده اقدام

برخی از مواردی که فقها به قاعده اقدام استناد کرده و حکم به عدم ضمان و یا عدم ثبوت مسئولیت کیفری داده‌اند، عبارتند از (موسوی بجنوردی، ۱۴۰۱ق، ج ۱، ص ۱۰۵):

۱. زمانی که خریدار به فضولی بودن معامله عالم باشد.

۲. اقدام خریدار با علم به معیب بودن مبیع، مسقط ضمان بایع و حق خیار مشتری است.

[۱] لا یحل مال إمرئ مسلم إلا بطیب نفسه
[۲] سألت أبا عبدالله علیه السلام عن رجل ضمن علی رجل ضمانا، ثم صالح علیه؛ قال لیس له إلا الذی صالح علیه

۳. ارتداد زوجه پیش از دخول است؛ به این دلیل که ارتداد، نوعی اقدام بر ابطال مهر بوده و موجب اسقاط آن است.

۴. اسلام آوردن زن کافر است که موجب سقوط مهر می‌باشد، در صورتی که پیش از گذشتن عده شوهرش مسلمان نشود.

۵. ناشزه شدن زن است که اقدام بر اسقاط نفقه می‌باشد.

۶. اعراض از اموال است که اگر آن را دیگری تملک نماید و تلف گردد؛ به لحاظ اقدام مالکش ضامن نمی‌باشد.

۷. اقدام شخص بر ضرر مال خود یا جان و اعضا و جوارح خود با وجود هشدار و تحذیر و رسیدن هشدار به وی و امکان فرار وی.

۱.۳.۲ شرایط قاعده اقدام

امور ذیل را می‌توان به عنوان شرایط قاعده اقدام برشمرد:

۱. مالک بودن:
پیش شرط قاعده اقدام این است که فردی که اقدام به ضرر خویش کرده، باید مالک آن مال باشد. بنابراین این قاعده در مورد کسانی که مالک نیستند، جاری نمی‌شود.

۲. بالغ بودن:
فردی که اقدام به ضرر خویش می‌کند، باید عاقل باشد، بنابراین افراد نابالغ هرچند که از حق مالکیت برخوردار باشند اما اگر اقدام به ضرر خویش نمایند، نمی‌توان عامل زیان را مبرا از مسئولیت مدنی دانست.

۳. عاقل بودن:
همچنین این فرد باید عاقل باشد، پس اگر فردی که از نعمت خِرَد برخوردار نیست اقدام به ضرر خویش نماید، بازهم نمی‌توان حکم به عدم ضمان او نمود.

۴. عالم و آگاه بودن:
برخی از صاحب‌نظران در راستای تعریف قاعده اقدام، شرط آگاهانه بودن را عنوان کرده‌اند؛ بنابراین اگر فرد، بالغ، عاقل و مالک، بر اثر عدم آگاهی اقدام به ضرر خویش نماید، بازهم نمی‌توان عامل زیان را فاقد مسئولیت مدنی دانست (شکاری، تقوایی، ۱۳۹۶، ص ۶).

۴.۲ قاعده اقدام در حقوق مدنی ایران

برای تحقق مسئولیت مدنی وجود سه رکن لازم و ضروری است که عبارتند از:

۱. وجود ضرر

۲. ارتکاب فعل زیان‌بار

۳. وجود رابطه سببیت میان فعل شخص و ضرری که وارد شده است.

این سه رکن در حقیقت پایه‌های تشکیل‌دهنده مسئولیت مدنی به شمار می‌آیند به‌گونه‌ای که اگر یکی از این ارکان وجود نداشته باشند، مسئولیت مدنی محقق نخواهد شد. در مواردی که خود شخص اقدام به ضرر خویش می‌کند، یا حرمت مالش را نادیده می‌گیرد، دو رکن از ارکان مسئولیت که وجود ضرر، و فعل زیانبار باشد، تحقق یافته‌اند، اما رکن سوم که رابطه سببیت باشد، منتفی است چرا که در چنین مواردی نمی‌توان ضرر وارده را به عامل زیان نسبت داد.

به همین دلیل است که هرگاه شخصی با آگاهی به غبن فاحش، اقدام به معامله غبنی نماید نه حق خیار فسخ دارد و نه می‌تواند مطالبه خسارت نماید زیرا خودش به زیان خویش اقدام کرده است. و یا در صورتی که فردی با علم و آگاهی، مال خود را در اختیار مجنونی بگذارد و او آن را تلف کند، ضمان بر عهده مجنون نخواهد بود، زیرا صاحب مال با اقدام خویش، مالش را در معرض تلف قرار داده است (عرب احمدی، فهرستی، ۱۳۹۴).

۱.۴.۲ مصادیقی از قاعده اقدام در قانون مدنی

- ماده ۲۶۳ ق.م: هرگاه مالک، معامله را اجازه نکند و مشتری هم بر فضولی بودن آن جاهل باشد، حق دارد که برای ثمن و کلیه‌ی غرامات به بایع فضولی رجوع کند و در صورت عالم بودن، فقط حق رجوع برای ثمن را خواهد داشت.
- ماده ۱۷۸ ق.م: مالی که در دریا غرق شده و مالک از آن اعراض کرده است، مال کسی است که آن را بیرون بیاورد.
- ماده ۷۱۴ ق.م: اگر ضامن زیادتر از دین به داین بدهد حق رجوع به زیاده ندارد، مگر در صورتی که به اذن مضمون‌عنه داده باشد.
- ماده ۲۶۷ ق.م: ایفای دین از جانب غیر مدیون هم جایز است، اگر چه از طرف مدیون اجازه نداشته باشد؛ ولیکن کسی که دین دیگری را ادا می‌کند، اگر با اذن باشد حق مراجعه به او دارد والا حق رجوع ندارد.
- ماده ۴۱۸ ق.م: اگر مغبون، در حین معامله عالم به قیمت عادله بوده است، خیار فسخ نخواهد داشت.

- ماده ۱۰۸۶ ق.م: اگر زن قبل از اخذ مهر به اختیار خود به ایفای وظایفی که در مقابل شوهر دارد قیام نمود، دیگر نمی‌تواند از حکم ماده قبل استفاده کند، معذلک حقی که برای مطالبه‌ی مهر دارد ساقط نخواهد شد.
- ماده ۱۲۱۵ ق.م: هر گاه کسی مالی را به تصرف صغیر غیرممیز و یا مجنون بدهد، صغیر یا مجنون مسئول ناقص یا تلف شدن آن مال نخواهد بود.

۳ مال و مالکیت

آنچه در ادله فقهی قاعده اقدام بیان شده مربوط به اقدام یک فرد بر اموال خویش است. همچنین این اقدام دارای شرایطی بود که از جمله آن مالک بودن فرد است. لذا در اینجا ضروری است که بحث مالیت و مالکیت و تفاوت آن دو را بررسی نماییم.

۱.۳ مفهوم مال

از نظر حقوقی به چیزی مال گویند که دارای دو شرط اساسی باشد:

۱. مفید باشد و نیازی را برآورده کند، خواه این نیاز مادی باشد یا معنوی؛

۲. قابل اختصاص یافتن به شخص یا ملت معین باشد.

اشیایی مانند دریاهای آزاد، هوا و خورشید از ضروری‌ترین وسایل زندگی است ولی هیچ کس نمی‌تواند نسبت به آن ادعای مالکیت انحصاری کند، پس مال محسوب نمی‌شوند.

۱.۱.۳ مال و ارزش اقتصادی

مال به معنای مادی و محدود آن به چیزی گفته می‌شود که ارزش داد و ستد دارد و در برابر آن پول یا مال دیگر داده می‌شود. معیار تمیز این ارزش نوعی و در اختیار عرف است؛ یعنی، در بازار معادل مبلغی پول می‌باشد. این تعریف را باید از دو جهت تعدیل کرد و در رابطه مال و ارزش اقتصادی به آن توجه داشت:

۱) ارزش نتیجه رغبتی است که اشخاص برای به دست آوردن چیزی در خود احساس می‌کنند؛ خواست‌ها و نیازهای مردمی که در جامعه زندگی می‌کنند با هم شباهت دارد و از این روست که به ارزش چهره نوعی و همگانی داده‌اند؛ ولی هیچ مانعی ندارد که مالی در رابطه دو طرف قرارداد ارزش مالی داشته باشد، هرچند دیگران برای موضوع آن بهایی نپردازند؛ کافی است که انگیزه معامله عقلایی و مشروع باشد. برای مثال خرید و فروش عکس‌ها و یادگاری‌های خانوادگی صحیح می‌باشد، در حالی که احتمال دارد بازار برای آنها ارزشی قائل نباشد.

۲) مال اندک مانند یک دانه گندم، موضوع داد و ستد واقع نمی‌شود و عرف بی اعتنا از آن می‌گذرد ولی نباید چنین پنداشت که مالیت ندارد؛ به همین جهت اگر دزدی خرمن گندمی را دانه دانه برباید نمی‌گویند

بر ارزشی دست نیافته و مالی را نربوده است، وانگهی اگر دانه‌ای از گندم مالیت نداشته باشد، باید دید ارزش مجموع از کجا آمده است؟ آیا نتیجه مجموع اجزاء است یا اثر وجود ارزش در هر جزء؟ و به نظر می‌رسد هر دانه گندم هم مفید است و هم قابل تملک (کاتوزیان، ۱۳۹۲، صص ۹-۱۲).

۲.۱.۳ حق مالی و غیر مالی

حق غیرمالی امتیازی است که هدف آن رفع نیازهای عاطفی و اخلاقی انسان است وموضوع آن روابط غیرمالی اشخاص بوده و ارزش داد و ستد را ندارند و قابل ارزیابی به پول و مبادله با آن نیستند. مانند حق زوجیت، حق ولایت یا حقی که پدیدآورنده اثر ادبی یا هنری در انتشار آن دارد. غالب این حقوق غیر مالی، آثار مالی دارد؛ چنان که حق وراثت سبب می‌شود که شخص دارایی خود را تملک کند، و حق زوجیت امکان مطالبه نفقه را به دنبال دارد؛ ولی اصل حق را نمی‌توان به دیگری واگذارد و وسیله تحصیل مال قرار دارد.

حق مالی امتیازی است که به منظور تأمین نیازهای مادی اشخاص، به آنها داده شده است. هدف از ایجاد حق مالی تنظیم روابطی است که به لحاظ استفاده از اشیاء، بین اشخاص وجود دارد و موضوع مستقیم آن تأمین حمایت از نفع مادی است. این دسته از حقوق، بر خلاف گروه نخست، قابل مبادله و تقویم به پول هستند؛ مانند حق مالکیت و حق انتفاع.

نه تنها آثار مالی حقوق غیرمالی سبب نزدیک شدن این حقوق به حقوق مالی می‌گردد، بلکه در پاره‌ای از حقوق، چهره مالی و غیر مالی با هم مخلوط شده است. برای مثال، حقی که مؤلف بر آثار خود دارد هر دو جنبه را داراست. به همین جهت، هنگامی که نویسنده‌ای حق انتشار آثار خود را به دیگری واگذار می‌کند، می‌گویند جنبه مالی حق تألیف را انتقال داده، ولی حق اخلاقی او در باب دفاع از انتقادهای نابجای دیگران و جلوگیری از تقلید و تحریف آن باقی و محفوظ مانده است. همچنین، یادگارهای خانوادگی با اینکه به طور معمول ارزش مالی ندارد، اگر به امضای شخص مشهور، یا اثر هنرمند برجسته‌ای باشد، هر دو جنبه‌ی مالی و معنوی را داراست (همان، ۱۳۹۲، صص ۱۱-۱۲).

۲.۳ مفهوم مالکیت

از نظر حقوقی مالکیت حقی است دائمی که به موجب آن شخص می‌تواند در حدود قوانین تصرف در مالی را به خود اختصاص دهد و از تمام منافع آن استفاده کند. مالکیت کامل‌ترین حق عینی است که انسان می‌تواند بر مالی داشته باشد و سایر حقوق عینی از شاخه‌های این حق است: ۱) مالک می‌تواند با هر شیوه‌ای که مایل است و یا هر انگیزه‌ای که دارد از عین مال خود بهره‌برداری کند یا آن را بی‌استفاده باقی گذارد. ۲) مالک حق دارد از ثمره‌ها و محصول مالی که در اختیار اوست منتفع شود. ۳) مالک می‌تواند مال خود را از بین ببرد یا به دیگری منتقل کند.

از نظر فقهی تعریف مالکیت محل اختلاف نظر فقهاست. شیخ طوسی در تعریف مالکیت بیان می‌دارد: «مالک کسی است که بر تصرف در مالش قادر باشد؛ تصرفی که شخص دیگری نتواند مانع از آن شود.» (شیخ طوسی، بی‌تا، ج ۱، ص ۳۴).

آیت‌الله خوئی به پیروی از محقق اصفهانی، ملکیت را در چهار قسم بیان کرده است:

۱. ملکیت خداوند متعالی، نسبت به تمام ممکنات: این ملکیت به «اضافه اشراقیه» شهرت دارد و عبارت است از اینکه وجود تمام موجودات از وجود خداوند متعال است و به آن تعلق دارد و مربوط می‌شود. این ملکیت حقیقی است، نه اعتباری و قراردادی؛

۲. ملکیت هر شخص نسبت به خود و کارها و ذمه‌اش:این ملکیت به معنای قدرت و سلطنت تکوینی است، به‌گونه‌ای که اگر خواست، انجام می‌دهد و اگر خواست، ترک می‌کند. این ملکیت نیز حقیقی است، نه جعلی و اعتباری؛

۳. ملکیت به معنی جِده: جده یکی از مقولات نه‌گانه فلسفی است؛ نظیر تعمم (صاحب عمامه)، تقمص (صاحب پیراهن)، تنعل و تختم (صاحب کفش و انگشتر)؛ پس مالک، محیط است و مملوک محاط. این نوع از ملک نیز حقیقی است، نه اعتباری؛

۴. ملکیت شخصی بر اموال: بحث کرده‌اند که آیا ملکیت مزبور، حقیقی است یا اعتباری و جعلی؟ و در صورت دوم، آیا ملکیت مستقلاً وضع شده، یا از چیزی انتزاع شده است؟ (خوئی، ۱۴۱۷، ج ۲، ص ۲۰-۲۵)

۳.۳ رابطه مالیت و ملکیت

میان مال بودن چیزی و ملک بودن آن چیز رابطه تالزم برقرار نیست، بلکه رابطه عموم و خصوص من وجه برقرار است. آیت الله خویی در بحث مالیت عمل انسان آزاد (حر) می‌گوید: مالیت اشیاء به عالقه و نیاز مردم بستگی دارد و در صدق عنوان مال بر اشیاء، صدق عنوان ملک لازم نیست، زیرا نسبت میان آن دو عموم و خصوص من وجه است، چون گاهی مال هست و ملک نیست، مانند مباحات اصلی پیش از حیازت (مثل پرندگان قیمتی و ماهی‌ها) چون اینها مال هستند، ولی ملک نیستند. گاهی ملک هست، ولی مال نیست، مانند یک دانه گندم که مفهوم ملک بر آن صادق است، ولی مفهوم مال صادق نیست، زیرا در برابر آن چیزی داده نمی‌شود. گاهی هر دو عنوان هست، مانند بسیاری از چیزها (مثل ماشین و خانه). روشن است که عمل حر پیش از عقد معاوضه (اجاره) از مهم‌ترین اموال عرفی است گرچه ملک اعتباری برای کسی نیست و تنها ملک ذاتی برای صاحبش است (همان، ج ۲، ص ۳۴). به عبارت دیگر عدم مالیت چیزی است و ملک بودن چیز دیگری و نسبت این دو عموم و خصوص من وجه است که هر دو عنوان مال و ملک در مثل خانه وجود دارد، اما در جایی مانند معادن زیر زمین، مالیت وجود دارد اما ملکیت وجود ندارد یا اینکه در دانهای گندم ملکیت وجود دارد، اما مالیت ندارد (مغنیه، ۱۴۱۴، ج ۳، ص ۱۱۸).

۴ قاعده اقدام در فضای مجازی

با توجه به ادله قاعده اقدام، باید گفت که اقدام یک فرد تنها به چیزی تعلق می‌گیرد که تحت مالکیت او باشد و با عنایت به رابطه مال و مالکیت که در نظام فقهی و حقوقی به صورت جداگانه مطرح شد، اقدام افراد در

فضای مجازی نیز به تبع موارد مذکور تعریف می‌شود. در ابتدای این بخش به بررسی مال و مالکیت در فضای مجازی و نیز در ادامه به مصادیق اقدام در فضای مجازی و تعیین مسئولیت کاربران می‌پردازیم.

۱.۴ مال در فضای مجازی

از مجموع مطالب بخش گذشته برای مفهوم مال، ویژگی‌ها و مؤلفه‌های ذیل را می‌توان برشمرد:

۱. ارزش داشتن

۲. برآوردن نیاز فردی و اجتماعی، مادی یا معنوی

۳. قابل اختصاص یافتن به شخص

۴. قابلیت معامله و انتقال

مال در فضای مجازی، همان معیارهای کلی مال در فضای حقیقی را خواهد داشت، اما لازم است این معیارها با توجه به ویژگی‌های فضای مجازی بازخوانی شوند.

۱.۱.۴ ارزش داشتن

بسیاری از داده‌های موجود در فضای مجازی دارای ارزش اقتصادی هستند و به همین خاطر است که اشخاص متعددی در مقابل این داده‌ها، حاضر به پرداخت وجه می‌باشند. برای مثال اطلاعات موجود در پایگاه داده‌های وسیع که به کلان‌داده معروفند، برای بسیاری از فعالین حوزه‌های اقتصادی و تبلیغاتی جذابیت فراوانی داشته و شرکت‌ها و سازمان‌های زیادی برای به دست آوردن این کلان‌داده‌ها تلاش می‌کنند. مثال دستیابی به بانک اطلاعاتی شماره تماس کاربران یک نرم‌افزار کاربردی معروف برای شرکت‌های تبلیغاتی جهت ارسال محتوا جذابیت فراوانی دارد. البته لازم به ذکر است تک تک اطلاعات موجود در این پایگاه‌های داده در شکل‌گیری این کلان‌داده‌ها مؤثر بوده فلذا خود به‌تنهایی دارای ارزش به حساب می‌آیند.

۲.۱.۴ برآوردن نیازها

اساس شکل‌گیری فضای مجازی برای برطرف ساختن بسیاری از نیازهای فردی و اجتماعی بوده و با توجه به این موضوع سرویس‌دهنده‌های فراوانی در بستر این فضا در حال ارائه خدمات به کاربران می‌باشند. حضور کاربران در این عرصه، همراه با رد و بدل شدن اطلاعات و داده‌های زیادی می‌باشد. البته صرف برآورده ساختن نیاز، مالیت را ایجاد نمی‌کند ولی اگر چیزی از نظر عرف و شرع، نیازی از افراد جامعه را برطرف سازد، یکی از شروط مالیت را دارا می‌باشد. لازم به ذکر است که این نیاز می‌تواند فردی، اجتماعی، مادی و معنوی باشد. برای مثال ارائه خدمات آموزشی در بستر فضای مجازی می‌تواند از جمله این موارد باشد. به این نحو که استادی در یک نرم افزار خاص آموزشی محتوای درسی را بارگذاری کرده که در فضای حقیقی اساساً چنین کلاس آموزشی تشکیل نشده است و شاگردان و استاد صرفاً از این بستر برای تعلیم و تعلم بهره‌برداری می‌کنند.

۳.۱.۴ قابلیت اختصاص به شخص

قابلیت مملوک بودن یک شیء و به عبارت دیگر قابلیت اختصاص آن به شخص، از دیگر ویژگی‌های مالیت آن شیء است. در فضای مجازی بسیاری از داده‌ها توسط افراد تولید می‌شود که عرفاً تولیدکننده آنها، صاحب آن داده‌ها به حساب می‌آید. برای مثال اگر کسی در یک شبکه اجتماعی صاحب صفحه‌ای باشد که دنبال‌کننده‌ها[3]ی مختلفی دارد، تمام این صفحه به همراه اطلاعات آن و امتیازات مربوط به دنبال‌کننده‌های آن، اختصاص به تولیدکننده داشته و عرفاً مالک آن صفحه خواهد بود.

۴.۱.۴ قابلیت معامله و انتقال

از آنجا که بسیاری از داده‌های موجود در فضای مجازی دارای ارزش اقتصادی هستند و قابلیت معامله و انتقال این داده‌ها در فضای مجازی در عرف جامعه امروزی پذیرفته شده است؛ فلذا این ویژگی مالیت برای آن داده‌ها صادق است. برای مثال در بستر فضای مجازی داده‌های بسیاری همچون محتوای صوتی، تصویری و انواع فایل‌های چندرسانه‌ای خرید و فروش می‌گردد. لکن صحت شرعی و قانونی این نوع معامله وابسته به محتوای داده‌ها می‌باشد.

با توجه به مطالب مذکور باید گفت مال بودن داده‌های موجود در فضای مجازی با ویژگی‌های مطرح شده سازگار و منطبق است، چرا که عرف عقال برای آنها مالیت قائل است و دارای ارزش اقتصادی هستند و معامله بر آنها صحیح است. برخی از فقها مالیت داده‌های فضای مجازی را پذیرفته‌اند و بر اساس آن فتاوی مختلفی را ایراد داشته‌اند. برای مثال آیت الله مکارم شیرازی در پاسخ به استفتائی در مورد حکم سرقت اطلاعات سری رمزدار، از شبکه‌های کامپیوتری و یا کامپیوترهای شخصی و نیز سرقت و فروش غیرمجاز شماره‌های موبایل دیگران فرموده‌اند: «سرقت به هر حال حرام است و اگر اطلاعاتی باشد که جنبه مالیت دارد و در عرف عقالی امروز خرید و فروش می‌شود، در صورتی که شرایط حد سرقت در آن جمع باشد، اجرای حد سرقت در آن بعید نیست البته این در مورد کسانی است که اموال آنها محترم است.»

۲.۴ مالکیت در فضای مجازی

مالکیت بر داده‌هایی که هنوز در تصرف شخصی هستند و عرضه نشده‌اند، از سنخ مالکیت بر اعیان است. همچنین برخی از وجوه مالکیت مربوط به فضای مجازی، از سنخ مالکیت بر منافع است. از مهم‌ترین موارد مالکیت بر منافع، می‌توان به هاست و دامنه اشاره داشت. منشأ مالکیت در فضای واقعی، اعتباری عرفی است و عقلا پس از اعتبار عرف، به سامان آن پرداخته و با اعتبارات قانونی از آن حمایت کرده‌اند. مالکیت در فضای مجازی پیش از تقنین آغاز شد و این نشان می‌دهد مالکیت در فضای مجازی از سنخ مالکیت عرفی است (حسنی، ۱۳۹۹، ص ۳۸). مالکیت در فضای مجازی دارای مصادیق متعددی می‌باشد که در اینجا به برخی از آنها اشاره مختصری می‌گردد (همان، ۱۳۹۹، صص ۴۶-۵۶).

[3] Followers

۱.۲.۴ مالکیت هویت مجازی

پیدایش فضای مجازی و حضور در آن، به پیدایش مؤلفه‌هایی در هویت می‌انجامد که اساساً ویژه فضای مجازی‌اند و پیش از پیدایش این فضا معنا نداشتند. ازجمله این مؤلفه‌ها می‌توان به حساب‌ها[۴]، رتبه[۵]، رکورد یا سطح[۶] دنبال‌کننده‌ها، دنبال‌شونده‌ها[۷]، پسندها[۸]، بازدیدکننده‌ها[۹]، آدرس IP و مانند آنها اشاره کرد. برخی از مؤلفه های هویت مجازی قابل مالکیت‌اند و برخی دیگر چنین نیستند. برای نمونه، حساب یک فرد در بانک قابل مالکیت نیست و تنها درگاه ورود او به حساب شخصی‌اش در بانک است، یا IP شناسه دستگاهی است که کاربر با آن وارد اینترنت شده است، اما حساب شخصی در سرویس‌های ایمیل یا سرویس وبلاگ و مانند آنها قابل مالکیت است.

۲.۲.۴ مالکیت محیط مجازی

محیط مجازی به‌مثابه مکانی در فضای مجازی است که کاربر در آنجا می‌تواند فعالیت‌های اختصاصی خود را متمرکز کند و فعالیت دیگران در آن مکان منوط به اجازه وی باشد. محیط مجازی ممکن است مکانی برای نشر پیام‌ها باشد؛ مانند سایت، پست الکترونیکی، کانال، گروه و وبلاگ. همچنین امکان دارد محیط مجازی، مکانی برای فعالیت‌های مجازیِ خدماتی باشد؛ مانند سرویس پست الکترونیکی، پیام‌رسانها، شبکه‌های اجتماعی، سرویس وبلاگ‌ها و مانند آنها.

۳.۲.۴ مالکیت معنوی در فضای مجازی

فضای مجازی از جهات مختلف می‌تواند در مباحث مربوط به مالکیت معنوی مورد توجه باشد. یک‌سوی این مباحث، توانایی بسیار بالای فضای مجازی در شکستن مالکیت معنوی و تجاوز به حقوق پدیدآورندگان است و سوی دوم آن، پر بودن فضای مجازی از موضوعات مالکیت معنوی است که برخی در حوزه‌های معمول مالکیت معنوی قرار می‌گیرند و برخی به‌صورت ویژه در فضای مجازی پدید آمده‌اند و معنا دارند. محتوای سایت‌ها و وبلاگ‌ها، ایده‌های فعالان فضای مجازی، اعم از ایده‌های خدمات‌رسان‌ها و ایده‌های کاربران، کدهای برنامه‌نویسی است.

۴.۲.۴ مالکیت پول و اجناس مجازی

پول در فضای مجازی صورت‌های مختلفی دارد. یکی از صورت‌های پول مجازی، اعتباری است که به شکلی گسترده جای پول کاغذی را گرفته است و بخش عمده‌ای از حجم پول در گردش را در جهان تشکیل می‌دهد. نوع دیگر پول مجازی، پولی است که در برخی از برنامه‌های کاربردی نظیر بازی‌ها به‌صورت ارزش اعتباری

[4] Accounts
[5] Rank
[6] Level
[7] Followings
[8] Like
[9] Visitors

جمع می‌شود و دارنده آن می‌تواند با آن پول، ابزارهای لازم را برای ادامه بازی بخرد و تنها در همان بازی اعتبار دارد. نوع سوم پول مجازی، رمزارز است که مسائل بسیاری در حوزه اقتصاد، سیاست و حتی امنیت پدید آورده است. مراد از اجناس مجازی، اشیاء مجازی از قبیل کتاب‌های دیجیتال، تصاویر، ویدئوها، اشیاء مجازی لازم در بازی ها و مانند آنهاست. مالیت پول و اجناس مجازی به‌خودی‌خود بدون اشکال است و به این علت قابل تملک‌اند.

۳.۴ بررسی مصادیق اقدام در فضای مجازی و تعیین مسئولیت کاربران

پس از آنکه معلوم شد اقدام یک فرد بر روی مالی است که تحت مالکیت اوست و نیز بعد از بررسی مفهوم مال و مالکیت در فضای مجازی می‌توان گفت هر جا فرد آگاهانه و با اختیار مملوک خویش را در معرض تلف و تصرف قرار دهد و در جهت ضرر مالی خود اقدامی کند، کسی به نفع او ضمان قهری نداشته و شرع و قانون از چنین کسی حمایت نمی‌کند. البته رفتارهای کاربران در فضای مجازی متنوع بوده و فقط برخی از آنها مشمول قاعده اقدام خواهد شد. در ادامه به ارائه این‌گونه رفتارها پرداخته و مصادیق قاعده اقدام را معین می‌سازیم.

۱.۳.۴ دارای مالیت عرفی عمومی

برخی از داده‌های موجود در فضای مجازی دارای مالیت عرفی عمومی هستند به این معنا که در عرف جامعه همه افراد برای این داده‌ها مالیت قائل هستند. برای مثال می‌توان به انواع پول‌های مجازی، دامنه‌ها، نرم‌افزارهای کاربردی و ... اشاره کرد. در صورتی که فردی با اقدام خویش اینگونه اموال مجازی را که در مالکیت اوست در معرض تلف قرار دهد، مشمول قاعده اقدام خواهد بود.

۲.۳.۴ دارای مالیت غیر عمومی

برخی از داده‌ها در فضای مجازی برای عموم کاربران مالیت ندارد، لکن تنها برخی از افراد قائل به مالیت برای آن داده می‌باشند. داده‌های مذکور به دو دسته تقسیم می‌شود:

الف) داده‌هایی که تنها برای صاحب آن مالیت دارند؛ مانند عکس‌ها و تصاویر یادگاری متوفایی که تنها برای فرزندان آن فرد مالیت دارند. در این فرض، اگر صاحب داده آن را در معرض تلف قرار دهد، طبق قاعده اقدام مسئولیت تلف بر عهده خودش است.

ب) داده‌هایی که برای صاحبان آن مالیت ندارند، ولی ممکن است شخص دیگری با استفاده از آنها تولید ارزش نماید و به تبع آن ارزش، مالیت ایجاد شود؛ مانند علاقه یک شخص به پیتزا؛ با این توضیح که مثلاً با استفاده از داده‌های مربوط به سفارش‌های متعدد یک شخص در نرم‌افزارهای خرید آنلاین غذا، علاقه وی به پیتزا احراز می‌شود. حال شخص دیگری با جمع‌آوری علائق کاربران این نرم‌افزار و نرم‌افزارهای دیگر و تشکیل بانک اطلاعاتی مربوطه، از طریق فروش اطلاعات مذکور به رستوران‌ها اقدام به درآمدزایی می‌کند. در این حالت، اقدام صاحبان داده‌های اولیه (علاقه‌های شخصی به پیتزا) در ارائه اطلاعات، مشمول قاعده اقدام فقهی نخواهد شد.

ج) داده‌هایی که برای صاحب آن و همزمان برای برخی اشخاص دیگر نیز مالیت دارند ولی عموم جامعه قائل به مالیت آن نیستند. مثلاً ایده خامی که فردی تولید کرده است و متخصصان مربوطه قادر به پرورش و ارتقاء ارزش آن هستند، در این بخش قرار می‌گیرد. در این حالت، این ایده خام برای عموم جامعه ارزشی ندارد اما دست‌یابی افراد خاص به این ایده می‌تواند به ضرر صاحب ایده باشد. در نتیجه بر اساس قاعده اقدام، شرع و قانون از صاحب ایده‌ای که خود سبب نشر آن شده است، حمایت نمی‌کند.

۳.۳.۴ فاقد مالیت

از آنجا که یکی از شروط قاعده اقدام، مالیت داشتن موضوع آن می‌باشد، شمول یا عدم شمول قاعده اقدام بر فعالیت‌های مختلف کاربران در فضای مجازی، تنها با مالک مالیت و مملوکیت سنجیده می‌شود. بنابراین اگر کاربری اقدام به انتشار و اتلاف داده‌هایی نماید که مالیت نداشته، اما سبب جعل و سوء استفاده غیر مالی دیگران و یا از بین رفتن عرض و آبرو و مانند اینها شود، عمل او مشمول قاعده اقدام نمی‌باشد. مثال اگر خانمی در صفحات شخصی خود که قابلیت مشاهده عمومی دارد، تصاویر خود را منتشر نماید، نمی‌توان با استناد به قاعده اقدام، شخص دیگری را که بدون اذن صاحب عکس، آنها را منتشر نموده، از مسئولیت مبرا دانست.

۵ جمع بندی

پس از بیان ادله فقهی قاعده اقدام، مشخص شد که دایره شمول این قاعده، اقدامات آگاهانه و با اختیار افراد بر روی اموالی است که مالکیت آن را بر عهده دارند؛ لذا اقدامات غیر مالی نظیر اقدام علیه عرض و آبروی خویش تخصصاً از این بحث خارج می‌شوند. همچنین با بررسی مفاهیم مال و مالکیت از منظر فقهی و حقوقی، مشخص شد که این موضوع مورد اختلاف نظر جدی فقها و حقوقدانان می‌باشد. اما آنچه مسلم است، این است که طبق قاعده اقدام، اگر کسی مال خویش را در معرض تلف قرار دهد، ضمان بر عهده خودش خواهد بود. سپس با بررسی مفهوم مال و مالکیت در فضای مجازی، آن دسته از اقدامات کاربران که متناسب با قاعده اقدام بود، مشخص گردید و علیرغم اهمیت، فراگیری و به‌روز بودن موضوع، پژوهش راه‌گشا و قابل توجهی در این خصوص انجام نگرفته فلذا با بررسی‌های صورت گرفته در پژوهش حاضر، مشخص شد هرگاه در فضای مجازی کاربری در جهت اتلاف مال خویش اقدامی انجام دهد، مسئولیت آن به عهده خود اوست و هرگاه اقدامی غیرمالی انجام دهد که مورد سوءاستفاده دیگران واقع شود، طبق این قاعده نمی‌توان سوءاستفاده‌گر را از مسئولیت مبرا دانست.

مراجع

[۱] حسنی، ابوالحسن (۱۳۹۹). مالکیت در فضای مجازی از منظر فقهی. تهران: دفتر مطالعات اسلامی و ارتباطات حوزوی پژوهشگاه فضای مجازی.
[۲] حسینی، سید میر عبدالفتاح (۱۴۱۷ ق). العناوین الفقهیه (چاپ دوم). قم: موسسه نشر اسلامی.
[۳] خوئی، ابوالقاسم (۱۴۱۷ ق). مصباح الفقاهة. قم: انصاریان.

[۴] دهخدا، علی‌اکبر (۱۳۷۷). لغت‌نامه (چاپ اول). تهران: انتشارات دانشگاه تهران.

[۵] شکاری، محمد؛ تقوایی، عباس (۱۳۹۶). تحلیل قاعده اقدام در فقه و حقوق مدنی ایران، فصلنامه مطالعات علوم سیاسی، حقوق و فقه، دوره ۳، ش ۲، صص ۱۶-۱.

[۶] شیخ طوسی، محمد بن حسن (بی‌تا). التبیان فی تفسیر القرآن. بیروت: دار إحیاء التراث العربی.

[۷] شیخ طوسی، محمد بن حسن (۱۳۸۷ ق). المبسوط فی فقه الامامیه (چاپ سوم). تهران: المکتبة المرتضویة إلحیاء الآثار الجعفریة.

[۸] عرب احمدی، فاطمه؛ فهرستی، زهرا (۱۳۹۴). تحلیل ماهیت قاعده اقدام از منظر فقه و قانون، نخستین کنگره بین‌المللی جامع حقوق.

[۹] عمید، حسن (۱۳۹۰). فرهنگ فارسی عمید (چاپ سی و هشتم). تهران: امیرکبیر.

[۱۰] کاتوزیان، ناصر (۱۳۹۲). دوره مقدماتی حقوق مدنی: اموال و مالکیت (چاپ سی و نهم). تهران: میزان.

[۱۱] کلینی، محمد بن یعقوب (۱۳۸۷ ش). الکافی (چاپ اول). قم: دارالحدیث.

[۱۲] محقق داماد، سید مصطفی (۱۴۰۶ ق). قواعد فقه (چاپ دوازدهم). تهران: مرکز نشر علوم اسلامی.

[۱۳] مصطفوی، سید محمد کاظم (۱۴۲۱ ق). القواعد مائة قاعدة فقهیة معنی و مدرکا و موردا. قم: مؤسسه نشر اسلامی.

[۱۴] معین، محمد (۱۳۸۶). فرهنگ معین (چاپ سوم). تهران: زرین.

[۱۵] مغنیه، محمد جواد (۱۴۱۴). فقه الإمام جعفر الصادق (ع). قم: انصاریان.

[۱۶] موسوی بجنوردی، محمد (۱۴۰۱ ق). قواعد فقهیه (چاپ سوم). تهران: مؤسسه عروج.

بررسی نگرش‌ها نسبت به تحولات رفتاری زیست جنسی متأثر از ابژگی زنان در فضای مجازی

حمیده حسین‌زاده[۱]، محبوبه موسیوند[۲]، شهین قربانی[۳]

[۱] کارشناسی‌ارشد رشته مطالعات زنان گرایش زن و خانواده، دانشکده علوم اجتماعی دانشگاه الزهرا(س)، تهران، ایران
hi.hosseinzadeh@gmail.com
[۲] استادیار گروه مطالعات اجتماعی و توسعه، عضو هیئت علمی پژوهشکده زنان دانشگاه الزهرا(س)، تهران، ایران
m.moosivand@alzahra.ac.ir
[۳] دانشجوی کارشناسی‌ارشد رشته مطالعات زنان گرایش زن و خانواده، دانشکده علوم اجتماعی دانشگاه الزهرا (س)، تهران، ایران
hana.qorbani@gmail.com

چکیده

یکی از وسایل ارتباط جمعی که از اهمیت و تأثیرگذاری بالایی برخوردار است، پلتفرم اینستاگرام می‌باشد که در عصر امروز به‌طور گسترده‌ای فراگیر شده و مورد استقبال قرار گرفته است؛ از این رو این مطالعه با هدف بررسی نگرش‌ها نسبت به تحولات رفتاری زیست جنسی متأثر از ابژگی زنان در فضای مجازی به روش کیفی صورت گرفته است؛ نمونه‌ی هدف ۱۱ خانم ۱۶ تا ۳۵ بوده است، که جمع‌آوری اطلاعات از طریق مصاحبه‌های نیمه‌ساختاریافته صورت پذیرفته است. نتایج شامل چهار مضمون اصلی شامل نگرش‌های جنسی، جامعه‌پذیری رفتاری، سایبرسکس و آواتاریسم و ایماژ بدنی است، نتایج نشان داد که علاوه بر استفاده از محتواهای تولید شده توسط دیگران که به‌آسانی و راحتی قابل دسترس است، هر شخص می‌تواند تولیدات تصویری و شخصی خود را با دیگران جهت استفاده به اشتراک بگذارد و درک افراد از جهان پیرامون تحت تاثیر تصاویری است که از طریق رسانه‌های گوناگون در ذهنشان شکل می‌گیرد و از طریق مشاهده‌ی آن می‌توان به بخشی از رویاها، ارزش‌ها، ایدئولوژی‌ها و کاستی‌های موجود در جامعه دست یافت.

کلمات کلیدی: زیست جنسی، تحولات رفتاری، ابژگی، شبکه‌های اجتماعی.

۱ مقدمه و بیان مسئله

قدیمی‌ترین و مهم‌ترین گروه اجتماعی تحت عنوان واحد بنیادین جامعه و کانون اصلی رشد و تعالی انسان، خانواده است؛ خانواده از نظر کارکردی هم می‌تواند به گونه‌ای موثر باشد، که قوه‌ی عاقله‌ی اعضاء آن را

در یک نظام دانشی خاص و تحت مآثر فرهنگی، تاریخی و بومی قرار دهد و هم می‌تواند به گونه‌ای عمل نماید که هر عضوی آنچنان که مطلوب خود می‌داند، ارزش‌ها را به نحوی از انحاء تئوریزه کند و تناقضات رفتاری و مبنایی پدیدار گردد، که در نهایت نیازمند بازفهم و بازتفسیری از خانواده، ملزومات آن و بررسی و تحلیل تغییرات اجتماعی پیرامونی آن باشیم. در میدانی که صحنه‌ی تفکر عمیق، از نسل امروزی بر اثر عصبیت‌های بی‌بنیاد و تجربه‌ی غریبه و غربیه‌ی حاصل از سیطره‌ی رسانه‌ای و شبکه‌های اجتماعی گرفته شده است و انقطاع و گسست را شاهد هستیم، درک واقعیت یا پندار بودن تغییرات اجتماعی بر محور خانواده کمی مشکل است، و نمی‌توان گفت با مسئله‌ای بسیط و ساده مواجه هستیم. درسال‌های اخیر بررسی‌ها و تحلیل تغییرات خانواده از طریق تحقیقات مختلف حاکی از آن است، که رسانه‌های دیداری و شنیداری، نقش به‌سزایی در این تغییرات و احیاناً چالش‌ها داشته است، از جمله این تغییرات که در پژوهش‌های متفاوت مطرح شده است: بی‌اعتمادی زوجین به یکدیگر (حاج‌محمدی، ۱۳۹۶)، هرزه‌نگاری (شهرکی‌محمدی، ۱۳۹۵)، تغییر سبک‌زندگی (حسین‌پور و مومنی، ۱۳۹۶)، کاهش ارتباطات خانوادگی (انصاری و همکاران، ۱۳۹۷)، تغییر سلیقه در نوع پوشش (فرقانی و مهاجری، ۱۳۹۶) محو هویت اسلامی در بستر فضای‌مجازی و جهانی شدن (الوندی و نایبی، ۱۳۹۱) کاهش ارتباط فرد با خانواده، افزایش احساس تنهایی و افسردگی (زندوانیان و همکاران، ۱۳۹۲) نقض مالکیت فکری در فضای‌مجازی (شفیعی و دهقان‌چناری، ۱۳۹۸) افت تحصیلی دانش‌آموزان (جعفرپور، ۱۴۰۰) تمایل به مدگرایی (فرخ‌نیا و لطفی،۱۳۹۰) چالشی‌شدن فضای تعلیم‌وتربیت فرزندان در عین کارکردهای ارتباطی و ابزاری فضای مجازی (ترابی‌زاده، ۱۳۹۹) و...می‌باشد، که هر کدام از این تحقیقات خود شاهدی بر این مدعاست که افزایش استفاده از فضای‌مجازی در کنار مزایایی که دارد همچون: همدلی اجتماعی دانشجویان (مصلحی‌نیک و حاجیانی، ۱۳۹۵) ارتقاء جایگاه زنان از طریق حس استقلال و اعتمادبه‌نفس (مجیدی‌قهرودی و آذری، ۱۳۸۹) افزایش تعاملات اجتماعی زنان از طریق ایجاد فرصت‌های ارتباطی و اطلاعاتی (امیرمظاهری و ایرانشاهی، ۱۳۸۸) و...منجر به گونه‌گی و تغییراتی در ساختار و ماهیت نظام خانواده شده است.

از این‌رو گسترش دامنه‌ی استفاده از فضای این شبکه‌ها، آسیب‌های احتمالی و لزوم نظارت و فراهم‌سازی بسترها و زیرساخت‌های امن‌تر، بر ضرورت این مطالعه افزود، در این مقاله محققین با پرداختن به چهار پیج اینستاگرامی ساسان حیدری (معروف به ساسی‌مانکن)، امیرحسین مقصودلو (معروف به امیرتتلو)، پویان مختاری و ندا یاسی سعی بر شناخت واکنش‌های کاربران این پیج‌ها نسبت به محتوای نشر شده که غالباً با برساختگی بدن زنانه همراه است و همینطور بررسی چگونگی تاثیرگذاری و تاثیرپذیری آن‌ها دارند، بر همین نظر، در پژوهش حاضر ضمن بررسی محتوای پیج‌های مذکور، به سؤالات زیر پاسخ داده می‌شود:

- آیا ابژگی زنان در فضای‌مجازی نگرش‌های جنسی و جنسیتی را تقویت کرده است؟
- نحوه‌ی مواجهه‌ی آن‌ها با محتوای جنسی و مسائل مرتبط با آن چگونه است؟
- آیا ابژگی زنان در فضای‌مجازی منجر به جامعه‌پذیری رفتاری بیشتر در سایر زنان جامعه شده است؟
- آیا ابژگی زنان در فضای‌مجازی منجر به نارضایتی از وضعیت جسمانی و ظاهری زنان شده است؟

۲ پیشینه تحقیق

از آن‌جایی که بحث تحولات زیست‌جنسی متاثر از ابژگی زنان در بستر فضای‌مجازی شامل مفاهیم گسترده‌ای می‌باشد، سعی شده است، مقالات در دسترس و مرتبط که وجوه ذکر شده را شامل شود، مورد بررسی قرار گیرند. عموم تحقیقات به بیان پیامدهای مثبت و منفی فضای مجازی پرداختند و کمتر تحقیقی اختصاصاً بحث زنان را بررسی کرده است و یا پیامدها و نگرش‌های مرتبط با ابژگی زنان در فضای‌مجازی را مورد واکاوی قرار داده است، با این وجود در این بخش ضمن بررسی تحقیقات پیشین به نقاط متمایزکننده‌ی پژوهش حاضر نسبت به پیشینه‌ها پرداخته می‌شود. پرور و همکاران (۱۳۹۸)؛ در پژوهشی با عنوان «فضای مجازی و مانکن شدن کاربران (تحلیل نشانه‌شناختی چالش مانکن)» شش ویدیوی ایرانی و خارجی از یوتیوب انتخاب و از طریق تحلیل نشانه‌شناسی رولان بارت به تحلیل آن‌ها پرداخت. نتایج حاصل از تحلیل‌ها نشان داد که مصرف نمایشی، نمایش تن‌آسایی، نمایش چشمگیر و ... مهم‌ترین دلایل و عوامل ترغیب کاربران به مشارکت در چالش‌ها بوده است. انصاری و همکاران (۱۳۹۷)، با هدف بررسی تاثیر فضای‌مجازی بر فرهنگ شفاهی افراد در خانواده‌ها تحقیقی با عنوان «تحلیل جامعه‌شناختی تاثیر استفاده از فضای‌مجازی بر فرهنگ شفاهی: مورد مطالعه شهر اصفهان» انجام دادند، نتایج حاکی از آن بود که کیفیت و کمیت استفاده از فضای‌مجازی بر فرهنگ شفاهی خانواده‌ها اثرگذار می‌باشد، به‌طوری که این کمیت و کیفیت منجر به کاهش ارتباط افراد در دنیای واقعی و ارتباطات رودررو می‌شود. عباسی‌شوازی و عباسی‌آتشگاه (۱۳۹۷)، در پژوهشی تحت عنوان«اینترنت، خانواده شبکه‌ای و زمان خانواده، چگونه تکنولوژی‌های نوین ارتباطی روابط خانوادگی را متاثر می‌کنند؟» به پیچیده‌تر شدن چالش‌های خانواده پس از نفوذ اینترنت و تکنولوژی‌های نوین ارتباطی در این نهاد مهم اشاره می‌کند. نتایج حاکی از آن بود که هیچ‌گونه ارتباط مستقیم و معناداری بین نوع و میزان استفاده از تکنولوژی‌های نوین ارتباطی با روابط خانوادگی وجود ندارد، بلکه این ارتباط از مسیر متغییرهای میانجی یعنی زمان خانواده و خانواده‌ی شبکه‌ای محقق می‌شود. فرقانی و مهاجری (۱۳۹۶)، در مقاله‌ای با عنوان «رابطه بین میزان استفاده از شبکه‌های اجتماعی مجازی و تغییر در سبک‌زندگی جوانان» به این نتیجه رسید که مولفه‌های سبک‌زندگی همچون تغییر سلیقه در نوع پوشش، تغییر در شیوه‌ی تغذیه، تغییر در خودآرایی با افزایش استفاده از شبکه‌های اجتماعی ارتباط معناداری دارد. در تحقیقی که حسین‌پور و عرب‌مومنی (۱۳۹۶)، تحت عنوان «تاثیر شبکه‌های اجتماعی مجازی بر هویت نهاد خانواده» انجام دادند، نتایج نشان داد که بین شبکه‌های اجتماعی مجازی و هویت نهاد خانواده رابطه‌ی معناداری وجود دارد. کفاشی و پیرجلیلی (۱۳۹۵) در مقاله‌ای با عنوان «گذران اوقات فراغت زنان در فضای‌مجازی» به این نتیجه دست یافتند که زنان معتقدند فضای‌مجازی امکان کسب داده‌ها را بیشتر می‌کند، در تربیت فرزندان موفقیت بیشتری را فراهم می‌کند و ارتباط آسان با دوستان و آشنایان راحت‌تر می‌شود. با توجه به بررسی پیشینه‌ی تحقیقات صورت گرفته، مشخص شد که هر چند پژوهش‌هایی به بررسی ابژگی زنان و یا آسیب‌های فضای‌مجازی به صورت مجزا پرداخته است، ولی پژوهشی که مستقیماً ابژگی زنان را در فضای مجازی بصورت مطالعه‌ی موردی خصوصاً در رابطه با چهار پیج «تتلو، ساسی‌مانکن، پویان مختاری و ندا یاسی» مورد بررسی قرار داده باشد، وجود ندارد، لذا می‌توان گفت از این حیث که گسترش بیش از پیش

فضای‌مجازی تحولاتی از نظر نگرشی و رفتاری و به تبع آن در زیست‌جنسی داشته است ،این پژوهش حائز اهمیت است و به همین جهت انجام و نتایج آن در قالب یک مطالعه‌ی موردی، مورد بررسی قرار گرفته است.

۳ چارچوب مفهومی

اینترنت در کنار امکاناتی مثل شبکه‌های اجتماعی که به مخاطبان خود می‌دهد یک تعامل اجتماعی مجازی و فراگیر در سطح جهانی را جایگزین تعاملات محدود شده و یا از دست‌رفته‌ی انسانی می‌کند (کفاشی و پیرجلیلی، ۱۳۹۵) در رابطه با سطح اثرگذاری شبکه‌های اجتماعی شریفی‌ساعی و آزاد ارمکی (۱۳۹۱: ۱۴۸) می‌گوید، درک ما از جهان پیرامونمان تحت تاثیر تصاویری است که از طریق رسانه‌های گوناگون در ذهنمان شکل می‌گیرد و از طریق مشاهده‌ی آن می‌توان به بخشی از رویاها، ارزش‌ها، ایدئولوژی‌ها و کاستی‌های موجود در جامعه دست یافت. از این‌رو در جامعه‌ی امروز، تکنولوژی نوین ارتباطی و شبکه‌های اجتماعی علاوه بر زندگی مادی و اقتصادی مردم، بر چارچوب‌های نمادین آن‌ها نیز اثر خواهد گذاشت (حسین‌پور و مومنی، ۱۳۹۶: ۳۷). اگر به تاریخ اجتماعی در سده‌ی اخیر بنگریم، می‌بینیم که با گسترش تکنولوژی‌های دیجیتال و اینترنتی مبتنی بر دانش، به میزانی از سطحیت و نافرهیختگی شخصیتی، رفتاری و فرهنگی رسیدیم که به گفته‌ی (خسروانیان و خسروانیان، ۱۳۹۷: ۱۰-۱۲)، در عصر اطلاعات که عصر انفجار اطلاعات و در نتیجه‌ی آن آلودگی اطلاعاتی است، کسی که خواندن و نوشتن می‌داند و حتی تحصیلات دانشگاهی دارد ولی نحوه‌ی استفاده از اینترنت را نداند باسواد تلقی نمی‌شود. به بیانی دیگر در زمانه‌ای که زیست‌جنسی در چنبره‌ی ابرواژه‌ها، ابرتصاویر و ابرژانرهای ادبی-هنری بیگانه به سر می‌برد، نادیده‌انگاری تاثیر و تاثرات فرهنگی و اضمحال و انحلال ارزش‌های بومی، نه نیازهای جامعه را مرتفع می‌سازد و نه آسیب‌ها را کنترل و مدیریت می‌کند، لذا پیش از آنکه به صورت‌بندی گفتمان ابژگی زنان در فضای‌مجازی بپردازیم، نیاز است مستحیل‌شدن شخصیتی، رفتاری و فرهنگی افراد اجتماع را در سایه‌ی نفوذ مویرگی عمیق‌ترین ساحت‌های ضدارزشی در زندگی روزمره‌ی افراد را بررسی کنیم، به گفته کاستلز، فضای‌مجازی یک مکان نیست، یک راهرو و دالان بین مکان‌ها است. هنگام اقامت در محل خود، در فضای‌مجازی سفر می‌کنید و با افرادی که در مکان‌های دیگر زندگی می‌کنند، ملاقات می‌کنید، اما با استفاده از فضای مجازی، شما در دنیای گسترده‌تر دیگری در حال سیر هستید. بنابراین فضای‌مجازی نوعی ابرفضا و فضای‌ذهن است، فضایی که ما هر روز در آن دست به عمل می‌زنیم و با افراد، ایده‌ها، مکان‌ها و زمان‌های دیگر ملاقات می‌کنیم (کاستلز، ۱۳۸۴: ۴۷).

۴ روش تحقیق

در این پژوهش کیفی که از رویکرد پدیدارشناسی تفسیری استفاده شده است، به بررسی و شناخت پدیدارهای حاصل از تجربیات مشترک کاربران فضای مجازی به دور از دخالت نظری محقق در امر ذهنی مخاطب پرداخته شده است. هدف پژوهش‌های پدیدارشناسی، رسیدن به فهم عمیق‌تری از نمودها یا ظهوریت چیزها، ماهیت و معانی تجارب روزانه دیگران از پدیده‌ها می‌باشد (سلیمی و شریفی، ۱۳۹۴). از همین‌رو آن چه در این پژوهش بررسی می‌شود، توصیفات طرح شده‌ی ۱۱ نفر از زنان ۱۶-۳۵ ساله‌ای است که به طور روزانه با بهره‌گیری

جدول ۱: سیمای مصاحبه‌شوندگان

اسم	سن	تحصیلات	شغل	میزان استفاده	وضعیت تاهل
محدثه	۲۶	فوق دیپلم	خانه‌دار	۸ساعت	متعهد به یک رابطه
نگین	۲۹	لیسانس	آزاد	۳ ساعت	مجرد
عارفه	۲۶	دیپلم	خانه‌دار	۷ ساعت	متاهل
سارا	۲۷	لیسانس	آزاد	۶-۷ ساعت	متعهد به یک رابطه
فاطمه	۳۵	لیسانس تربیت بدنی	خانه‌دار	۴ساعت	متاهل
زهره	۲۷	ارشد حقوق	دانشجو	۶ ساعت	مجرد
الهام	۲۲	دیپلم	مغازه‌دار	۳-۴ ساعت	مجرد
کوثر	۲۹	دیپلم	مشاور پوست و مو	۵ ساعت	متاهل
یلدا	۲۴	کارشناسی حسابداری	آموزش موتورسواری به بانوان در پیست	۱۰ ساعت	متعهد به یک رابطه
فائزه	۳۰	لیسانس	خانه‌دار	۷ ساعت	مجرد
مهدیه	۱۶	سوم دبیرستان	دانش‌آموز	۲ ساعت	مجرد

از محتوای تولید شده در ۴ پیج اینستاگرامی مذکور، تجربه‌ی مشترکی در استفاده از فضای‌مجازی دارند، روش کاربردی برای جمع آوری داده‌ها در این پژوهش، بهره‌گیری از مصاحبه‌ی نیمه‌ساختاریافته‌ای است که مجوعه‌ای از سؤالات باز را شامل می‌شود و با استفاده از روش هدفمند انتخاب شده‌اند. ملاک‌هایی که برای انتخاب نمونه‌ها در نظر گرفته شد، شامل: ۱- فعالیت و وقت‌گذرانی زیاد در فضای‌مجازی خصوصاً اینستاگرام، ۲- دنبال کردن و شناخت کامل پیج‌های مورد مطالعه، ۳- کامنت‌هایی که در واکنش به پست‌های این ۴ پیج گذاشته می‌شد، است؛ از این رو ابتدا نمونه‌هایی انتخاب شدند که با شناخت قبلی، ملاک‌های مد نظر را داشتند و یا با معرفی از طریق دوستان که از پیش در جریان موضوع مصاحبه قرار گرفته بودند، برای مصاحبه آماده شدند و از طرفی برخی از مصاحبه شونده‌ها، از طریق کامنت‌هایی که زیر پست‌های این ۴ پیج گذاشته بودند، شناسایی شدند. پس از مشخص شدن نمونه‌ها، مصاحبه‌کننده به انجام مصاحبه‌ها پرداخت، که مصاحبه‌ها در آن با رضایت کامل نمونه‌های شرکت‌کننده به‌طور متوسط ۳۰ الی ۵۰ دقیقه صورت گرفت. در ابتدای کار به جهت ارتباط‌گیری مناسب‌تر با مشارکت‌کننده، سؤالات زمینه‌ای پرسیده شد، که پس از آن که ارتباط‌گیری مثبت‌تری بر فضای بین مصاحبه‌گر و شرکت‌کننده ایجاد شد، به سؤالات اصلی پرداخته شد.

۵ یافته‌ها

در این پژوهش در مجموع از ۱۱ نفر از کاربران زنی که در بازه‌ی سنی ۲۲ تا ۳۰ سال بودند، مصاحبه انجام شد. با توجه به اطلاعات به‌دست‌آمده مشخص شد که اکثر مصاحبه‌شوندگان به میزان زیادی از اینترنت و فضای‌مجازی استفاده می‌کنند و بعضاً خود را معتاد به این فضا می‌دانند. به منظور بررسی سؤالات تحقیق، پرسش‌هایی در طیفی از مسائلی که رشد نگرش‌های جنسی، جامعه‌پذیری رفتاری، ایماژ بدنی و ... را بررسی می‌کند، پرسیده شد.

جدول ۲: مقوله‌بندی تأثیرات فضای سایبرسکس بر خانواده‌ها

مقوله‌های اصلی	مقوله‌های فرعی	مقوله‌های جزئی
رشد نگرش‌های جنسی	تمایلات دگرباشانه – تمایلات هم‌باشی – رابطه نامشروع با جنس مخالف – رشد نگرش‌های جنسی – سوء استفاده‌ی جنسی از زنان	گفت‌وگو درباره‌ی نحوه مواجهه با نیازهای جنسی به‌صورت شوخی و طنز – خودارضایی – تجربه یک رابطه عاطفی و دوستی با جنس مخالف – عادی شدن ایجاد رابطه با جنس مخالف – برطرف شدن نیازهای فرد به جنس مخالف در طول رابطه – رابطه‌ی جنسی با هم‌جنس برای کسب تجربه
جامعه‌پذیری رفتاری	تغییر سبک پوشش – میزان حضور زنان در فضای سایبرسکس – تن و تنانگی – تغییر سبک زندگی و رفتاری	استفاده از زنان در صنعت تجاری سکس – استفاده از زنان در صنعت تبلیغات – ترغیب زنان به هنجارشکنی و تابوشکنی
سایبرسکس و آواتاریسم	آشکار کردن روابط با جنس مخالف – رابطه‌های جدید و تشکیل زندگی مجازی و خارج از عرف	تنوع‌طلبی، سرگرم‌سازی، زندگی دوم، نفوذ مویرگی سایبرسکس، تفردگرایی
ایماژ بدنی	عدم رضایتمندی از وضعیت جسمانی و ظاهری – تقویت سرمایه‌های جنسی	افسردگی ناشی از نارضایتی از ظاهر – افزایش عمل‌های زیبایی – تقویت جذابیت‌های جنسی – تقویت مهارت‌های شناساندن خود به جنس مخالف

۱.۵ رشد نگرش‌های جنسی

الف) پارتنر جنسی باهم جنس: به‌طور کلی این موضوع در سطح جامعه وجود دارد که گفتمان‌های جدیدی در روابط اجتماعی و سبک‌های‌زندگی توسط رسانه‌های اجتماعی تصویر–محور در حال برساخته‌شدن است. محدثه ۲۶ ساله:

«حدود پارسال بود فک می‌کنم که ندا یاسی و پویان مختاری لایوهای مکرر می‌ذاشتن و خب افرادی که در لایوها حضور داشتن از نظر سنی متفاوت بودن، یکی از لایوهاش رو که من دیدم دو تا خانم دبیرستانی بودن که از راهنمایی باهم بودن و اون‌جور که اونا صحبت می‌کردن، کلاسشون اکثرشون دو به دو پارتنر جنسی هم بودن و با هم رابطه‌هایی داشتن، متاسفانه خوب فضای این لایوها برای قشر دانش‌آموزی وقتی این لایوها رو می‌بینن که همه چیز عادی شده ...»

ب) بسترسازی در راستای دوستی با جنس مخالف: نمونه‌ی دیگری از این مهم از زبان نگین ۲۹ ساله:

«یادم میاد پارسال بود که ندا یاسی دیگه از خودش پستی نمی‌ذاشت یه دفعه یه شخصی منو تو گروهی دعوت کرد و به دلیل اینکه ایشون جواب نمی‌دادن میخواستن کمپینی راه بندازن و ایشون رو هم فالو کنن تا وقتی که قول می‌ده در این ساعت در لایو باشه بیاد و اعلام حضور بکنه و نه اینکه غیبش بزنه، خوب افراد زیادی در این گروه بودند و همینطور هی اضافه می‌شدن در این گروه، تا جایی که من یادمه جنسی نبود ولی خوب

بیشتر با هم چت میکردن، آشنا می‌شدن و ممکن بود با هم دیگه رابطه داشته باشن و مشخصات همدیگر رو که می‌گفتنن، اصل میدادن از کجا هستن، چند سالشونه که ببین کسی همشهری هستش و ... ممکن بود که منجر به رابطه هم شده باشه ...»

پ) تمایلات هم‌باشانه: تمایلات هم‌باشانه، یکی از مسائلی است که در جامعه امروزی ایرانی مورد گفت‌وگو است، که البته ناتوانی در توضیح امر و تحولات یا مفاهیم خلق‌شده‌ی جدید به عنوان یک امر اجتماعی و برساخته شده توسط گفتمان‌های مسلط، چالش‌های مسئله را نیز بیش‌ازپیش می‌کند. عارفه ۲۶ ساله می‌گوید:
«صرفاً این چهار تا پیج نه، پیج‌های زیادی از اینا الگو گرفتن و همینطورن، خصوصاً پویان مختاری خیلی تاثیر داره که میگه زندگی با جنس مخالف، بدون ازدواج هیچ اشکالی نداره، مثلاً یه مدت با یه نفری باشی، بعد یه مدت می‌بینی به درد هم نمی‌خورین، بیخیالش میشی مشکلی هم نداره، همونطور ک تا الان با افراد متفاوتی رابطه داشته و مدام پارتنر عوض می‌کنه ...»

ت) رابطه‌ی نامشروع با جنس مخالف: در جامعه‌ی جنسیتی شده، زن و بدن زنانه به نوعی در مرکز توجهات مردانه صورت‌بندی می‌شود، طوری که زن نه به عنوان یک جنس و سوژه‌ی انسانی، بلکه بعنوان یک ابژه‌ی کاملا جنسی‌شده به تصویر کشیده می‌شود، در این صورت است که فضای مجازی با ایجاد فرصتی برای تغییر نگرش‌ها نسبت به تعهدات خانوادگی و ارتباطی، زمینه‌ی جدیدی برای روابط فراعرفی فراهم می‌کند؛ سارا ۲۷ ساله در این زمینه می‌گوید:
«به طور غیرمستقیم همینکه اثری که روی نگرش زنان و دختران گذاشته عملاً خیلی سوءاستفاده جنسی میشه از زنان، براشون عادی‌سازی شده، که رابطه با جنس مخالف مشکلی نداره و میره ارتباط برقرار می‌کنه، چرا؟ چون از مدت‌ها قبل این پیج‌ها رو دنبال می‌کنه و تاثیر می‌پذیره، این هم خود خانم‌ها باعث میشن که ازشون سوء استفاده بشه»

۲.۵ جامعه‌پذیری رفتاری

اصطلاحاً جامعه‌پذیری به روندی گفته می‌شود که اشخاص یاد می‌گیرند خود را با ارزش‌ها و هنجارهای اجتماعی سازگار و هماهنگ کنند، مهم‌ترین اهداف جامعه‌پذیری: انتقال فرهنگ از نسلی به نسل دیگر، شکل‌گیری شخصیت فردی، شکل‌گیری رسوم و عادات آرزوهای فردی، تمرکز بر ارزش و اعتقادات اساسی جامعه و کسب مهارت‌های لازم برای زندگی در جامعه است.

الف) میزان حضور زنان در فضای سایبرسکس: در اصل بدن‌نمایی زنانه در مناسبات تن‌وتنانگی در جامعه‌ی فعلی تبدیل به امری عادی شده است، و عرف اجتماعی به نوعی این‌چنین بدن‌نمایی را جزء انتظارات خود از زن می‌داند. در حقیقت بدن زن در نزد جامعه به عریانی فراخوانده می‌شود و مرد نیز به مخاطب اصلی این نمایش زنانه تبدیل شده است. فاطمه ۳۵ ساله می‌گوید:
«کسایی که در لایوشون میان معمولاً افرادی هستن که راهنمایی، دبیرستان هستن که اینا بیشتر دوست

دارن در لایوشون بیان وگرنه همه سنین ایشون رو دنبال می‌کنه و خوب وقتی این‌ها یک چالش رو میذارن خیلی‌ها در این چالش‌ها شرکت می‌کنن و وقتی که این‌ها شرکت می‌کنن فیلم‌هاشون رو براشون می‌فرستن، در استوری‌های پویان و ندا پارسال دیدم که چالش‌ها رو خود مردم اجرا می‌کردن و خیلی هم شرکت کرده بودن در حدی که خیلی استوری‌ها پر می‌شد و جا نبود و میگفتن در روزهای آتی بقیه‌ی استوری‌ها رو میزاریم»

ب) سوء استفاده‌ی جنسی از زنان: مهم‌ترین پیام پدیده‌هایی که در فضای‌مجازی و خصوصاً سایبرسکس خلق می‌شوند، تقلیل زنانگی به تنانگی است که بدن زن را در متن توجهات قرار می‌دهد، نگاه جنسیتی به زن و ابژگی جنسی گاهی زن را از حاشیه به متن و از متن به فرامتن می‌رساند، همچنان که در این پیج‌ها، پازل هر کدام از بلاگرها بدون زن تکمیل نمی‌شود و اساساً مشهوریت و مقبولیت این افراد به نوعی بخاطر تن زن و نه خود زن می‌باشد. زهره ۲۷ ساله:
«شاید اون خانم‌هایی که در یک‌سری کلیپ‌هاشون بازی می‌کردن، خصوصاً کلیپ‌های پویان مختاری و ساسی‌مانکن و خوب یسری‌ها بخوان تو این کلیپ‌ها بازی کنن شاید بهشون پیشنهاد بدن، ولی خوب درصد کمی هستن، البته صرفا این چهار تا پیج نیست، یه پیج دیگه هم بود که اسم اون شخص رو یادم نمیاد، به دوست من پیشنهاد داده بودن شما میتونی بیای خارج از کشور و ما شما رو ساپورت می‌کنیم، ممکنه که حالا اینطوری بخوان پیشنهاد بدن، که تعدادشون هم زیاد نیست البته، ولی در هر صورت ورود به این کارا داره عادی و گسترده میشه ...»

پ) تغییر سبک‌پوشش: اهمیت پلتفرم‌های رسانه‌های اجتماعی تصویر–محور، میزان تأثیر آن بر ذهنیت افراد به عنوان یک عنصر فرهنگی است، حال اینکه این عنصر فرهنگی می‌تواند به تقویت ارزش‌های یک جامعه بیانجامد و یا وضعیتی ضد ارزش‌گونه ایجاد کند. الهام ۲۲ ساله در این زمینه می‌گوید:
«هم این پیج‌ها و هم خیلی پیج‌های دیگه میتونه بر فعالیت بیشتر دختران و زنان موثر باشه، خیلی از دخترا و زن‌های دیگه هم هستن که فعالیت این‌چنینی دارند، بیکینی و لباس‌های عریان می‌پوشن، میرقصن، خیلیا هم نگاهشون می‌کنن و فالو می‌کنن و اندازه ندا یاسی هم فالوور دارن ...»

۳.۵ سایبرسکس و آواتاریسم

الف) آشکار کردن روابط با جنس مخالف: از جمله روش‌های جذب مخاطب توسط شاخ‌های مجازی نمایان ساختن درونی‌ترین مسائل خصوصی با نمایش روابط خارج از عرف است، هر چند عشق و رابطه یکی از بنیادی‌ترین مسائل زندگی هر شخصی است، اما فرهنگ مصرف‌گرایی نمایشی از طریق این بسترها، ابزاری برای دریافت و نمایش الگوهای گوناگون در زمینه‌های متفاوت است. کوثر ۲۹ ساله می‌گوید:
«فضای‌مجازی ۹۰ درصدش همینه، خیلی روابط آزاد شده و خیلی تاثیر گذاشته، دختر پسرا بیشتر با هم دوست میشن، خیلی هم عادی شده همچنین چیزی، خوب اینا عادی‌سازی کردن دیگه، ندا یاسی، ساسی مانکن، پویان مختاری که کلا با دوست دخترش نیلی زندگی می‌کنه، اینجا با هم بودن و رفتن اون طرف با

همن، الانم که پویان با ریحانه پارسه هست، برادر پویان مختاری هم باز با یک زن رقاصه دوست شده، هیچ کدومشون هم نه عقدی نه چیزی، دوست پسر دوست دخترن، با هم زندگی میکنن که روی ما هم خیلی تاثیر میذاره صددرصد».

ب) رابطه‌های جدید و تشکیل زندگی مجازی و خارج از عرف: یکی از مسائل جدی و شاید وجه منفی فضای‌مجازی ایجاد زمینه‌ای برای روابط آزاد اجتماعی است که گاهاً در چارچوب‌هایی فراتر از عرف سنتی جامعه شکل می‌گیرد، یلدا ۲۴ ساله: «استفاده از این فضا صددرصد منجر به شکل‌گیری زندگی دوم شده، خصوصاً کسانی که این چهار نفر رو و افراد مشابه این‌ها را دنبال می‌کنن، فضای مجازی به نظر من ۸۰، ۹۰ درصد باعث میشه افراد رابطه خارج از عرف و خارج از زندگیشون داشته باشن، اگر ازدواج کرده باشن که رابطه فرازناشویی هست اگر ازدواج نکرده باشن من خیلی‌هارو دیدم حتی ۱۳، ۱۴ ساله‌ها، مادرها همه می‌نالن، همه مشکل دارن تو خونه، دختر دوست داره یه جوری لباس بپوشه، یک جور فکر میکنه، با کیا بره بیرون، با پسر دوست بشه، بره پارک، مسافرت بدون پدر و مادر...»

۴.۵ ایماژ بدنی

الف) عدم رضایتمندی از وضعیت جسمانی و ظاهری: به طور معمول نمی‌توان گفت که شبکه‌های اجتماعی خود الگو هستند، بلکه فضای‌مجازی می‌تواند زمینه را جهت دسترسی آسان‌تر به الگوها فراهم نماید، در این میان الگوسازی از الگوهای زنانگی و تنانگی برتر از دید فضای مدرنیته‌ی امروزی، بستر نارضایتی از وضعیت جسمانی و ظاهری در بین افراد ایجاد خواهد شود. فائزه ۳۰ ساله:
«یکی از دلایلی که هیچ وقت از ظاهر خودم راضی نبودم ترس از قضاوت شدنه که دیگران خیلی بد این کارو انجام میدن، خب یکی از دلایلی که ظاهر و قیافه خیلی مهم شده همین رسانه‌س و باعث میشه همیشه دنبال این باشم که یه جوری به خودم برسم».

ب) تقویت سرمایه‌های جنسی: شبکه اجتماعی اینستاگرام بستری را مهیا نموده که افراد در آن می‌توانند به ارائه و نمود خود در آن اقدام نمایند، از این‌رو فضای لازم از طریق این بستر جهت بازنمایی، فراهم شده که در قالب آن، الگوی تقویت سرمایه‌های جنسی به صورت مکرر تولید و بازتولید می‌شود. مهدیه ۱۶ ساله:
«خب یکی از راه‌هایی که آدم بتونه جذاب باشه عمل زیباییه، یا حداقلش اینه آدم به ظاهرخودش در هر صورت برسه این چیزیه که یاد گرفتیم، غیر از اینم نیست واقعیتش، چون الان همه چشمشون به اطرافشونه، فضای مجازی قطعا بی‌تاثیر نبوده تو این سلیقه‌سازی».

۶ نتیجه‌گیری

ورود به عصر جدید و آغاز بکارگیری تکنولوژی‌های نوین مثل گسترش شبکه‌های اجتماعی؛ در بسترهای اینترنتی و فضای مجازی عصر جدیدی را در پیش‌روی بشر و اجتماعات و به تبع آن اجتماع کوچک خانواده

قرار داده است، به گونه‌ای که شکل جدیدی از ارتباط بین انسان‌ها و نیز بین اعضای خانواده شکل گرفته است. شکلی از ارتباط که ماهیت مخصوص به خود را دارد و می‌تواند پنهان یا آشکار باشد؛ دارای سرعت بسیار زیاد در ایجاد ارتباط و اتمام ارتباط است. قابلیت ایجاد شبکه‌ای بزرگ از طرف‌های مرتبط را دارد و این نقطه‌ی عطف، تغییر و تحول در ایجاد روابط بین انسان‌ها می‌باشد. تجربه‌ی این شکل از ارتباطات در کنار روابط قبل از آن برای افراد جذابیت‌ها و چالش‌هایی را به دنبال دارد. خانواده و اعضای خانواده که با این بستر ارتباطی با ویژگی‌های نوین و منحصر به فرد خود مواجه‌اند از چالش‌های آن مصون نبوده و همسو کردن و تطبیق این شکل ارتباط جدید با ارتباطی که در فضای سنتی خانواده آموخته‌اند، می‌تواند مسئله‌ای چالش برانگیز باشد. از نظر مستنه افراد و گروه‌های مختلف مردم از این فرصت‌ها برای کسب منفعت و مزیت بهره می‌برند که در عمل باعث ایجاد نوعی تعارض بین ارزش‌های قدیم و فنون جدید و یا تعارض بین گروه‌های طرفدار ارزش‌ها، اهداف و فنون سابق و حامیان ابزار جدید می‌گردد، که همین امر باعث بروز تعارضاتی می‌شود که توسط ابزار و فناوری‌های جدید منجر به بروز تغییرات اجتماعی و سیاسی می‌شود. در این مطالعه که چهار مقوله‌ی اصلی رشد نگرش‌های جنسی، جامعه‌پذیری رفتاری، سایبرسکس و آواتاریسم و ایماژ بدنی به دست آمد، اهمیت مطالعهٔ فضای مجازی و بررسی آسیب‌های احتمالی و پیامدهای استفاده از آن شفاف‌تر شد. در همین راستا می‌توان گفت که نتایج این پژوهش با مطالعاتی که اسلامی و جهانگیر (۱۳۹۶)، فرخ‌نیا و لطفی (۱۳۹۰)، معمار و همکاران (۱۳۹۱)، پرور و همکاران (۱۳۹۸) و حسین‌پور و عرب‌مومنی (۱۳۹۶)، انجام دادند، همسو بوده است؛ مطالعاتی که آسیب‌هایی چون اختلال در شکل‌گیری شخصیت افراد، تعارض در ارزش‌ها و هنجارها، سواستفاده‌های جنسی، کاهش روابط دوستانه و خانوادگی، نمایش الگوهای غلط فرهنگ‌های بیگانه، دلزدگی از فرهنگ خودی و بروز و ظهور ناهنجاری‌های فرهنگی را برمی‌شمرد. براساس پژوهش صورت گرفته و مضامین استخراج شده، واقعیت اینستاگرام نشان می‌دهد کاربران زیادی در این پلتفرم تمایل نسبتاً زیادی برای نمایش خود با هر نوع پوششی و گاهاً حتی بدون پوشش دارند که معمولاً از فعالیت‌های روزمره و اکثر اوقات از فعالیت‌های آنلاین در لحظه، جهت گرفتن بازخورد از طریق کامنت و لایک تصاویر و فیلم‌های کوتاهی به اشتراک می‌گذارند. اهمیت مطالعه‌ی این شبکه‌ها این است که کاربران با تبدیل شدن به یک تولیدکننده و مصرف‌کننده‌ی محتوا آن‌چنان توان اثرگذاری و معنادهی پیدا می‌کنند که با استفاده از امکانات اینستاگرام آنچه را دوست دارند، تایید می‌کنند و آنچه را دوست ندارند و مطلوبشان نیست را به نحوی از انحاء تئوریزه می‌کنند، در همچین فضایی است که بدن علاوه بر اینکه ویژگی‌های جدید و ویژه‌ای پیدا می‌کند، باعث می‌شود افراد صورت‌بندی جدیدی در مواجهه با بدنشان داشته باشند (راودراد و گیشنیزجانی، ۱۳۹۶). که معمولا بصورت رضایت یا عدم رضایت از ظاهر مادی و جسمانی نمود پیدا می‌کند. لذا این امر مهم است که بررسی کنیم، آیا شعائر بی‌محتوا یا توهمی که منجر به کاهش درک مفهومی در افق مبنایی ما می‌شود و اصول و خط مشی‌گذاری‌ها را وادار به کنش در افق دیگری می‌کند، نجات‌بخش در بن‌بست‌ها، کنج نشینی‌ها، بست‌نشینی‌ها و تحقیرشدگی‌های نسل امروز خواهد بود یا خیر؟ به همین جهت، تنوع و تفاوت‌ها، قبض و بسط‌ها، جزومدها، زیروزبر شدن‌های وجودی در موضوع تحولات خانواده و مهم‌تر از آن ابژگی زنان در بستر شبکه‌های اجتماعی را قبل از آنکه مورد بحث و تحلیل قرار دهیم، باید مورد کشف و شناخت عمیق قرار داد، چرا که تفکر و ارائه‌ی راهکار در خلاء، بدون شناخت مسئله امری

سودمند نخواهد بود؛ که این مهم، از جمله مهمترین اهداف این پژوهش بوده است.

مراجع

[۱] انصاری، ابراهیم، کیانپور، مسعود، و عطایی، پری (۱۳۹۷). تحلیل جامعه شناختی تأثیر استفاده از فضای مجازی بر فرهنگ شفاهی (مورد مطالعه: شهر اصفهان). جامعه‌شناسی کاربردی (مجله پژوهشی علوم انسانی دانشگاه اصفهان)، ۲۹(۱) (پیاپی ۶۹)، ۱۸-۴۰.

[۲] اسلامی، علی، و جهانگیر، زهرا (۱۳۹۶). شبکه‌های اجتماعی مجازی، آسیب‌شناسی روانی و فرهنگی در خانواده. کنفرانس بین‌المللی فرهنگ آسیب‌شناسی روانی و تربیت.

[۳] الوندی، هومن، و نایبی، محسن (۱۳۹۱). بررسی رابطه هویت اسلامی، فضای مجازی و جهانی شدن. مطالعات رسانه‌ای، ۷(۱۹)، ۳۵-۴۳.

[۴] امیر مظاهری، امیر مسعود، ایرانشاهی، اعظم (۱۳۸۸). «چالش‌های تعامل اجتماعی زنان ایرانی در فضای مجازی از دید زنان فعال در فضای مجازی». مطالعات رسانه‌ای. ۵(۱) (پیاپی ۸).

[۵] پرور، مهدی، عباسی شوازی، محمدتقی، و حمیدی زاده، احسان (۱۳۹۸). فضای مجازی و مانکن‌شدگی: تحلیل نشانه‌شناختی چالش مانکن. مطالعات فرهنگی و ارتباطات، ۱۵(۵)، ۱۵۳-۱۷۷.

[۶] ترابی‌زاده، سمیه (۱۳۹۹). تأثیر فضای مجازی بر تعلیم و تربیت رسمی. پژوهشنامه اورمزد، ۵۱ (ضمیمه شماره ۲)، ۹۷-۱۱۴.

[۷] جعفرپور، محبوبه (۱۴۰۰)، بررسی تأثیر فضای مجازی بر عملکرد تحصیلی دانش‌آموزان پسر، مطالعات روانشناسی و علوم تربیتی، ۴(۲۳)، ۴۰-۲۵.

[۸] حاج‌محمدی، فرشته، حاج محمدی، سمیرا (۱۳۹۶). تأثیرات اخلاقی استفاده از فضای مجازی بر پیوند زناشویی و روابط فرزندان در خانواده. فصلنامه علمی-پژوهشی مطالعات اخلاق کاربردی، ۱۳(۵۰)، ۱۱-۳۷.

[۹] حسین‌پور، جعفر، و عرب‌مومنی، علی (۱۳۹۶). تأثیر شبکه‌های اجتماعی مجازی بر هویت نهاد خانواده. برنامه‌ریزی رفاه و توسعه اجتماعی، ۸(۳۲)، ۳۳-۶۰.

[۱۰] خسروانیان، سجاد؛ خسروانیان، نجمه (۱۳۹۷). تفکر انتقادی و سواد رسانه: با تأکید بر آموزه‌های سواد رسانه‌ای، نشر: پشتیبان، چاپ یکم.

[۱۱] راودراد، اعظم، و گیشنیزجانی، گلنار (۱۳۹۶). گونه‌شناسی الگوهای بازنمایی بدن رسانه‌ای کاربران ایرانی در اینستاگرام. مطالعات رسانه‌های نوین، ۳(۱۰)، ۲۵۹-۳۰۴.

[۱۲] زندوانیان، احمد، حیدری، مریم، باقری، ریحانه، و عطارزاده، فاطمه (۱۳۹۲). آسیب‌های فضای مجازی بین دانش‌آموزان دختر. مطالعات فرهنگ - ارتباطات، ۱۴(۲۳) (مسلسل ۵۵)، ۱۹۵-۲۱۶.

[۱۳] سلیمی، محمدرضا، و شرفی، روح‌انگیز (۱۳۹۴). بررسی ساختار و ابعاد روش تحقیق کیفی پدیدارشناسی. کنفرانس بین‌المللی علوم انسانی، روان‌شناسی و علوم اجتماعی.

[۱۴] شفیعی، فروزنده؛ دهقان چناری، مجید (۱۳۹۸). بررسی نقض مالکیت فکری در فضای مجازی، قانون‌یار، ۳(۱۰)، ۱۳۴-۹۴.

[۱۵] شریفی‌ساعی، محمدحسین؛ آزادارمکی، تقی (۱۳۹۵). تغییرات، چالش‌ها و آینده خانواده ایرانی، ناشر: موسسه تیسا ساغر مهر.

[۱۶] شهرکی محمدی، آزیتا (۱۳۹۵). باتلاق مجازی: نگاهی به جنبه‌های منفی استفاده از فضای مجازی. کنفرانس بین‌المللی وب‌پژوهی.

[۱۷] عباسی شوازی، محمد تقی، عباسی آتشگاه، پروین (۱۳۹۷). اینترنت، خانواده شبکه‌ای و زمان خانواده؛ تأثیر تکنولوژی‌های نوین ارتباطی بر روابط خانوادگی. مطالعات رسانه‌های نوین، ۴(۱۴)، ۳۳-۶۵.

[۱۸] فرقانی، محمدمهدی، و مهاجری، ربابه (۱۳۹۷). رابطه بین میزان استفاده از شبکه‌های اجتماعی مجازی و تغییر در سبک زندگی جوانان. مطالعات رسانه‌های نوین، ۴(۱۳)، ۲۵۹-۲۹۲.

[۱۹] فرخ نیا، رحیم، و لطفی، اعظم (۱۳۹۰). بررسی تأثیر فضای مجازی اینترنت بر مدگرایی. مطالعات فرهنگی و ارتباطات، ۷(۲۲)، ۹۵-۱۱۸.

[۲۰] کفاشی، مجید، و پیرجلیلی، زهرا (۱۳۹۵). گذران اوقات فراغت زنان در فضای مجازی (شهر تهران سال ۱۳۹۴). زن و جامعه (جامعه‌شناسی زنان)، ۷(ویژه نامه)، ۱۰۵-۱۲۳.

[۲۱] کاستلز، م. و اینس، م. (۱۳۸۴). گفتگوهايي با مانوئل کاستتلز، ترجمه: چاوشیان، م.، تهران: نشر نی.

[۲۲] مصلحی‌نیک، فائزه، و حاجیانی، ابراهیم (۱۳۹۶). بررسی تأثیر فضای مجازی بر همدلی اجتماعی دانشجویان. راهبرد اجتماعی فرهنگی، ۶(۲۲)، ۳۳۱-۳۵۵.

[۲۳] معمار، ثریا، عدلی پور، صمد، و خاکسار، فائزه (۱۳۹۱). شبکه‌های اجتماعی مجازی و بحران هویت (با تأکید بر بحران هویتی ایران). مطالعات و تحقیقات اجتماعی در ایران، ۱(۴)، ۱۵۵-۱۷۶.

[۲۴] مجیدی قهرودی، نسیم، و آذری، فاطمه (۱۳۸۹). بررسی نقش اینترنت در ارتقای جایگاه زنان. پژوهشنامه زنان، ۱(۲)، ۸۷-۱۰۹.

راهکارهای رسانه‌ای مقابله با رویکرد ضدفرهنگی سلاح اجتماعی جوکر

حسن ضیائی جباری[۱]، حمیدرضا حسینی دانا[۲]، بی‌بی‌سادات میراسماعیلی[۲]

[۱]دانشجوی دکتری، گروه مدیریت رسانه‌ای، دانشکده علوم انسانی و هنر، واحد دماوند، دانشگاه آزاد اسلامی، دماوند، ایران
tash.ziaee@yahoo.com
[۲]استادیار، گروه مدیریت رسانه‌ای، دانشکده علوم انسانی و هنر، واحد دماوند، دانشگاه آزاد اسلامی، دماوند، ایران
{hhoseinidana,f.miresmaili}@gmail.com

چکیده

امروزه رسانه‌ها می‌توانند عامل توسعه فرهنگی یا تهاجم فرهنگی باشند. چالش جدید جوامع در دنیا، استفاده از رسانه برای تقویت سلاح نرمی بنام «سلاح اجتماعی جوکر» می‌باشد. این سلاح نرم به‌واسطه محتوای جعلی خبری و فیک‌نیوزها در راستای ایجاد ناهنجاری‌های فرهنگی پشتیبانی می‌شود. هدف اصلی این مقاله بررسی راهکارهای رسانه‌ای جهت مقابله با ناهنجاری‌های فرهنگی سلاح اجتماعی جوکر می‌باشد. سئوال اصلی این است که آیا بین راهکارهای رسانه‌ای و ناهنجاری‌های فرهنگی سلاح اجتماعی جوکر رابطه معنی‌داری وجود دارد؟ این پژوهش فرض را بر این گرفته که بین راهکارهای رسانه‌ای و ناهنجاری‌های فرهنگی سلاح اجتماعی جوکر رابطه معنی داری وجود دارد. با توجه به اهداف این تحقیق و موضوع پژوهش، از روش پژوهش آمیخته یا ترکیبی از روش‌های کمی و کیفی استفاده شده است.نهایتاً گزاره‌ها در یک دسته‌بندی کلی، سازماندهی و تجزیه و تحلیل شدند و راهکارهای رسانه‌ای حاصل؛ در قالب سه مقوله شامل فناوری‌های شناخت محتوای خبری جعلی، فرهنگ‌سازی شناخت و راهکارهای حکمرانی معرفی شدند. بنابراین و با استناد به مقوله‌های به‌دست آمده، افراد ومخاطبان رسانه می‌توانند با استفاده از راهکارهای ارائه شده با آسیب‌های فرهنگی سلاح اجتماعی جوکر مقابله کنند.

کلمات کلیدی: ناهنجاری‌های فرهنگی، فیک‌نیوزها، راستی‌آزمایی محتوای خبری، سلاح اجتماعی جوکر.

۱ مقدمه

راستی آزمایی محتوای رسانه‌ای و شناخت فیک نیوزها یکی از ابزارهای مقابله با سلاح اجتماعی جوکر می‌باشد. اهمیت مقابله با محتوای خبری جعلی در سطح جهان به حدی است که از سال ۲۰۱۷، دوم آوریل هر سال

به‌عنوان «روز جهانی راستی‌آزمایی[1]» نام‌گذاری شده است. خبر جعلی قبل از سال ۲۰۱۶ اصطلاح پرکاربردی نبود؛ اما امروزه یکی از بزرگ‌ترین تهدیدها برای فرهنگ جوامع، دموکراسی، نظم، سیاست‌گذاری، برنامه‌ریزی، سلامت و برای انتخاب درست است. این اصطلاح پرکاربرد که همان اخبار جعلی[2] است در سال ۲۰۱۷ به‌عنوان واژه سال توسط واژه‌نامه کالینز[3] انتخاب شده است. در این میان موضوع «محتوای خبری جعلی» در مواجهه با سیل داده‌های خبری و اطلاع‌رسانی برجسته‌تر می شود، تا جایی که مردم عادی و حتی اصحاب رسانه نیز نیازمند راهکارها و دستورالعمل‌هایی هستند که بتوانند اخبار، تصاویر و فیلم‌های دستکاری شده را تشخیص دهند. این موضوع وقتی اهمیت مضاعف پیدا می‌کند که بدانیم سلاح نرمی بنام سلاح اجتماعی جوکر در سال‌های اخیر امنیت اجتماعی، فرهنگی و سیاسی کشورها را تهدید می‌نماید (مشابه ناآرامی‌های ایران و فرانسه در زمستان و بهار ۲۰۲۳). هدف اصلی این پژوهش بررسی راهکارهای رسانه‌ای در راستای مقابله با رویکرد فرهنگی سلاح اجتماعی جوکر می‌باشد. سؤال اصلی این است که آیا بین راهکارهای رسانه‌ای و رویکرد فرهنگی سلاح اجتماعی جوکر رابطه معنی‌داری وجود دارد؟ پژوهش حاضر فرض را بر این گرفته که بین راهکارهای رسانه‌ای و ناهنجاری‌های فرهنگی سلاح اجتماعی جوکر رابطه معنی‌داری وجود دارد.

۲ پیشینه تحقیق

این مقاله با هدف ارائه راهکارهای رسانه‌ای و راستی‌آزمایی محتوای رسانه‌ای جهت مقابله با رویکرد فرهنگی سلاح اجتماعی جوکر تنظیم شده و برای حکمرانی، مخاطبان و فعالین رسانه مفید خواهد بود. با توجه به نوظهور بودن سلاح اجتماعی جوکر، پژوهش‌های انگشت‌شماری در این مورد انجام شده است. بنابراین جهت ارائه راهکار نیاز به مطالعات جدیدی و جامع می‌باشد . با بررسی اطلاعات ارائه شده در بانک اطلاعاتی مقالات و پایان‌نامه‌ها[4] پی می‌بریم که پژوهش‌های انجام یافته در این بحث بیشتر از دید شناخت موضوع بوده است. با این حال در این تحقیق سعی شده موضوع راهکارهای رسانه‌ای در یک بخش تخصصی و با نگاه تأثیر بر رویکرد فرهنگی سلاح اجتماعی جوکر بررسی شود. با توجه به پژوهش‌های انجام یافته در این زمینه، موارد زیر در منابع خارجی ارائه شده اند. منابع داخلی در این موضوع یافت نشد.

- هلمز. جی. اس در مقاله‌ای به تحلیل روان‌شناختی عمومی سلاح اجتماعی جوکر پرداخته است.

Holmes, J. S. (2019). Journal of Popular Culture, 52(2), 465-479.

- در مقاله‌ای دیگر نویسنده به اهمیت آموزش رسانه‌ای و مهارت‌های رسانه‌ای در جامعه اشاره کرده است.

Huber, B., Borah, P., & Gil de Zúñiga,H. (2022) Journal of Media Literacy Education, 14(2), 1-14.

[1] Fact-Checking Day
[2] Fake news
[3] Collins Dictionary

[4] ایرانداک

- تری وینگارتنر و تری جونز در کتابی به بررسی روان‌شناسانه جوکر در زنان می‌پردازد.
Wingardner, T., & Jones, T. (2019). Sterling.

- جاناتان کریستوفر در مقاله‌ای دیگر به بررسی تأثیر جوکر بر جامعه پرداخته است.
Christopher, J. (2019). Philosophy Now, (132), 22-25.

- جان دو، در پایان‌نامه خود به بررسی ویژگی‌های جوکر و تأثیر آن بر روابطش با دیگران می‌پردازد.
Doe, J. (2018). (Master's thesis, University of California, Los Angeles).

- جیمز باتلر، به فلسفه جوکر به‌ویژه نیهیلیسم و هرج‌ومرج، نیز تأثیر آن بر روابط او با دیگران پرداخته است.
Butler, J. (2019). Journal of Popular Culture, 52(2), 480-494.

۳ مبانی نظری

در این بخش مفاهیم، نظریه‌ها و چارچوب نظری را مورد بررسی قرار می‌دهیم.

۱.۳ مفاهیم نظری

در این مقاله، برای توضیح مسئله و پاسخ‌های به‌دست آمده، به قرار زیر از برخی مفاهیم نظری استفاده شده است.

۱.۱.۳ راستی‌آزمایی محتوای رسانه‌ای خبری

راستی‌آزمایی محتوای خبری جعلی، فرآیند بررسی صحت گفته‌ها، اخبار، اظهارات، با استفاده از داده‌ها و اطلاعات معتبر را گویند (آزادی، ۱۳۹۹). در این فضا که افراد با حداقل‌ها و با کمترین توان علمی، به‌کمک اینترنت و رسانه‌های اجتماعی، هرزنامه‌ها، فیک نیوزها و مووها[۵] و نهنگ آبی‌ها[۶] را هدایت می‌کنند، لزوم شناخت و توسعه، مفاهیمی مانند: سواد رسانه‌ای، پدافند رسانه‌ای، سلاح اجتماعی جوکر و راستی‌آزمایی‌ها ظهور و نمود پیدا می‌کند.

۲.۱.۳ محتوای خبری جعلی، اخبار جعلی یا فیک نیوزها

مردم اخبار و محتوایی را تأیید می‌کنند که باورهای قبلی آنها را تأیید کند (تروور دیلا، سانگوون لیب، ۲۰۲۱) و مخاطبان هم معمولاً رسانه‌های همفکر را برای خبرگیری انتخاب می‌کنند. این همسویی باعث می‌شود اخبار جعلی خیلی راحت در بین مخاطبان مقبول افتد. ایران همواره در معرض آماج حملات خبرهای جعلی

[۵] چالش خودکشی در واتس‌اپ
[۶] بازی به قصد خودکشی

است به‌طوری که در بُعد تلویزیونی، ۲۸۴ شبکه فارسی‌زبان علیه ایران مشغول برنامه‌سازی هستند و مقابله با این حجم از اخبار جعلی نیازمند تدوین روش‌های راستی‌آزمایی محتوای خبری کارآمد می‌باشد.

۳.۱.۳ سلاح اجتماعی جوکر

یک تئوری است که بر اساس آن نهادهای قدرتمند به دست طرفدارانی از ایدئولوژی‌های راست و چپ و بین‌المللیسم، بهبود شرایط اجتماعی، سیاسی و فرهنگی جامعه را شناسایی و پیشنهاد می‌دهند، اما این اقدامات و تلاش‌ها به‌نحوی عملی نیست که بتوانند به بهبود دائمی منجر شوند. به‌عبارتی دیگر، به نظر می‌رسد که هدف نهایی این نهادهای قدرتمند، کنترل جامعه و کسب قدرت است و از جمله راهکارهایی که برای این منظور استفاده می‌شود، ایجاد هرج و مرج و تفرقه‌ای درون جامعه و نافرمانی‌های مدنی حتی تغییر فرهنگ‌ها (مانند فرهنگ حجاب اسلامی) در راستای اهدافشان می‌باشد. به عبارت دیگر، سلاح اجتماعی جوکر، نشان دهنده تناقضات و سیاست‌های متضاد نهادهای قدرتمند است که به‌مثابه نقشه فریب و کنترل جامعه عمل می‌کند. این تئوری در کره جنوبی، هنگ‌کنگ و اخیراً نیز در ایران (جنبش زن، زندگی، آزادی) و فرانسه اجرایی شده است. نیز از جدیدترین و مخرب‌ترین نوع سلاح‌های جنگ نرم می‌باشد. توسط این تئوری اعتراضات اجتماعی رادیکالی‌تر شده و به خشونت‌های جوکری کشیده می‌شود و هدف نهایی آن زمین سوخته و ویرانی کامل فرهنگی و اجتماعی می‌باشد.

۲.۳ نظریه‌ها

در ادامه نظریه‌هایی که برای تبیین و توضیح موضوع مقاله به کار رفته‌اند، مرور خواهند شد.

۱.۲.۳ نظریه جامعهٔ شبکه‌ای

از آنجا که کل تحولات و موضوع مورد اشاره در این مقاله، بر بستر «جامعهٔ شبکه‌ای» رخ می‌دهد، باید نسبت به این نظریه دید روشنی پیدا کنیم. بسیاری از نویسندگان، اصطلاح جامعهٔ شبکه‌ها را بر جامعهٔ اطلاعات ترجیح می‌دهند که «مانوئل کاستلز»، «جان ون دایک» و «یوزه ون دایک» از این دسته هستند. البته اندیشمند اخیر، در سال‌های گذشته از عبارت «جامعه پلتفرم» نیز بهره برده است (ون دایک، پل و دی وال، ۲۰۱۸)؛ اگرچه همه‌ی این نویسندگان از مفهوم جامعه‌ی اطلاعات نیز غفلت نمی‌کنند. جامعهٔ شبکه‌ای را می‌توان شکلی از جامعه تعریف کرد که به‌گونه‌ای فرآیند روابط خود را در شبکه‌های رسانه‌ای سامان می‌دهد؛ شبکه‌هایی که به‌تدریج، جایگزین شبکه‌های اجتماعی ارتباطات رودررو می‌شوند یا آنها را تکمیل می‌کنند. این بدان معنی است که شبکه‌های اجتماعی و رسانه‌ای در حال شکل دادن به شیوهٔ سازمان‌دهی اصلی و ساختارهای بسیار مهم جامعهٔ مدرن هستند. جامعه‌ی شبکه‌ای، در حال تغییر دادن همه‌ی مؤلفه‌های اساسی جامعه‌ی انسانی، از جمله خبر، اطلاع‌رسانی و فرهنگ است، که موضوع این مقاله خواهد بود. شیوه‌های شناختی انسانی و نسل‌های مأنوس با قواعد این جامعه، که از آنان به «بومیان سرزمین دیجیتال» یا «زاده سرزمین دیجیتال» یاد می‌شود، تغییرهای بنیادین به خود دیده و شرایط اجتماعی خاصی را در تولید، انتشار، بازنشر و دریافت محتواهای مختلف از جمله خبر، ایجاد خواهند کرد. پس از آن جهت، بستر اصلی تولید، انتشار و دیده شدن

خبرهای جعلی، به‌سبب حجم دسترسی شهروندان، سرعت بالای چرخش اطلاعات در این رسانه‌ها و عدم نظارت کافی بر آنها، رسانه‌های اجتماعی خواهند بود (ساعی و همکاران، ۱۳۹۸ب)، نظریه جامعه شبکه‌ای می‌تواند در تبیین هرچه بهتر مسئله پژوهش به ما کمک کند.

۲.۲.۳ نظریه حباب فیلتر

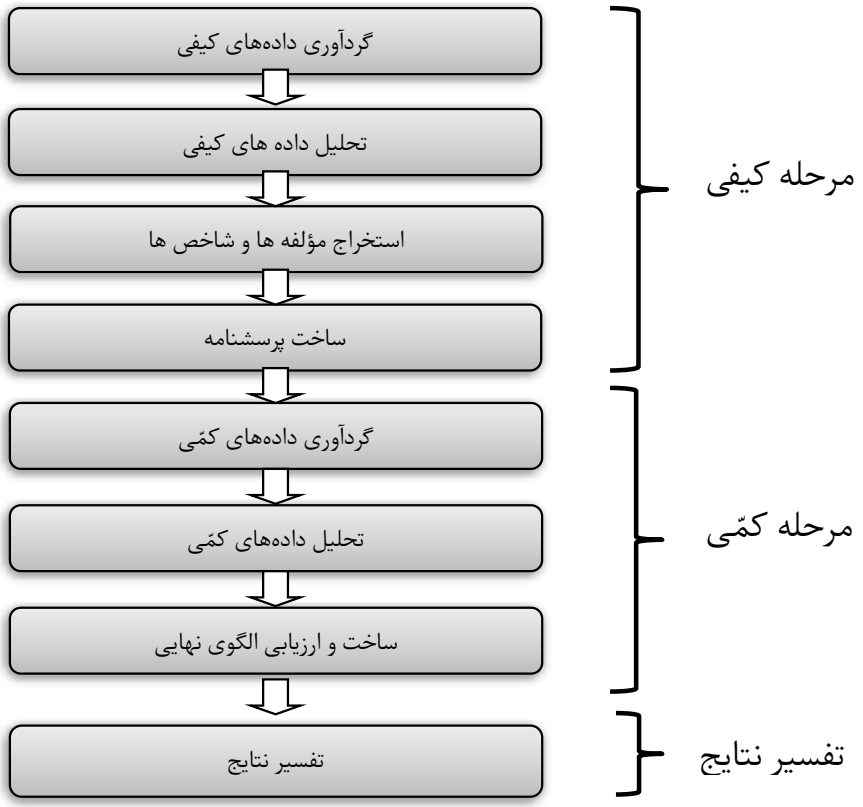
این نظریه، سعی دارد تا بستر اجتماعی لازم برای وقوع گسترده‌ی پدیده‌ی خبر جعلی که پشتیبان سلاح اجتماعی جوکر است را توضیح دهد؛ لذا در این مقاله به آن استناد شده است. حجم اطلاعات در جهان دیجیتالی امروز یک مشکل روبه رشد برای کاربران است. این مهم، نتیجهٔ ویژگی دوسویه گی و تعاملی بودن اینترنت و ورود صدها میلیون کاربر به فضای تولید محتوا در رسانه‌های اجتماعی است؛ علاوه بر این، بسترهای اطلاعاتی، افزایش زمان استفادهٔ کاربران از فضای برخط، تنظیماتی را تعبیه کرده اند که به احتمال زیاد منجر به تولید اطلاعات، واکنش به محتوا و کلیک کردن روی مطالب می شود (ویلمر و همکاران، ۴۱:۲۰۱۸). نتیجه آنکه، در این فضای جدید، علاوه بر تولید داده‌های دیجیتال توسط رسانه‌های رسمی، ارگان‌ها و سازمان‌ها، کاربران عادی هم به طور لحظه ای، حجم انبوهی از داده‌ها را از متن گرفته تا عکس، صوت و ویدئو در فضای مجازی منتشر و بازنشر می کنند. این مسئله اگرچه در ابتدا، برای حضور و فعالیت کاربران جذابیت زیادی داشت، اما پس از مدتی این «آلودگی اطلاعاتی» زمینهٔ کاهش جذابیت را ایجاد می کرد.

با توجه به ظهور الگوریتم‌های یاد شده، برخی از پژوهشگران، برخلاف نظر گروهی که معتقد به افزایش تنوع اطلاعاتی در عصر اینترنت و رسانه‌های اجتماعی هستند، معتقدند رسانه‌های مبتنی بر اینترنت منجر به اثری به نام «حباب فیلتر» شده‌اند؛ به این معنا که الگوریتم‌های شخصی‌سازی در فضای اینترنت باعث می‌شوند تا کاربران تنها، اطلاعات و محتواهای خاصی را که مورد پسندشان است مشاهده کنند (پاریزر، ۲۰۱۱) و در یک فضای اطلاعاتی محدود محصور شوند، از این رو تنوع اطلاعات قابل مشاهده برای کاربران، محدود می‌شود (لیز، ۲۰۱۴). پدیده‌ای که منجر به کاهش و حتی به صفر رسیدن مواجهه کاربران با ایده‌ها، اندیشه‌ها و افکار متفاوت و متضاد با آنها خواهد شد.از آنجا که خبر جعلی، به‌لحاظ ساختاری و محتوایی، تصویری غلط و اشتباه از جهان اطراف را برای کاربران پدید می‌آورد، اگر این کاربر، منابع رسانه‌ای خود را خواسته یا ناخواسته شخصی‌سازی کرده و در حباب فیلتر گیر افتاده باشد، تأثیر عمیقی بر فکر و ذهن و باورهای فرهنگی در زندگی فردی و اجتماعی ایجاد خواهد شد. در واقع این شخص، در دنیایی از اطلاعات غلط زندانی می‌شود، بدون آنکه از این موضوع مطلع باشد.

۴ روش تحقیق

از نظر هدف با توجه به اینکه پژوهش حاضر به بررسی راهکارهای رسانه‌ای جهت مقابله با رویکرد ضد فرهنگی سلاح اجتماعی جوکر می‌پردازد، در حیطه تحقیق کاربردی طبقه‌بندی میشود. همچنین، از نظر چگونگی گردآوری داده‌های مورد نیاز، در گروه «تحقیق آمیخته اکتشافی» می‌باشد. برای این منظور ابتدا داده‌های کیفی گردآوری شده که منجر به شناسایی جنبه‌های متعدد پدیده شده و امکان تدوین الگوی مفهومی تحقیق

فراهم میشود، سپس بر مبنای یافته‌های حاصل از دادههای کیفی ابزار تحقیق ساخته و دادههای کمی گردآوری شدند تا تعمیم‌پذیری یافته‌ها میسر شود. به‌طور کلی دلایل انتخاب روش تحقیق آمیخته برای تحقیق حاضر شناسایی ابعاد مختلف تأثیر محتوای خبری جعلی در رویکرد فرهنگی سلاح اجتماعی جوکر، ارزیابی الگوهای راستی‌آزمایی محتوای رسانه‌ای جعلی با رویکرد سلاح اجتماعی جوکر، لزوم استفاده از دیدگاههای خبرگان دانشگاهی متخصص این مهم می‌باشد.پس با توجه به موارد فوق، مراحل تحقیق حاضر به شیوه‌ای که در شکل ۱ آمده انجام شد.



شکل ۱: مراحل روش پژوهش

۱.۴ روش پژوهش در بخش کیفی

در این فاز بحث نقش محتوای خبری جعلی بر رویکرد ضد فرهنگی سلاح اجتماعی جوکر و نیز شناسایی مدل در خصوص ارائه الگوی راستی‌آزمایی محتوای خبری جعلی در راستای خنثی‌سازی اهداف ضد فرهنگی سلاح اجتماعی جوکر که یک «موقعیت نامعین» است مورد بررسی و موشکافی قرار گرفته است. در فاز کیفی با استفاده از مصاحبهٔ کیفی با متخصصان رسانه، و خبرگان دانشگاهی که دارای شناخت کافی از موضوع باشند، در دستور کار بود. مصاحبه‌ها تا آنجا ادامه یافت تا جنبهها و مؤلفههای نهفته و گوناگون پدیدهٔ مدل در

خصوص تأثیر محتوای خبری جعلی بر سلاح اجتماعی جوکر مورد شناسایی و توصیف قرار گرفته و به اشباع نظری رسد. در این مرحله، از روش اکتشافی متوالی استفاده شد که در زمرهٔ روش‌های پژوهش کیفی قرار دارد.

۲.۴ روش و ابزار گردآوری داده‌ها و اطلاعات در بخش کمی

روش تحقیق حاضر از نظر هدف کاربردی و از نظر ماهیت و روش، روشی توصیفی-پیمایشی است، تحقیق از این نظر کاربردی است که نتایج آن برای کاربران و فعالین رسانه قابل استفاده است، چون به رابطه محتوای خبری جعلی و رویکرد فرهنگی سلاح اجتماعی جوکر می‌پردازد و از این جهت توصیفی است، که به فرآیندهای جاری و آثار مشهود در زمان حال توجّه داشته و وضعیت موجود میان متغیرها را شناسایی می‌نماید.

۵ یافته‌های پژوهش

۱.۵ فیک‌نیوزها و اخبار جعلی ابزاری برای تقویت رویکرد مخرب فرهنگی سلاح اجتماعی جوکر

خبرهای جعلی به‌عنوان مهم‌ترین ابزار سلاح اجتماعی جوکر به‌طور گسترده در شبکه‌های اجتماعی و رسانه‌ها منتشر می‌شوند و ممکن است تأثیرات جدی بر فرهنگ جوامع داشته باشند، از جمله ناهنجاری‌های فرهنگی و اجتماعی افزایش اضطراب، افزایش ترس و نگرانی‌ها و حتی تحریک به خشونت. به‌عنوان مثال، خبر جعلی و سلاح اجتماعی جوکر، ممکن است باعث شوند که برخی افراد برای خرید سلاح‌های دفاع شخصی در راستای تأمین امنیت خود اقدام کنند که این امر می‌تواند به افزایش خطرات و احتمال وقوع خشونت در جامعه منجر شود.

به‌طور کلی، تحقیقات نشان داده است که خبرهای جعلی می‌توانند تأثیرات منفی بر روی رفتار افراد داشته باشند و به‌عنوان یکی از عوامل مؤثر در ایجاد ترس و نگرانی‌ها و افزایش اضطراب در جامعه شناخته می‌شوند. به‌عنوان مثال، یک مطالعه در سال ۲۰۱۸ نشان داد که خبرهای جعلی در مورد ویروس‌های جدید می‌توانند به افزایش ترس و نگرانی‌ها در جامعه منجر شوند و در نتیجه ممکن است به افزایش شیوع بیماری کمک کنند. با این اوصاف می‌توان گفت محتوای خبری جعلی می‌تواند عامل تشدید و تقویت اهداف سلاح اجتماعی جوکر باشد.

سلاح اجتماعی جوکر جدیدترین نوع سلاح نرم در عصر حاضر می‌باشد که مستقیماً با تأثیر بر رفتار و فرهنگ افراد آنها را جهت شورش‌ها و اغتشاشات خیابانی تحریک می‌کند و ابزار اصلی آن (به‌عبارتی خشاب آن) رسانه‌ها و محتوای رسانه‌ای جعلی می‌باشند. محتوای خبری جعلی در مورد سلاح اجتماعی جوکر، باعث افزایش اضطراب و ترس در جامعه می‌شود. این نوع اخبار، علاوه بر ایجاد اضطراب، می‌تواند باعث بروز اختلالات رفتاری و روانی در افراد شود.

یکی از مطالعاتی که در این زمینه انجام شده است، مطالعه‌ای است که توسط دانشمندان از دانشگاه کالیفرنیا صورت گرفته است. در این تحقیق، مشاهده شد که افرادی که با خبرهای جعلی درباره تهدیدات

امنیتی مواجه شده بودند، دچار اضطراب شدید و خود را در معرض خطر می‌دانستند. همچنین، این افراد با عدم اطمینان و اعتماد به نفس مواجه بودند و نمی‌توانستند به درستی تصمیم بگیرند.

مطالعات دیگر نیز نشان داده است که خبرهای جعلی می‌توانند باعث تغییرات شدید در رفتار و عملکرد افراد شوند. به‌عنوان مثال، در یک تحقیق دیگر، مشاهده شد که افرادی که با خبرهای جعلی درباره انتخابات مواجه می‌شوند، به اندازه کافی احساس ناامنی می‌کنند تا از رأی دادن خودداری کنند. همچنین، خبرهای جعلی می‌توانند باعث ایجاد تنش و ناهنجاری در ارتباطات فرهنگی و اجتماعی شوند.

بنابراین، محتوای خبری جعلی در مورد سلاح اجتماعی جوکر، می‌تواند تأثیرات شدیدی بر روی رفتار و روانی افراد داشته باشد. به همین دلیل، باید از منابع معتبر و قابل اطمینان استفاده کرد.

۲.۵ تقویت فعالیت مراکز دانشگاهی و علمی در جهت ارائه راهکارهایی برای راستی‌آزمایی محتوای خبری جعلی (رویکرد حکمرانی)

دانشگاه‌ها با بازوهای علمی و عملی همانند دفاتر ارتباط با صنعت، مراکز رشد، پارک‌های علم و فناوری، سراهای نوآوری، هسته‌های پژوهشی و شرکت‌های وابسته دانش‌بنیان می‌توانند خدماتی مفید در جهت صدور دستورالعمل‌های فناورانه کاربردی ارائه نمایند. با پیوند مراکز دانشگاهی و مراجع تصمیم‌گیری در کشور پژوهش‌های خود را به سوی موضوعات کاربردی سوق دهند. نتیجه این همکاری‌های علمی خروجی مثبت، در جهت تدوین الگوهایی برای علوم نوین خواهد داشت.

۳.۵ معرفی و آموزش بکارگیری نرم‌افزارها و سخت‌افزارهای آموزشی و بازی‌های کامپیوتری و آن‌لاین، مانند بازی واقعیت مجازی در رسانه‌ها جهت آشنایی با آسیب‌های فرهنگی (رویکرد معرفی فناوری‌های شناخت)

نرم افزارهای واقعیت مجازی می‌توانند به شکل مؤثری در پرورش نیروهای حرفه‌ای مورد استفاده قرار گیرند. ترکیب آن با قابلیت‌های آموزش مجازی، دیدگاه منحصر به‌فردی در پیشرفت روش‌های کاری افراد و آموزش نحوه استفاده از کامپیوترهای شخصی‌شان ایجاد می‌کند. از طریق شبیه‌سازی با استفاده از واقعیت مجازی می‌توان بازی‌هایی ترتیب داد که افراد در آن به بررسی و راستی‌آزمایی محتوا، پرداخته و سلاح جوکر را بشناسند.

۴.۵ جلب توجه مخاطبان در برنامه‌سازی به اعتبار رسانه یا اعتماد به رسانه‌ها (رویکرد فرهنگ سازی)

دو واژه اعتبار[۷] و اعتماد[۸] معانی مرتبط اما متفاوت دارند که البته در بسیاری موارد به‌جای یکدیگر و بعضاً با بی‌دقتی مورد استفاده قرار می‌گیرند. اعتبار به درستی و دقت یک متن باز می‌گردد، در حالی که اعتماد، به میزان باور مخاطبان به‌درستی متن مربوط است؛ در واقع در بسیاری موارد به جای واژه اعتماد، به‌درستی از

[7] Credit
[8] the trust

جدول ۱: برنامه‌های تلویزیونی راستی آزمایی

	عنوان	رویکرد	سازنده
۱	Show FakeNews The	طنز و راستی‌آزما	انگلیس
۲	CNNNN	به چالش کشیدن کانال سی ان ان و فاکس نیوز با طنز	استرالیا

عبارت اعتبار از دید مخاطب استفاده می‌شود. به‌عنوان مثال تحقیقی که به‌دنبال یافتن میزان دقت و صحت مطالبی است که در ویکی پدیا منتشر می‌شود، در واقع مفهوم اعتبار را دنبال می‌کند، اما پژوهشی که به‌دنبال مطالعه اعتبار از دید افراد است، همان اعتماد می‌باشد. ممکن است، کوچک‌ترین توجهی به این که واقعاً محتوای مورد بحث چقدر دقیق و قابل اطمینان است، نداشته باشد و صرفاً میزان اعتماد افراد را بسنجد.

۵.۵ آموزش توجه به نوع رسانه‌ها (رویکرد فرهنگ‌سازی)

به‌لحاظ نظری برخی از انواع رسانه ممکن است از انواع دیگر معتبرتر دانسته شوند. مثلاً ممکن است کسی استدلال کند که روزنامه از این جهت که قبل از چاپ و انتشار مورد بررسی قرار می‌گیرد و ویرایش می‌شود قابل اطمینان‌تر است. شایدفردی بگوید که اینترنت فضایی آزاد است و لذا مطالبش مورد اطمینان‌تر است. در دیدگاهی، یک شبکه تلویزیونی از اینترنت معتبرتر دانسته می‌شود. بنابراین آموزش توجه به نوع رسانه در برنامه‌های تلویزیونی در راستای مقابله با جنگ شناختی خواهد بود.

۶.۵ راه‌اندازی شبکه‌ها یا برنامه‌های تلویزیونی راستی‌آزمایی محتوا (رویکرد حکمرانی رسانه‌ای)

شبکه‌ها و برنامه‌های سیاسی، مخاطب بالایی دارند. برنامه‌ها و شبکه‌های بررسی اخبار و محتواهای منتشر شده روز، نیز توسط مخاطبان، با استقبال مواجه می‌شوند. در جدول ۱ به دو مورد از برنامه‌های تلویزیونی راستی‌آزما-محور اشاره می‌شود که تأثیر زیادی در شفاف‌سازی داشته‌اند.

۷.۵ توجه به جعل عمیق و استفاده از ابزار مبارزه با جعل عمیق از ملزومات دنیای فضای مجاز (رویکرد معرفی فناوری‌ها)

با هدف مبارزه با این روند منفی نوظهور اما بسیار قوی، مایکروسافت از دو ابزار رونمایی کرد: «مایکروسافت ویدئو اسنتی‌کیتور[۹]» که برای تجزیه‌وتحلیل تصاویر ثابت و ضبط‌های ویدئویی با هدف شناسایی دستکاری‌های احتمالی استفاده می‌شود، و همچنین ابزاری که در«مایکروسافت آزوور[۱۰]» تعبیه شده و قادر به شناسایی محتوای دستکاری‌شده است. همچنین، این دستاورد به‌گونه‌ای طراحی شده که می‌تواند به افراد بگوید ویدیوهایی که در حال مشاهده آن هستند، معتبر است یا خیر.

[9] Microsoft Video Authenticator
[10] Microsoft Azure

جدول ۲: سایت‌های واقعیت‌سنج

ابزار واقعیت سنج	نحوه عمل
POLITIFACT	دسته بندی محتوا به درست، تقریبا درست، نیمه درست، تقریبا نادرست، نادرست و سوزاندنی
FACTCHECK	وجود گزینه «پرسش» بالای سایت جهت ارسال درخواست بررسی صحت محتوای مخاطب
SNOPES	جدا از درستی یا نادرستی به مواردی مانند «سوء استفاده » و «بدجنسی » نیز اشاره می شود

۸.۵ فرهنگ سازی رسانه‌ای در راستای ارتقاء انواع سواد در کاربران (رویکرد فرهنگ‌سازی)

– سواد خبری – سواد بصری – سواد اطلاعاتی – سواد رسانه‌ای؛ با گسترش بسترهای رسانه‌ای، جوامع مجبور به داشتن آگاهی در مسائل رسانه‌ای می‌باشند. سواد رسانه‌ای نوعی درک متکی بر مهارت است که می‌توان بر اساس آن انواع محتوا را تشخیص داد. رنه‌هابز، سه فریم را برای معرفی سواد رسانه‌ای به زبان‌آموزان مشخص می‌کند: نویسندگان، مخاطبان، پیام‌ها و بازنمایی واقعیت. وی در سنتز ادبیات از سواد رسانه‌ای، سواد اطلاعاتی، سواد بصری و سواد جدید، این ایده‌های اصلی را شناسایی می‌کند که زمینه نظری برای سواد رسانه‌ای را تشکیل می‌دهد.

۹.۵ معرفی واقعیت‌سنج‌ها و تشویق به استفاده از سایت‌های تشخیص محتوای جعلی (رویکرد معرفی فناوری‌ها)

مانند آنچه که فارس‌نیوز، خبرآنلاین و سایت خبر خوب یا سایت‌های واقعیت‌سنج انجام میدهند؛ بسیاری از رسانه‌ها و پایگاه‌های اینترنتی ایرانی تلاش می‌کنند همواره واقعیت را بنویسند، اما در ایران رسانه‌ها و سایت‌هایی با عنوان صریح «واقعیت‌سنج» به معنای واقعی وجود ندارند! با این حال «واقعیت‌سنج»های غربی نیز گاهی اخبار ایران را بررسی می‌کنند که در جدول ۲ به چند مورد از واقعیت‌سنج‌های رایج در دنیا اشاره می‌کنیم.

۱۰.۵ آموزش استفاده از واقعیت‌سنج‌ها و فکت‌چک‌های رسانه‌های اجتماعی و سایر رسانه‌های خبری منطقه‌ای (رویکرد معرفی فناوری‌ها)

استفاده از برخی بخش‌ها یا امکانات و قابلیت‌ها در گوگل، فیس‌بوک، توییتر و ... جهت راستی‌آزمایی محتوای رسانه‌ای نیز به راستی‌آزمایی محتوای رسانه‌ای کمک می‌کند که در جدول ۳ به آنها اشاره می‌شود.

جدول ۳: واقعیت سنج‌های رسانه‌های اجتماعی و خبری

عنوان	روش	بکارگیری در
راستی آزمایی	بررسی صحت محتوا با واقعیت سنج‌ها	گوگل، فیسبوک
هشدار	هشدار به ناشرین محتوای فیک و توهین	اینستاگرام، توییتر
لینک دادن	افزودن لینک‌های مرتبط به محتوای منتشر شده	توییتر، گوگل
استفاده از نشان	افزودن تیک‌های رنگی به ناشران محتوا	فیسبوک، اینستاگرام، تلگرام
فکت نامه‌ها	به راستی آزمایی محتوای تخصصی	فکت نامه، فالس نیوز فارس
حذف خودکار	حذف محتوا با هوش مصنوعی	اینستاگرام
برچسب زنی	افزودن برچسب تاییدی به انتهای متن محتوا	گوگل
کدگذاری	کد دهی به محتوا و ارجاع به متن اصلی	ایران اینترنشنال

۱۱.۵ معرفی موتورهای جستجوی محتوای جعلی (رویکرد معرفی فناوری‌ها)

معرفی برخی موتورهای جست‌وجو ویژه تشخیص محتوای جعلی مانند«هوآکس[11]» در راستی‌آزمایی محتوای رسانه‌ای، گامی ضروری به‌نظر می رسد. البته با توجه به اینکه این موتورها، از هوش مصنوعی استفاده می‌کنند درصد اطمینان کمتری دارند. سایت‌هایی که محتوای جعلی و تحریف‌شده منتشر می‌کنند، معمولاً از زبان احساسی و هیجانی برای بیان استفاده می‌کنند تا آب‌وتاب بیشتری به خبر بدهند. الگوریتم هوش مصنوعی جدید می‌تواند ارتباط میان اعتبار یک سایت و صفحه ویکی‌پدیا و نشانی وب‌سایت آن را شناسایی کند. هرچه صفحه ویکی‌پدیای یک سایت اطلاعات بیشتری داشته باشد، قابل اعتمادتر است. نیز هرچه نشانی سایت پیچیده‌تر باشد احتمال این‌که اخبار جعلی و تحریف‌شده منتشر کند نیز بیشتر است.

۱۲.۵ آموزش استفاده از الگوهای شناخت محتوای خبری جعلی در فضای مجازی با مصادیق

آموزش استانداردهای شناخت یک محتوای جعلی بر پایه مطالعات کتابخانه‌ای (جدول ۴ و ۵).

۱۳.۵ ترویج راهکارهای فردمحور مقابله با محتوای جعلی (رویکرد فرهنگ‌سازی)

راهکارها و پیشنهاداتی برای جلوگیری از نشر محتوای جعلی ارائه شده است. راهکارهای نرم‌افزاری که شرکت‌های بزرگ مانند مایکروسافت، گوگل و فیس‌بوک ارائه کرده‌اند، ولیکن نکته‌ای که باید توجه کرد این است که: اولاً امکانات نرم‌افزاری شاید هیچ‌گاه نخواهند توانست به‌صورت قطع یقین، محتوای اصلی را از جعلی، تمیز دهند! چرا که گاهی منبع انتشار این محتواها، برخی رسانه‌های معتبر و حرفه‌ای می‌باشند. به‌همین دلیل، مؤثرترین راهکار مقابله با محتوای جعلی، کنترل توسط عوامل انسانی می‌باشد، یعنی در کنار مقابله با تولید و انتشار محتوای جعلی، مخاطبان را با راستی‌آزمایی محتوای رسانه‌ای، آشنا کرده و این فرهنگ ترویج

[11] Hoax

جدول ۴: جدول روش‌های شناخت یک محتوای خبری جعلی بر پایه مطالعات کتابخانه ای

	الگوهای شناخت محتوای جعلی در فضای مجازی
۱	دامنه مشکوک دارد ممکن است به چیزی مانند ".com.co" ختم شود
۲	تنها به یک منبع یا هیچ منبعی اشاره نمی‌کند
۳	محتوا پیرامون حدس و گمان تدوین می‌شوند
۴	محتوا در مورد یک نظر واحد شکل می‌گیرند، نه همه طرف‌ها از دیدگاه‌های مختلف داستان
۵	محتوا با زبان احساسات، تزئین شده است
۶	حالت‌ها یا وضعیت‌های نظریه‌های توطئه دارند
۷	تعصب حزبی سنگین در آن احساس می‌شود
۸	هیچ محتوای رسانه‌ای، در مورد آنها گزارش نشده است
۹	تاریخ و زمان انتشار قدیمی یا اصلاً هیچ یک را یادداشت نمی‌کند
۱۰	بررسی منبع اصلی علاوه بر نوع خبر، بررسی وب‌سایت اصلی، ماموریت، و اطلاعات تماس آن
۱۱	بررسی خبر از جهت رویکرد تبلیغاتی یا کلیک‌خوری آن
۱۲	بررسی نام نویسنده. آیا فرد قابل اطمینانی است؟ آیا واقعی است؟
۱۳	خبر، منبع تأییدکننده هم دارد؟
۱۴	بازبینی تاریخ خبر ارسال دوباره اخبار قدیمی به این معنا نیست که به رخدادهای جاری مربوط اند
۱۵	آیا خبر، شوخی نیست؟ شاید طنز بوده. برای اطمینان، سایت و نویسنده را بررسی کنید
۱۶	توجه به سوگیری‌های خود توجه داشته باشید که باورهای خود شما ممکن است بر قضاوتتان اثر بگذارد
۱۷	پرسش از کارشناسان، از یک کتابدار بپرسید، یا به یک سایت واقع‌نما مراجعه کنید

جدول ۵: جدول راهکارها و روش‌های شناخت محتوای واقعی بر پایه مطالعات کتابخانه‌ای

ردیف	الگوهای شناخت محتوای واقعی
۱	منابع مختلف را از دیدگاه‌های مختلف ذکر می‌کند
۲	زبانش ارائه ساده است
۳	حقایق با گزارش یا آمار اثبات می‌شوند
۴	حقایق جایگزین را ذکر نمی‌کند، به‌عبارتی طفره نمی‌رود
۵	تیتر حقایق را بیان می‌کند و منعکس‌کننده محتوا است
۶	شامل تمام عناصر یک داستان است نه فقط اجزای انتخابی
۷	حداقل تعصب حزبی را دارد
۸	خبرنگار، دارای سابقه‌ای معتبر از محتواهای رسانه‌ای، منصفانه است
۹	تاریخ و زمان انتشار جدید است

شود که حداقل، اگر به صحت محتوا یقین نیست، از بازنشر آن خودداری شود.

۱۴.۵ اصلاح برخی فرهنگ‌های غلط توسط مدیران بستر رسانه (رویکرد فرهنگ‌سازی)

دروغ سیزده، دروغ اول آوریل در فرهنگ ملل، نمونه بارز ترویج محتوای جعلی می‌باشد. این افکار ریشه در فرهنگ عمومی دارند، که باید اصلاح گردند. یکی از راه حل‌هایی که می‌تواند هزینه‌های این پدیده را برای یک جامعه کاهش دهد، فرهنگ است و این فرهنگ باید بر بستر یک سواد رسانه‌ای بنشیند تا مخاطب تحت تأثیر هر خبری که می‌خواند قرار نگیرد، و از تأثیر آن مصون بماند. در سال ۲۰۲۲ گوگل اعلام کرد که لزوم افزایش مسئولیت اجتماعی آن در بحران کنونی، رسم همیشگی و قدیمی دروغ آوریل را کنار خواهد گذاشت.

۶ ارائه و تحلیل داده‌ها

داده‌های به دست آمده در این پژوهش، به‌عنوان راهکارهایی جهت شناخت محتوای خبری جعلی با رویکرد، و مقابله با اهداف سلاح اجتماعی جوکر بر اساس نظام مقوله‌بندی و گزاره‌بندی در قالب مقوله‌های، رویکرد فرهنگ‌سازی در در شناخت محتوای خبری جعلی، رویکرد حکمرانی در شناخت محتوای خبری جعلی و نهایتاً رویکرد فناوری‌محور تقسیم شده‌اند. مقوله‌بندی، کدگذاری و گزاره‌های مرتبط با هر مقوله در جدول‌های ۶، ۷ و ۸ و تحلیل آنها به این شرح است. مهم‌ترین مقوله‌های مورد تأکید، فرهنگ‌سازی در شناخت محتوای خبری جعلی در راستای مقابله با اهداف سلاح اجتماعی جوکر، عبارت بودند از:

الف. فرهنگ‌سازی در جهت اصلاحات فرهنگی

ب. نیاز ضروری بستر رسانه‌ای به ارتقاء انواع سواد در کاربران

ج. ترویج راهکارهای فردمحور مقابله با محتوای جعلی

مصاحبه شوندگان مقوله‌های فرهنگی را نیاز ضرورت بستر شناخت محتوای خبری جعلی و مقابله با سلاح اجتماعی جوکر دانسته و توجه به آنها را توصیه نموده اند.

مهمترین مقوله‌ها، در زمینهٔ روش‌های حکمرانی در راستای مقابله با محتوای جعلی رسانه‌ای، عبارت بودند از:

الف. راه اندازی شبکه‌ها یا برنامه‌های رادیویی و تلویزیونی راستی‌آزما

ب. بررسی قوانین بازدارنده دنیا در برنامه‌های تلویزیونی

مصاحبه‌شوندگان نقش عوامل حکمرانی جهت تأمین اهداف مقابله با جنگ شناختی را غیر قابل انکار توصیف کرده و یکی از اصلی‌ترین مقوله‌های مقابله با سلاح اجتماعی جوکر معرفی نموده‌اند.

جدول ۶: جدول مقوله‌بندی رویکرد فرهنگ‌سازی در شناخت محتوای خبری جعلی

	مقوله‌های فرهنگی	مصاحبه شونده	گزاره‌ها
۱	ترویج راهکارهای فردمحور مقابله با محتوای جعلی	کد ۶ کد ۴	هوش ماشین ظرافت و انعطاف نیروی انسانی را ندارد مخاطبان برای مواجهه با محتوای جعلی باید آگاه شوند
۲	اصلاح برخی فرهنگ‌های غلط	کد ۱	دروغ سیزده و دروغ اول آوریل در فرهنگ ملل، نمونه بارز ترویج محتوای جعلی
۳	توجه دادن به مرامنامه، خط مشی و اسپانسرهای منبع محتوا	کد ۹	مرامنامه و خط مشی رسانه مرجع مطمئنی برای راستی آزمایی محتوای رسانه‌ای می باشد
۴	جلب توجه به اعتبار رسانه یا اعتماد به رسانه‌ها	کد ۱	اعتبار به درستی و دقت یک متن است اعتماد، میزان باور مخاطبان به درستی متن است
۵	آموزش توجه به نوع رسانه‌ها	کد ۳	برخی از انواع رسانه از انواع دیگر معتبرترند
۶	نیاز به ارتقاء انواع سواد کاربران	کد ۷	جوامع مجبور به داشتن آگاهی در مسائل رسانه‌ای اند
۷	آموزش استفاده از الگوهای شناخت	کد ۸	از لحاظ ظاهری می توان فیک نیوزها را شناخت

جدول ۷: جدول مقوله بندی رویکرد حکمرانی رسانه‌ای شناخت محتوای خبری جعلی

ردیف	مقوله‌های تدابیر حکمرانی	مصاحبه شونده	گزاره‌ها
۱	راه اندازی شبکه‌ها یا برنامه‌های رادیویی و تلویزیونی راستی آزما	کد ۵	برنامه‌ها و شبکه‌های، بررسی اخبار و محتواهای منتشر شده روز، نیز توسط مخاطبان، با استقبال مواجه خواهد شد.
۲	بررسی قوانین بازدارنده دنیا در برنامه‌های تلویزیونی	کد ۱۲	قانون بهبود تنفیذ قوانین در شبکه‌های اجتماعی آلمان
		کد ۶	فرانسه قانون نفرت پراکنی برخط را تصویب نموده است
		کد ۸	مالزی لایحه ضد اخبار جعلی
		کد ۱	سنگاپور الزامات قانونی برای تولید محتوا ارائه کرده است
۳	بررسی تقویت و نقش مراکز علمی	کد ۷	مراکز رشد، پارک‌های علم و فناوری، سراهای نوآوری، هسته‌های پژوهشی و شرکت‌های دانش‌بنیان

جدول ۸: مقوله بندی معرفی فناوری‌های اطلاعاتی راستی‌آزما در شناخت محتوای خبری جعلی

	مقوله‌های تدابیر فناورانه	مصاحبه شونده	گزاره‌ها
۱	توجه دادن ویژه به جعل عمیق	کد ۷	استفاده از ابزار مبارزه با جعل عمیق از ملزومات فضای مجازی Authenticator Video Microsoft Azure Microsoft -
		کد ۳	استفاده از سایت‌های تشخیص محتوای جعلی - POLITIFACT SNOPES - FACTCHECK
۳	معرفی واقعیت سنج‌ها و فکت چک‌های رسانه‌های اجتماعی	کد ۳	استفاده از واقعیت سنج‌ها و فکت چک‌های فیسبوک، اینستا
۴	معرفی موتورهای جستجوی محتوای جعلی	کد ۱	معرفی موتورهای جستجو ویژه تشخیص محتوای جعلی مانند Hoax

مهمترین مقوله‌های مورد تأکید مصاحبه‌شوندگان، در زمینهٔ معرفی تدابیر فناورانه مقابله با محتوای خبری جعلی و مقابله با سلاح اجتماعی جوکر عبارت بودند از:

الف. معرفی سایت‌های تشخیص محتوای جعلی

ب. معرفی واقعیت‌سنج‌ها و فکت‌چک‌های رسانه‌های اجتماعی

ج. توجه دادن ویژه به جعل عمیق

سایت‌های واقعیت‌سنج و ابزار واقعیت‌سنج رسانه‌های اجتماعی موجود در بستر آن‌لاین ابزارهای مؤثری هستند که می‌توان با استفاده از آنها به مقابله با محتوای جعلی رفت. بررسی کارشناسی ایجاد سایت‌های واقعیت‌سنج بومی و استفاده از متدهای جهانی آنها نیز باید در دستور کار مدیران رسانه قرار بگیرد.

مؤلفه‌های شناخت اخبار جعلی و نیز مؤلفه‌های شناخت خبر درست نیز مورد تأیید و تأکید مصاحبه‌شوندگان قرار گرفت. استانداردهای شناخت به مخاطبان می‌آموزند که هر خبر و محتوایی را بدون تحقیق نپذیرند و نیز به فعالین رسانه کمک می‌کند تا قبل از انتشار اخبار آن را راستی‌آزمایی کنند.

۷ بحث و نتیجه‌گیری

در عصر اطلاعات، واژگان جدید و متفاوتی همچون «رسانه»، «جنگ شناختی»، «سلاح اجتماعی جوکر»، «اخبار جعلی» و ... به دایره‌ی اصطلاحات رسانه‌ای ما افزوده شده است که نشان از ضرورت تأمل و تدبر بیش از پیش بر محتوای منتشره از سوی انواع رسانه‌ها، تلویزیون‌های بیگانه، بالاخص رسانه‌های آن‌لاین (به‌دلیل

سرعت در نشر خبر و امکان تکذیب فوری) دارد. رسانه‌های آن‌لاین که طی سال‌های اخیر رشد و گسترش چشم‌گیری داشته‌اند، امروزه پرچم‌دار دیگر رسانه‌ها محسوب می‌شوند. سرعت در انتشار اخبار، کوتاه‌نویسی و سهولت مخاطب در دسترسی به اخبار از مزیت‌های اصلی رسانه‌های آنلاین محسوب می‌شود. اما همین رسانه‌ها، معایبی نیز به همراه دارند که در صورت پایین بودن اطلاعات مخاطب و همچنین عدم توسل به سواد رسانه‌ای، می‌تواند آسیب‌زا نیز باشند. بدان معنا که اگر فردی درباره‌ی موضوعی خاص، اطلاعات و آگاهی کافی نداشته باشد، بی‌شک توانایی تمییز محتوای درست از نادرست را نداشته و به همین دلیل، در کنار پروپاگاندای گسترده‌ی انواع رسانه‌ها و حباب فیلتر محتوایی، گرفتار گرداب محتوای خبری جعلی خواهند شد. امروزه تکنیک‌های تولید محتوای جعلی به قدری پیشرفت نموده است که، حتی نخبگان رسانه و سواد رسانه‌ای نیز در معرض تهدید می‌باشند. در این راستا کنترل بر تولید و انتشار محتوا، با این حجم از انتشار، امری بس دشوار به‌نظر می رسد. حتی در مقاطعی، کنترل محتوای رسانه‌ای در تقابل با دموکراسی و آزادی اندیشه تفسیر خواهد شد. جدیدترین کارکرد رسانه‌ها، پشتیبانی از سلاح اجتماعی جوکر می باشد. سلاحی که هدف نهایی آن زمین سوخته بوده و با ابزار محتوای خبری جعلی رسانه‌ای، مخاطبان را به‌سمت زمین سوخته هدایت می‌کند. بنابراین برای مقابله با تهدیدات محتوای خبری جعلی و سلاح اجتماعی جوکر نیازمند توجه جدی به موارد پیشنهاد شده در پژوهش حاضر می‌باشند. در پاسخ به پرسش اصلی، نتایج این پژوهش در نخستین گام نشان داده شد که بین راهکارهای رسانه مبتنی بر شناخت محتوای خبری جعلی و اهداف فرهنگی و اجتماعی به‌کارگیری سلاح اجتماعی جوکر رابطه مستقیم وجود داشته و می‌تواند آن را پشتیبانی کند. بنابراین رسانه‌ها می‌توانند با راهکارهای ارائه شده به مقابله با رویکرد فرهنگی سلاح اجتماعی جوکر بپردازند. در گام دوم و جهت دستیابی به اهداف فرعی این پژوهش مجموعه‌ای از رویکردهای فرهنگی، حکمرانی و فناورانه در راستی‌آزمایی محتوای خبری جهت مقابله با سلاح اجتماعی جوکر معرفی گردید. خروجی تحقیقات پیشین در جهت شناخت اولیه اخبار جعلی و ارائه راهکارهای فنی و مهندسی برای راستی‌آزمایی محتوای رسانه‌ای بوده است. مقاله حاضر با بهره‌گیری از نتایج مطالعات پیشین و نیز یافته‌های جدید، روش‌هایی جدیدی برای شناخت محتوای خبری جعلی در راستای مقابله با سلاح اجتماعی جوکر پیشنهاد نموده است.

در پاسخ به سؤال فرعی نیز اولین یافته‌ای که از پژوهش حاضر به‌دست آمد مربوط به مقوله‌های رویکرد فرهنگ‌سازی می‌باشد. در هر عرصه و میدانی فرهنگ‌سازی از اولویت‌های اول می‌باشد. چنانچه با ورود هر تکنولوژی یا بستری به کشور بدون فرهنگ‌سازی تبدیل به معضل اجتماعی خواهد شد. ولنگاری در رسانه‌های اجتماعی نیر حاصل بی‌فرهنگی در این بستر می‌باشد. به‌همین دلیل در راستای پاسداری از شئونات فرهنگی جوامع، اقدامات فرهنگی رسانه از اولین اقدامات ضروری بستر رسانه‌ای می‌باشد. در این راستا انواع رسانه‌ها به‌خصوص رسانه‌های اجتماعی به‌عنوان یک رسانه فراگیر وظیفه فرهنگ‌سازی را برعهده دارند و فرهنگ‌سازی در جهت مقابله با فرهنگ جوکری نیاز ضروری رسانه می‌باشد.

دومین یافته این پژوهش توجه دادن به نقش حکمرانی در برنامه‌های فرهنگ‌سازی راستی‌آزمای محتوای خبری در راستای مقابله با رویکرد مخرب سلاح اجتماعی جوکر می‌باشد. برخی از رویکردهای رسانه‌ای خارج از توان افراد، اشخاص و شرکت‌های خصوصی بوده و در توان و وظایف حکمرانی می‌باشد. توجه و حمایت

از مراکز علمی، الزام به ایجاد واحدهای راستی‌آزما در رسانه‌ها بخصوص رسانه‌های مادر، نیز بررسی و الگو برداری از قوانین مشابه سایر کشورها از وظایف حکمرانی عمومی و حکمرانی رسانه‌ای می‌باشد.

سومین یافته این مقاله مربوط به معرفی فناوری اطلاعات مختص رسانه است که نیاز ضروری هر مخاطب در بستر رسانه می‌باشد. مخاطبان برای شناخت محتوای خبری جعلی یا همان فیک‌نیوزها نیازمند ابزاری هستند که بتوانند با توسل به آن اخبار جعلی، محتوای دستکاری شده و در کل پروپاگاندای سلاح اجتماعی جوکر را بشناسند. موتورهای جستجوی واقعیت‌سنج، سایت‌های واقعیت‌سنج، ابزارهای شناخت جعل عمیق و ... باید در رسانه‌ها و برنامه‌های تلویزیونی معرفی شده و راهکارهای شناخت محتوای خبری جعلی آموزش داده شود.

مخاطبان باید به این نتیجه برسند که هر محتوای خبری که ارائه می‌شود لزوماً درست نیست و باید در مورد آن تحقیق سپس پذیرش شود. یعنی در کل فرهنگ راستی‌آزمایی در مخاطب باید نهادینه شود. طبق نظریه شبکه‌ای، شبکه‌های اجتماعی، شبکه‌های تلویزیونی و سایر رسانه‌ها از مهم‌ترین ابزار اطلاع‌رسانی در عصر حاضر می‌باشند، که اگر این بسترها بدون برنامه‌ریزی رها شوند خطرات فرهنگی و اجتماعی جوامع بشری را تهدید خواهد کرد.

مطابق با نظریه حباب فیلتر با محدود شدن داده‌گیری در فضای مجازی مخاطبان با دیدگاه‌های مخالف روبرو نشده و همه دیدگاه‌ها را موافق خود خواهند دید و این اعلام خطری است که جوامع را تهدید می‌کند. مثلاً یک مخالف حاکمیت همیشه محتوای همسو با خود را در بستر آن‌لاین مشاهده خواهد کرد و به این نتیجه می رسد که همه با حاکمیت مخالف هستند و اگر این همسو، سلاح نرم جوکر باشد که نتایج آن مخرب‌تر خواهد بود (دقیقاً موضوعی که در اعتراضات آبان ۱۴۰۱ اتفاق افتاد و ناهنجاری‌های فرهنگی جوکری در قالب نافرمانی مدنی ظهور پیدا کرد و نهایتاً با اغتشاشات جوکری پایان یافت). این در صورتی است که این حباب فیلتر بستر آن‌لاین مانع در دسترس بودن افکار متفاوت در اختیار مخاطبان خواهد بود. بنابراین توجه به اهمیت و آموزش راهکارهای شناخت از مهم‌ترین رویکردها در بستر رسانه‌ای جوامع جهت مقابله با جنگ‌های نرم، جنگ‌های ادراکی و سلاح اجتماعی جوکر خواهد بود.

۸ جمع‌بندی و پیشنهاد

محتوای خبری جعلی همواره بر تصمیم‌گیری و افکار افراد تأثیر منفی دارد. این تأثیر می‌تواند تقویت‌کننده اهداف ضد فرهنگی سلاح اجتماعی جوکر باشد. این رویکرد در ناآرامی‌های سال ۱۴۰۱ ایران به‌وضوح قابل مشاهده بود. پرده‌دری و برگرفتن حجاب از سر یا نیمه‌برهنگی دختران و سایر هنجارشکنی‌های فرهنگی و اجتماعی از تأثیرات رسانه‌های بیگانه و سلاح اجتماعی جوکر بود. به‌همین دلیل، باید همیشه به منابع خبری و محتوایی که در فضای مجازی پخش می‌شود، اعتماد نکرده و با دقت و شفافیت بیشتری به آنها نگریست. با توجه به اینکه هدف نهایی سلاح اجتماعی جوکر زمین سوخته در موضوعات فرهنگی و اجتماعی می‌باشد، به‌همین دلیل باید اقدامات آفندی رسانه‌ای مناسبی جهت مقابله با این سلاح نرم خطرناک پیش‌بینی شود. مقاله حاضر به‌نوبه خود در بستر رسانه‌ای و راستی‌آزمایی محتوای خبری جعلی راهکارهای پیشگیرانه‌ای را

ارائه نموده است که با توجه به نوظهور بودن سلاح اجتماعی جوکر از پژوهش‌های پیشگام این بحث می‌باشد. عدم توجه به اهمیت ارتباط متغیرهای این مقاله آثار زیان بار همه‌جانبه‌ای برای جوامع به بار خواهد آورد. نمونه‌های بارز این امر ناآرامی‌های اخیر و ناهنجاری‌های فرهنگی و اجتماعی در بهار ۲۰۲۳ فرانسه و زمستان ۱۴۰۱ ایران می‌باشد که قابل تعمیم به سایر کشورها نیز است. حکمرانی رسانه‌ای و رسانه‌ها می‌توانند با استناد به خروجی مقاله حاضر به بررسی دقیق محتوای خبری پرداخته، از انتشار محتوای خبری جعلی و پشتیبانی از رویکرد ضد فرهنگی سلاح اجتماعی جوکر اجتناب کنند. حکمرانی رسانه‌ای می‌تواند با استفاده از نتایج این پژوهش مانع از بسترسازی فیک‌نیوزها جهت پشتیبانی از این سلاح نرم باشند. مخاطبان رسانه نیز می‌توانند با استفاده از این پژوهش و راستی‌آزمایی محتوای خبری با شناخت محتوای فیک مانع اهداف سلاح اجتماعی جوکر باشند. کلیت این مقاله، به ارائه راهکارهای رسانه‌ای جهت مقابله با رویکرد مخرب سلاح اجتماعی جوکر و تأکید بر اهمیت توجه ویژه به آن، پرداخته و در مورد مقابله با این سلاح نرم جدید هشدار می‌دهد. توجه به این امر به ویژه در زمان تهاجم فرهنگی اهمیت بیشتری پیدا می‌کند و قابل ذکر است که این راهکارها و اقدامات باید از خیلی وقت قبل از تهاجم فرهنگی بکار گرفته شود تا در آن زمان مخاطبان در دام فیک‌نیوزها و حباب فیلتر آن و نیز سلاح اجتماعی جوکر گرفتار نشوند. سلاح اجتماعی جوکر قدرت روانی مردم را هدف قرار می‌دهد. نهایتاً اینکه فیک‌نیوزها و سلاح اجتماعی جوکر هر دو ابزاری هستند که به کمک آنها می‌توان از ترس و نگرانی‌های افراد بهره برد و آنها را به سمت یک هدف خاص (اهداف ضد فرهنگی و اجتماعی) هدایت کرد. در عین حال فیک‌نیوزها به‌عنوان یک ابزار رسانه‌ای می‌توانند به‌عنوان عامل پشتیبانی کننده سلاح اجتماعی جوکر بکار گرفته شوند. پژوهشگران برای پژوهش‌های آینده می‌توانند سایر مقوله‌ها و مؤلفه‌های مرتبط همانند مقوله‌های آموزشی، روان‌شناختی، آفندی، اقتصادی، سیاسی، امنیتی و ... را بررسی نموده و راهکارهای متناسب را ارائه نمایند.

مراجع

[۱] ساعی، محمدحسین؛ آزادی، محمدحسین (زمستان ۱۴۰۰). «کلیات تشخیص خبر جعلی برای سازمان‌های رسانه‌ای با تأکید بر راستی‌آزمایی و مهارت اوسینت». فصلنامه انجمن ایرانی مطالعات فرهنگی و ارتباطات، ۶۵(۱۷)، ۱۸۷-۲۲۲.

[۲] ساعی، محمدحسین؛ آزادی، محمدحسین؛ البرزی دعوتی، هادی (۱۳۹۸). «مبانی طراحی نظام سواد رسانه‌ای برای مقابله با خبر جعلی». فصلنامه پژوهش‌های ارتباطی، ۱۰۰(۲۶)، ۲۳۵-۲۷۶.

[۳] خانیکی، هادی؛ خجیر، یوسف (۱۳۸۹). «گفت‌وگو در شبکه‌های اجتماعی مجازی (تحلیل سیستماتیک پژوهش‌های مرتبط)». فصلنامه انجمن ایرانی مطالعات فرهنگی و ارتباطات، ۲۶(۶۰)، ۶۳-۷۷.

[۴] کیهان، امیر؛ فرقانی، مهدی؛ مظفری، افسانه (۱۳۸۷). «نقش رسانه‌های اجتماعی موبایلی در شکل‌گیری هویت قومی دانشجویان». فصلنامه انجمن ایرانی مطالعات فرهنگی و ارتباطات، ۲۰(۶۳)، ۲۴۹-۲۸۴.

[۵] سلطانی‌فر، محمد؛ سلیمی، مریم؛ فلسفی، سید غلامرضا (۱۳۹۶). «اخبار جعلی و مهارت‌های مقابله با آن». فصلنامهٔ رسانه، ۲۸(۳)، ۴۳-۶۹.

[۶] غراب، حسنا (۱۳۹۸). «شناسایی و کشف الگوهای انتشار اخبار جعلی در ساختار شبکه‌های اجتماعی». پایان‌نامه کارشناسی ارشد، دانشگاه شهید بهشتی.

[۷] حسینی دانا، حمیدرضا (۱۳۹۹). «جنگ‌های رسانه‌ای و تغییر رفتار مخاطبان». تبریز: انتشارات مؤسسه علمی چیت‌سازان.

[۸] حسینی دانا، حمیدرضا (۱۳۹۸). «ملی‌سازی فضای مجازی». تبریز: انتشارات مؤسسه علمی چیت‌سازان.

[۹] ضیایی جباری، حسن (۱۳۹۷). «بررسی روش‌های پدافند رسانه‌ای در رسانه‌های اجتماعی»، نشست ملی الزامات و ویژگی‌های نظام جامع پدافند رسانه‌ای (۲/۱۲/۱۳۹۷).

[۱۰] پاتر، جیمز (۱۳۹۹). «سواد رسانه‌ای». تهران: انتشارات جهاد دانشگاهی.

[۱۱] کریمی، صدیقه؛ نصر، احمدرضا. (۱۳۹۲). «روش‌های تجزیه و تحلیل داده‌های مصاحبه». دوفصل‌نامه پژوهش، سال چهارم، شماره ۷۱، ۳۳-۹۴.

[۱۲] مک لوهان، مارشال (۱۳۷۷). «برای درک رسانه‌ها». ترجمه سعید آذری. تهران: مرکز پژوهش صداوسیما.

[۱۳] آزادی، محمدحسین (۱۳۹۸). «راهکارهای مقابله با خبر جعلی برای معاونت سیاسی سازمان صداوسیمای جمهوری اسلامی ایران». پایان‌نامه کارشناسی ارشد، دانشگاه صداوسیمای جمهوری اسلامی ایران.

[۱۴] آزادی، محمدحسین (۱۳۹۹). «رویکردها و چالش‌های مقابله با اخبار جعلی در جهان». فصلنامه دانش آینده‌پژوهی رسانه، ۱(۱)، ۳۳-۶۴.

[۱۵] تافلر، الوین (۱۳۸۵). «موج سوم». ترجمه شهیندخت خوارزمی. تهران: علم.

[۱۶] رستمی، زهرا (۱۳۹۸). «تشخیص اخبار کاذب در رسانه‌های اجتماعی». پایان‌نامه کارشناسی ارشد، دانشگاه حکیم سبزواری.

[۱۷] ساعی، محمدحسین؛ آزادی، محمدحسین؛ البرزی دعوتی، هادی (۱۳۹۸ ب). «ظهور خبر جعلی در عصر پساحقیقت؛ اهداف و پیامدها». فصلنامه رسانه‌های دیداری و شنیداری، ۱۳(۳۱)، ۵۹-۸۵.

[۱۸] سورین، ورنر جوزف؛ تانکارد، جیمز (۱۳۸۶). «نظریه‌های ارتباطات». ترجمه علیرضا دهقان. تهران: چاپ و انتشارات دانشگاه تهران.

[۱۹] افشانی، فریده (۱۳۹۳). «بررسی میزان اعتبار تبلیغات ماهواره‌ای و اعتماد مخاطب به آن». مطالعات ماهواره و رسانه‌های جدید، شماره ۵، ۸-۲۸.

[۲۰] فلسفی، سید غلامرضا (۱۳۹۸). «دیپ‌فیک، تیغی در کف زنگیان مست». رشد آموزش علوم اجتماعی، شماره ۵۵، ۶۰-۸۲.

[۲۱] سودایی، علی (۱۳۹۷). «رسوایی کمبریج آنالیتیکا و فیسبوک؛ بازی قدرت در سایه داده‌ها». بی‌بی‌سی فارسی. منتشر شده در ۴ فروردین ۱۳۹۷. به نشانی:
https://www.bbc.com/persian/world-feature.

[22] Huber, B., Borah, P., & Gil de Zúñiga, H. (2022). Taking corrective action when exposed to fake news: The role of fake news literacy. Journal of Media Literacy Education, 14(2), 1-14.

[23] Butler, J. (2019). “The Joker’s Philosophy: An Analysis of Nihilism and Chaos”. Journal of Popular Culture, 52(2), 480-494.

[24] Christopher, J. (2019). “The Joker’s: Can We Hold a Mirror Up to Nature?” Philosophy Now, (132), 22-25.

[25] Doe, J. (2018). “The Joker: A Study in Sociopathy” (Master’s thesis, University of California, Los Angeles).

[26] Barclay, D. A. (2018). “Fake News, Propaganda, and Plain Old Lies”. Rowman & Littlefield Publishers.

[27] Holmes, J. S. (2019). “The Joker’s Weapon of Choice: A Psychological Analysis”. Journal of Popular Culture, 52(2), 465-479.

[28] Pennycook, G., & Rand, D. G. (2019). “Who falls for fake news? The roles of bullshit receptivity, overclaiming, familiarity, and analytic thinking”. Journal of personality, 88(2), 185-200.

[29] Swire-Thompson, B., & Lazer, D. (2019). “Public health and online misinformation: challenges and recommendations”. Annual review of public health, 40, 429-451.

[30] Van der Meer, T. G. L. A., Jin, Y., & Seeking, A. (2019). “Rumours and corrections in the age of misinformation”. European Journal of Communication, 34(2), 175-190.

[31] Van der Meer, T. G., & Jin, Y. (2018). “Seeking and avoiding uncertainty: The impact of message frames on responses to fake news about vaccination”. Health communication, 33(1), 1-9.

[32] Zarocostas, J. (2018). “Fake news about disease outbreaks can cause unnecessary panic”. BMJ: British Medical Journal (Online), 363.

[33] Allcott, H. & Gentzkow, M. (2017). “Social media and fake news in the 2016 Election”. Journal of Economic Perspectives, 31 (2): 21-136.

[34] Flood, Alison. (2017). “Fake news is ’very real’ word of the year for 2017”. The Guardian. Published at 2 Nov 2017.

[35] Golafshani, N. (2003). “understanding reliability and validity in qualitative research”. The qualitative report,8 (4): 597 - 606.

[36] Kim, A., Moravec, P. L., & Dennis, A. R. (2019). “Combating fake news on social media with source ratings: the effects of user and expert reputation ratings”. Journal of Management Information Systems, 36 (3): 931 - 968.

[37] discriminatory Leese, M. (2014). “The new profiling: Algorithms, black boxes, and the failure of anti safeguards in the European Union”. Security Dialogue, 45(5): 494 - 511.

[38] McGonagle, T. (2017). “Fake news False fears or real concerns?” Netherlands Quarterly of Human Rights,35 (4): 203 - 209.

[39] Rubin, V. L. (2017). “Deception detection and rumor debunking for social media”. In The SAGE Handbook of Social Media Research Methods. Sage.

[40] Pennycook, G., Cannon, T. D., & Rand, D. G. (2018). “Prior exposure increases perceived accuracy of fake news”. Journal of experimental psychology: general, 147(12), 1865.

[41] Roozenbeek, J., & van der Linden, S. (2019). “The fake news game: actively inoculating against the risk of misinformation”. Journal of Risk Research, 22(5), 570-580.

[42] Kahan, D. M. (2017). “Fake news and alternative facts: The role of science literacy in determining the credibility of information”. The ANNALS of the American Academy of Political and Social Science, 672(1), 130-144.

[43] Lewandowsky, S., Ecker, U. K., & Cook, J. (2017). "Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era". Journal of Applied Research in Memory and Cognition, 6(4), 353-369.

[44] Wingardner, T., & Jones, T. (2019). "The Joker Psychology: Evil Clowns and the Women Who Love Them". Sterling.

ارزیابی دادگان تجمیع رتبه‌بندی نتایج جستجو از منظر گراف

فاطمه پاک مهر[۱]، امیرحسین کیهانی‌پور[۲]

[۱] کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
f.pakmehr@ut.ac.ir
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
keyhanipour@ut.ac.ir

چکیده

با افزایش اهمیت شبکه‌ها در زندگی امروزه، تحلیل دادگان بر اساس نظریه شبکه به منظور استخراج ویژگی‌های پنهان در مجموعه داده، به عنوان یک رویکرد تحقیقاتی جدید، مورد توجه جامعه محققان قرار گرفته است. از سوی دیگر، این روش تحلیل، امکان مقایسه بین مجوعه‌های داده مختلف را نیز فراهم می‌آورد. در این پژوهش، دو مجموعه داده تجمیع رتبه‌بندی نتایج جست‌وجو یعنی MQ2007-agg و MQ2008-agg، از منظر گراف مورد بررسی قرار گرفته است. برای این‌کار، ابتدا دادگان را به‌وسیله شاخص کندال به گراف شباهت ویژگی تبدیل کرده و ویژگی‌هایی از جمله اندازه اجزا، طول مسیر، اثر دنیای کوچک، توزیع درجه، قوانین توانی و ضرایب خوشه‌بندی را برای این شبکه‌ها محاسبه می‌شود و سپس بررسی تحلیلی ویژگی‌های به‌دست آمده در هر مجموعه داده، صورت گرفته است. نتایج بررسی‌ها نشان می‌دهد که گراف هیچ کدام از دادگان مورد ارزیابی، از نوع گراف‌های بدون مقیاس نبوده و تنها گراف متناظر با مجموعه MQ2007-agg از نوع دنیای کوچک است.

کلمات کلیدی: تحلیل داده، نظریه گراف، تحلیل شبکه، ویژگی‌های گراف، شاخص کندال.

۱ مقدمه

تجزیه و تحلیل گراف شامل استفاده از الگوریتم‌هایی برای تعیین روابط بین اشیاء در یک گراف و همچنین ویژگی‌های ساختاری کلی آن است. در حالی که کاربردهای سنتی تجزیه و تحلیل گراف مانند بهینه‌سازی کامپایلر، زمان‌بندی کار در سیستم عامل‌ها، برنامه‌های کاربردی پایگاه داده، پردازش زبان طبیعی، هندسه محاسباتی و غیره همچنان مهم هستند، سازمان‌ها برای به دست آوردن بینش‌هایی که می‌تواند در بازاریابی یا شبکه‌های اجتماعی استفاده شود، از مدل‌های گرافی استفاده می‌کنند [۱].

در این مقاله به صورت خاص، با بهره‌گیری از نظریه گراف، به تحلیل دو مجموعه داده از مجموعه LETOR4.0، مربوط به سال‌های ۲۰۰۷ و ۲۰۰۸، خواهیم پرداخت که مربوط به حوزه تجمیع رتبه‌بندی[۱]

[1] Rank Aggregation

می‌باشند. روند کلی روش پیشنهادی به صورت زیر خواهد بود:

- ارائه یک بازنمایی مبتنی بر گراف به ازای هر مجموعه داده
- استخراج ویژگی‌های مبتنی بر گراف برای هر مجموعه داده
- مقایسه تحلیلی این دو مجموعه بر اساس ویژگی‌های گرافی استخراج شده

همانطور که بیان شد، تحلیل دادگان با استفاده از نظریه گراف می‌تواند به منظور شناخت ویژگی‌های مجموعه داده مورد بررسی، مفید باشد. از سوی دیگر، استخراج این ویژگی‌ها می‌تواند امکان مقایسه تطبیقی دادگان متفاوت را نیز فراهم آورد. علاوه بر آن، با شناسایی ویژگی‌های مبتنی بر گراف، امکان ارزیابی دادگان دیگری که ممکن است بعدها عرضه شود، وجود خواهد داشت.

۲ مروری بر پژوهش‌های مرتبط

کاربرد نظریه گراف در حوزه بازیابی اطلاعات سابقه نسبتاً طولانی دارد. ادامه این بخش به معرفی برخی از این پژوهش‌ها می‌پردازد. در [۲] و [۳] روشی برای انتخاب ویژگی به منظور رتبه‌بندی نتایج جستجو با استفاده مدل‌سازی گرافی دادگان، عرضه شده است. در این الگوریتم، خوشه‌یابی طیفی[۲] روی بازنمایی گرافی مجموعه داده اعمال شده است تا زیرمجموعه‌ای از ویژگی‌های پایه دادگان، انتخاب شده و از آنها در رتبه‌بندی نتایج، استفاده شود.

در [۴] از نظریه گراف، جهت خوشه‌یابی گراف‌های دانش با مقیاس بسیار بزرگ و بهره‌گیری از آنها در سامانه‌های پرسش و پاسخ استفاده شده است. در این روش، از دادگان اولیه، گرافی تحت عنوان گراف شباهت ویژگی‌ها استخراج می‌شود و با استفاده از این گراف، مجموعه‌ای از ویژگی‌های مبتنی بر گراف، به ازای هر مجموعه داده، حاصل می‌شود که از آنها می‌توان در مقایسه دادگان مختلف، بهره گرفت. در [۵] از نظریه گراف در امر بازیابی تصاویر استفاده شده است. در این روش، گراف مشابهت بین مجموعه تصاویر دادگان یادگیری، تولید می‌شود و ویژگی‌های حاصل از این گراف در کنار ویژگی متنی متناظر با تصاویر، ادغام می‌شود تا بتواند مشابهت پرسش کاربر با تصاویر را محاسبه نموده و نهایتا تصاویر مرتبط را شناسایی و استخراج کند. در [۶] از نظریه گراف برای رتبه‌بندی تیم‌های ورزشی استفاده شده است. برای این منظور، بر اساس بازیهای انجام شده بین تیمهای مختلف و نتایج آنها، یک بازنمایی گرافی تهیه شده است و سپس از این گراف برای تعیین اولویت نسبی بین گره‌های مختلف که متناظر با تیمهای ورزشی می‌باشند، کمک گرفته شده است. از سوی دیگر، گراف دانش[۳] به‌عنوان روشی برای نمایش روابط پیچیده بین عناصر اطلاعاتی، سهم و جایگاه مهمی در بازیابی اطلاعات معنایی دارد و پژوهش‌های مختلفی از جمله [۷]-[۹]، به بررسی استفاده از گراف دانش در کاربردهای مختلف حوزه بازیابی اطلاعات پرداخته‌اند. در [۱۰] روشی برای ایجاد پیوند ضمنی بین

[2] Spectral clustering
[3] Knowledge Graph

عناصر اطلاعاتی در گراف دانش، پیشنهاد شده است که قادر است این عناصر اطلاعاتی را نسبت به توییت کاربر، اولویت‌بندی نماید. در کنار پژوهش‌های فوق در [۱۱] به شکل ویژه از نظریه گراف به منظور ایجاد چارچوبی برای مقایسه دادگان مختلف حوزه یادگیری رتبه‌بندی، کمک گرفته شده است. بر اساس ایده روش اخیر، در این مقاله پس از معرفی مفاهیم در موضوع تحلیل گراف [۱]، با کمک [۱۲] ویژگی‌های قابل بررسی در گراف‌ها را شناسایی کرده و به کمک قواعد و معیارهای آن به تحلیل و مقایسه گراف‌ها پرداخته‌ایم. همچنین با نگاهی به [۲] نحوه یادگیری رتبه‌بندی و بدست آوردن مقدار معیار شباهت ویژگی در گراف را پیاده‌سازی کرده و با راهنمایی‌های [۱۳] معیارهای خوشه‌بندی را محاسبه می‌کنیم. سپس مشابه رویکرد استفاده شده در [۱۱] به تحلیل و مقایسه چند مجموعه از دادگان حوزه تجمیع رتبه‌بندی می‌پردازیم.

۳ معرفی مجموعه دادگان

LETOR مجموعه‌ای از مجموعه داده‌های معیار برای تحقیق در مورد یادگیری رتبه‌بندی است که شامل ویژگی‌های استاندارد، قضاوت‌های مرتبط، تقسیم بندی داده‌ها، ابزارهای ارزیابی و چندین خط پایه است [۱۴]. LETOR 4.0 شامل ۸ مجموعه داده برای چهار دسته از رتبه‌بندی شامل Supervised ranking، Semi-supervised ranking، Rank aggregation و Listwise ranking است.

در جمع آوری داده‌ها از استراتژی اعتبار سنجی متقابل ۵-بخشی[۴] استفاده شده است و تقسیم‌بندی‌های ۵-تایی در هر بسته گنجانده شده که در هر پوشه، سه زیرمجموعه برای یادگیری وجود دارد: مجموعه آموزشی، مجموعه اعتبار سنجی و مجموعه تست.

در این پژوهش از بخش تجمیع رتبه‌بندی دادگان LETOR4.0، از دو مجموعه داده MQ2007-agg و MQ2008-agg استفاده نموده و آنها را با یکدیگر مقایسه خواهیم کرد. در ادامه این نوشتار، به منظور رعایت اختصار، این دو مجموعه را MQ2007 و MQ2008 می‌نامیم. در مجموعه داده‌های MQ2007 و MQ2008، به ترتیب حدود ۱۷۰۰ و ۱۸۰۰ پرس‌وجو با اسناد برچسب‌دار متناظر با آنها، وجود دارد.

در این قسمت، یک پرس‌وجو با مجموعه‌ای از لیست‌های ورودی رتبه‌بندی شده همراه است. شایان ذکر است که فرآیند تجمیع رتبه‌بندی با هدف بهبود نتایج رتبه‌بندی، اقدام به ادغام تعدادی لیست رتبه‌بندی پایه می‌کند.

هر سطر از مجموعه داده مورد استفاده، متناظر با یک زوج سند و پرس‌وجو می‌باشد. ستون اول برچسب مربوط به این زوج، ستون دوم query id، ستون‌های شماره‌گذاری شده از ۱ تا ۲۱ رتبه‌های سند در لیست‌های رتبه‌بندی ورودی و انتهای سطر نظر درباره زوج، از جمله شناسه سند است. در مثال بالا 2:30 به این معنی است که رتبه سند در لیست ورودی دوم ۳۰ است. توجه داشته باشید که رتبه‌های بزرگ به معنای موقعیت‌های برتر در فهرست رتبه‌بندی ورودی است و «NULL» به معنی این است که سند در لیست رتبه‌بندی شده ظاهر نشده است. ۲۱ لیست ورودی در مجموعه داده MQ2007 و ۲۵ لیست ورودی در مجموعه داده MQ2008 وجود دارد که برای مقایسه هر دو را ۲۱، در نظر خواهیم گرفته‌ایم.

[4] 5-fold cross validation

۴ معیارهای مورد توجه در گراف

در این بخش به صورت مختصر به توضیح معیارهای مورد توجه در بحث تحلیل داده از منظر گراف می‌پردازیم.

۱.۴ شاخص کندال تاو

شاخص کندال تاو[5] یک معیار غیر پارامتری پرکاربرد است که می‌تواند میزان همبستگی (یا شباهت) بین دو لیست رتبه‌بندی را ارزیابی کند [۲]. همبستگی به مفهوم ارتباط میان دو یا چند کمیت با یکدیگر است و ضریب همبستگی مقدار عددی این ارتباط را بیان می‌کند. هر چقدر قدر مطلق ضریب همبستگی به عدد یک نزدیک‌تر باشد ارتباط بین کمیت‌ها بیشتر و کامل‌تر است.

در این پژوهش، از شاخص کندال تاو استفاده شده است تا به ارتباط بین دو لیست رتبه‌بندی اسناد، به عنوان شباهت بین دو ویژگی با توجه به پرس‌وجو داده شده، اشاره کنیم؛ سپس با استفاده از آن، دادگان را به یک گراف وزن‌دار مدل می‌کنیم.

۲.۴ ویژگی‌های مبتنی بر گراف

ویژگی‌های زیادی –مانند تعداد گره‌ها، تعداد یال‌ها، میانگین درجه گره‌ها، میانگین وزن یال‌ها– در تحلیل یک گراف مورد توجه قرار می‌گیرند. در ادامه به توضیح برخی از مهم‌ترین آنها می‌پردازیم:

- تعداد مؤلفه‌های گراف و اعضای هر مؤلفه: با تقسیم شدن گراف به مؤلفه‌های گوناگون می‌توانیم شاهد میزان ارتباط هر ویژگی (گره) بر دیگری باشیم. برای مثال اگر دو ویژگی در دو مؤلفه جداگانه باشند تاثیر چندانی بر یکدیگر نخواهند داشت. به همین منوال اگر یک ویژگی عضو هیچ مؤلفه‌ای نباشد، میزان اهمیت آن ویژگی را به خوبی متوجه خواهیم شد.

- بزرگترین مؤلفه: به صورت معمول در اکثر شبکه‌های بدون جهت، یک جزء بزرگ وجود دارد که بخش قابل توجهی از شبکه را اشغال می‌کند، در حالی که بقیه شبکه به تعداد زیادی مؤلفه کوچک تقسیم می‌شود که معمولاً هر کدام از آنها حاوی اعضای انگشت شماری هستند. این مؤلفه بزرگ در اصطلاح «مؤلفه غول پیکر»[6] نامیده می‌شود.

- قطر شبکه: قطر شبکه در واقع بلندترین کوتاه‌ترین مسیر میان دو گره است. به عبارتی برای بدست آوردن آن بایستی کوتاه‌ترین مسیر بین هر دو گره در گراف را محاسبه کرده و بزرگ‌ترین آنها قطر شبکه است. قطر یک شبکه نشان دهنده گستردگی مؤلفه بزرگ یک شبکه است. در این پژوهش به دلیل اینکه طول یال کوتاه‌تر به معنای وابستگی کم دو گره به یکدیگر است، قطر یک گراف به معنای بی ارتباط‌ترین گره‌های مرتبط شناخته می‌شود. این نشان می‌دهد که کدامین گره‌ها با آنکه ارتباط چندانی به یکدیگر ندارند، اما بر هم اثر می‌گذارند.

[5] Kendall's τ
[6] Giant Component

- میانگین فاصله یا اثر دنیای کوچک[۷]: یکی از قابل توجه‌ترین و گسترده‌ترین بحث‌ها در مورد آثار شبکه، اثر جهان کوچک است. به این معنا که در بسیاری از شبکه‌ها فواصل بین زوج گره‌ها به طور شگفت‌آوری کوتاه است [۱۲]. اثر دنیای کوچک به ارتباطات درون یک شبکه اشاره دارد. در مورد شبکه‌های بررسی شده در این پژوهش، اثر دنیای کوچک نشان دهنده میزان همبستگی کلی ویژگی‌ها با یکدیگر است. به عبارت دیگر هرچقدر این فاصله بزرگ‌تر باشد نشان دهنده تاثیر مستقیم گره‌ها بر یکدیگر است. و هرچه این فاصله کوتاه‌تر باشد به معنی این است وابستگی ویژگی‌ها به صورت مستقیم بر یکدیگر اثر نداشته و همبستگی گره‌ها به صورت میانگین کم‌تر است.

۵ شبیه‌سازی

در اولین مرحله از شبیه سازی لازم است دادگان موجود را به یک گراف شباهت ویژگی تبدیل کرده و با استفاده از شاخص کندال که در قبل تشریح کردیم، گراف را وزن‌دهی کنیم.

باید توجه داشت که به دلیل حجیم بودن کل مجموعه داده، در این پژوهش از ۱۰٪ کل نمونه‌های موجود در هر مجموعه را برای انجام محاسبات، استفاده شده است. از سوی دیگر، در قسمت وزن‌دهی گراف با استفاده از شاخص کندال مسئله دیگری به نام شاخص sigma وجود خواهد داشت. این شاخص تعیین می‌کند که یال‌های قابل رسم باید در چه محدوده عددی وجود داشته باشند. به عبارتی اگر شاخص کندال میان دو ویژگی از معیار sigma کوچک‌تر باشد، هیچ رابطه‌ای در گراف میان آن دو ویژگی وجود نخواهد داشت.

در مرحله بعد به پیاده‌سازی و محاسبه هر یک از ویژگی‌های تعریف شده می‌پردازیم. در ادامه برخی توزیع‌ها را که به تحلیل گراف کمک خواهند کرد، پیاده سازی می‌کنیم. این توزیع‌ها در ادامه تشریح خواهند شد. شایان ذکر است که به منظور تسهیل دسترسی محققان به پیاده‌سازی روش مورد استفاده در این پژوهش، تمام کدهای پیاده‌سازی شده، قابل دسترس می‌باشد[۸].

۶ تحلیل و مقایسه

۱.۶ توزیع درجه

برای آنکه نشان دهیم درجه‌های گراف چه نسبتی با یکدیگر دارند از توزیع درجه استفاده می‌کنیم و آن را در قالب نمودار هیستوگرام نشان خواهیم داد. اهمیت بدست آوردن توزیع درجه در این است که می‌توانیم دید خوبی نسبت به تعداد ارتباط‌های شبکه و شلوغ بودن آن بدست آوریم. هرچقدر توزیع درجه در قسمت راست نمودار بالاتر باشد به معنی آن است که ویژگی‌ها با یک دیگر ارتباط بیشتری داشته و بر ویژگی‌های بیشتری اثر می‌گذارند. در واقع هرچقدر درجه یک گره بیشتر باشد یعنی آن گره مؤثرتر است.

[7] Small-world Effect

[8] https://drive.google.com/file/d/1rV5HUJg3ans9WBXSzkPD2MDiKStnxt0Q/view?usp=sharing

با توجه به نمودار توزیع درجه در شکل ۱ در می‌یابیم که با این وجود که توزیع درجات بالاتر در برخی قسمت‌های دنباله نزولی است اما گراف‌های رسم شده توزیع واضحی به سمت راست ندارند. لذا این دو مجموعه از قانون توزیع درجه پیروی نمی‌کنند.

۲.۶ توزیع توانی و شبکه‌های بدون مقیاس

اگر هیستوگرام مرحله قبل را با استفاده از مقیاس‌های لگاریتمی دوباره ترسیم کنیم، نمودار توزیع توانی[۹] را بدست خواهیم آورد.

شبکه‌هایی با توزیع درجه توانی، گاهی اوقات شبکه‌های بدون مقیاس[۱۰] نامیده می‌شوند و ویژگی‌های جالبی از خود نشان می‌دهند. برای بررسی اینکه یک شبکه بدون مقیاس است یا خیر ساده‌ترین استراتژی این است که به هیستوگرام توزیع درجه با اعمال لگاریتم بر محورهای آن توجه کنیم. اما این نمودار مشکلاتی دارد، از جمله اینکه آمار هیستوگرام در انتهای دنباله، که دقیقاً منطقه‌ای است که قانون توان در آن به طور معمول با دقت بیشتری بررسی می‌شود، ضعیف است.

ساده‌ترین راه، استفاده از هیستوگرام با عرض ستون‌های بیشتر است، به طوری که نمونه‌های بیشتری، در هر ستون قرار بگیرند. برای این کار از روش logarithmic binning استفاده می‌کنیم که در این طرح، هر سطل[۱۱] با یک عامل ثابت گسترده‌تر از مدل قبلی خود می‌شود [۱۲].

با توجه به نمودارهای مختلف مربوط به توزیع توانی در شکل ۱ در می‌یابیم که هیچ یک از گراف‌ها از قانون توان در توزیع توانی خود پیروی نمی‌کنند. لذا هیچ یک از این دو گراف جزء شبکه‌های بدون مقیاس، محسوب نمی‌شوند.

۳.۶ توزیع تجمعی

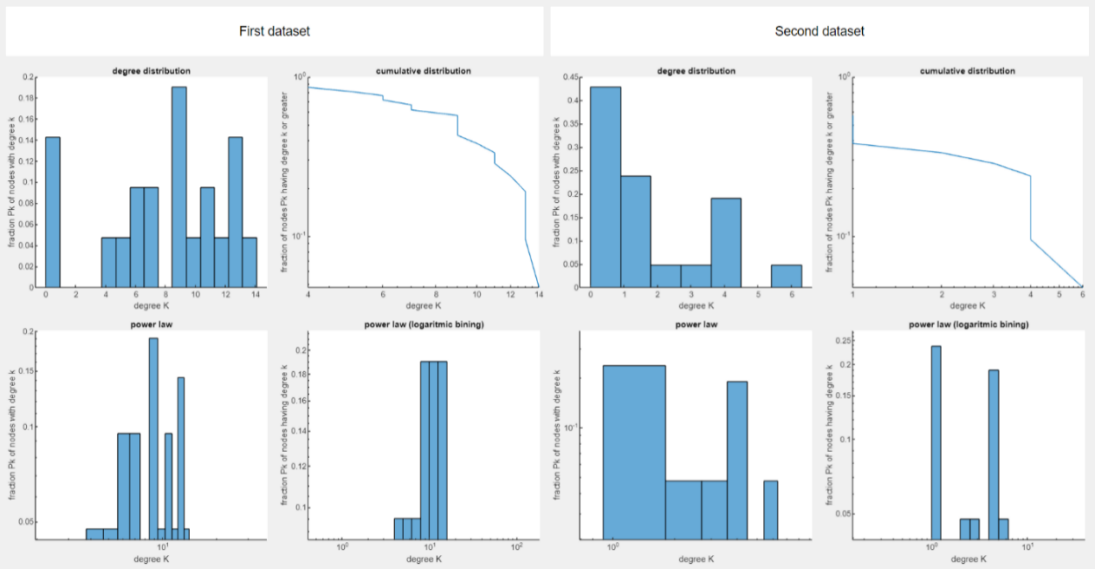
یک راه حل متفاوت برای مشکل تحلیل توزیع توانی، ساخت تابع توزیع تجمعی است [۱۲]. می‌توانیم تابع توزیع تجمعی را در مقیاس‌های لگاریتمی، همانطور که برای هیستوگرام اصلی انجام دادیم، رسم کرده و دوباره به دنبال رفتار خطی باشیم.

در تصویر ۱ می‌بینیم که هر دو گراف باز هم به‌خوبی از قانون توان پیروی نمی‌کنند. هر چند روند کاهشی در این نمودار بیشتر از دیگر توزیع‌ها قابل مشاهده است و این به دلیل حفظ تمام اطلاعات موجود در دادگان توسط این توزیع است.

۴.۶ توزیع معیارهای مرکزیت

به‌صورت کلی نحوه اتصال یک گره به گره‌های دیگر در یک شبکه می‌تواند اطلاعاتی راجع به میزان اهمیت آن گره در کاربردهای خاص مشخص نماید. به‌عنوان مثال می‌توانیم مشخص کنیم کدام گره بیشترین تأثیر

[9] Power Laws
[10] Scale-free Networks
[11] Bin



شکل ۱: توزیع درجه، توزیع توانی، توزیع توانی با الگوریتم logarithmic bining و توزیع تجمعی برای هر دو گراف از دیتاست‌های مورد پژوهش. در اینجا مقدار سیگما ۰٫۳ فرض شده است و منظور از first dataset مجموعه MQ2007 و second dataset مجموعه MQ2008 است.

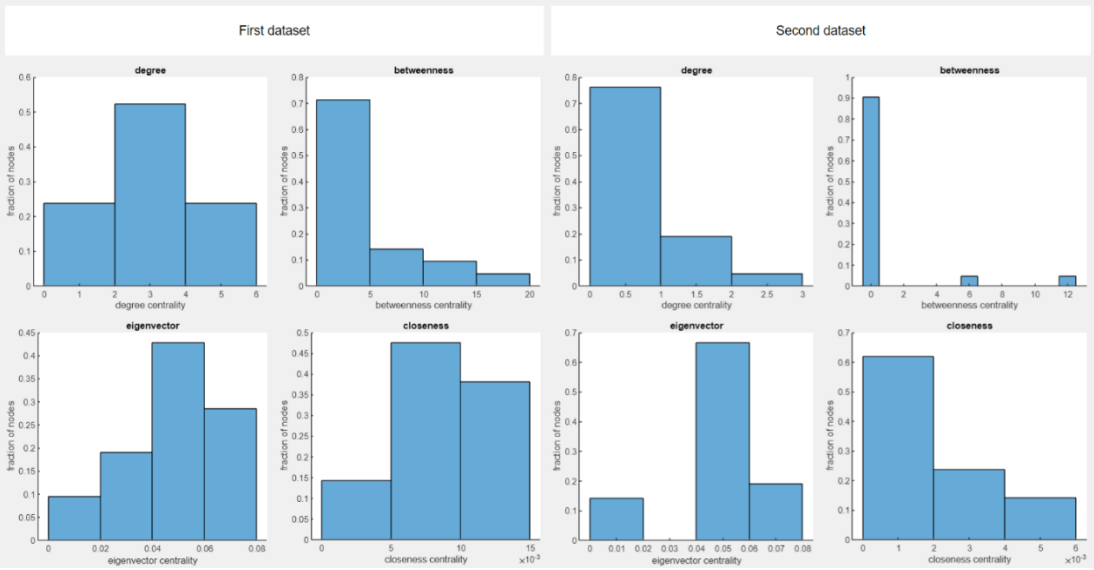
را در یک انتشار دارد.

برای سنجش میزان اهمیت، از شاخص‌های کمّی استفاده می‌شود که معیارهای مرکزیت[۱۲] نام دارند [۱۲]:

- فراوانی درجات گره‌ها که مبتنی بر همسایگی است: درجه یک گره تعداد گره‌هایی است که با آن گره در همسایگی مستقیم قرار دارد. هر چقدر درجه یک گره بیشتر باشد، اهمیت آن گره بیشتر می‌شود. با توجه به شکل ۲ می‌توانیم دریابیم که در گراف دوم تعداد گره‌ها با ارزشمندی پایین بیشتر از تعداد همین گره در گراف اول است.

- بینابینی که مبتنی بر مسیر است: بینابینی عبارت است از نسبت تعداد دفعاتی که یک گره یا یک یال بر روی کوتاه‌ترین مسیر میان نودهای مختلف یک گراف قرار می‌گیرد [۱۲]. به عبارتی بینابینی یک گره خاص در شبکه عبارت است از تعداد کوتاه‌ترین مسیرهای میان گره‌های شبکه که از یک گره خاص رد می‌شوند. این معیار محاسبه می‌کند چه تعداد از گرههای شبکه برای ارتباط سریع‌تر با هم، با واسطه کم‌تر، به این گره نیاز دارند. هر چه بینابینی گره زیادتر باشد یعنی اینکه گره در مکان استراتژیک‌تری قرار گرفته است. همچنین نشان‌دهنده درصدی از اطلاعات است که از یک گره می‌گذرد. در واقع نمایشی برای میزان قابلیت هر گره برای کمک به دسترسی سایرین به اطلاعات و یا گسترش یک تاثیر در شبکه می‌باشد. جالب است که با توجه به شکل ۲ میزان این معیار در دو

[12] Centrality



شکل ۲: معیارهای مرکزیت در قالب هیستوگرام. در اینجا مقدار سیگما ۰٫۳ فرض شده است و منظور از first dataset مجموعه MQ2007 و second dataset مجموعه MQ2008 است.

گراف مورد پژوهش بسیار به یکدیگر شبیه است. به عبارتی گره‌ها در هر دو گراف بر تعداد کمی از دیگر گره‌ها اثر می‌گذارند.

- نزدیکی که مبتنی بر مسیر است: نزدیکی عبارت است از عکس متوسط فاصله یک گره تا گره‌های دیگر گراف .[۱۲] گره‌ای که دارای بیشترین مقدار نزدیکی است سرعت دسترسی بیشتری به گره‌های دیگر دارد و می‌تواند در مدت زمان کمی به همه گرهها اطلاعات ارسال نماید یا از آن‌ها اطلاعات بگیرد. این مسئله جهت پیدا کردن سریع‌ترین محل انتشار، بسیار مناسب است. همچنین با توجه به تصویر ۶. ۲ در می‌یابیم که در گراف دوم ارزشمندی گره‌ها به صورت کلی کم است و گره‌ها تاثیر چندانی بر یکدیگر ندارند، اما در گراف دوم تعداد گره‌هایی که موثر هستند بسیار بیشتر است.

- مقادیر ویژه که مبتنی بر ارزش است: این روش اهمیت گره‌ها را بر اساس گره‌های مجاور محاسبه می‌کند .[۱۲] این محاسبه در گراف‌های با اتصال قوی اتفاق می‌افتد. اگر گره‌ای به گره‌هایی که دارای اهمیت بالایی هستند متصل باشد تحت تأثیر آن‌ها اهمیت او نیز بالا می‌رود.

در این معیار نیز با توجه به شکل ۲ میزان ارزشمندی گره‌ها در دو گراف مورد پژوهش بسیار به یکدیگر شبیه است. به عبارتی گره‌ها در هر دو گراف به گره‌ها با ارزش‌های نسبتا یکسانی متصل شده‌اند.

جدول ۱: برخی از ویژگی‌های اندازه‌گیری شده عبارتند از: مقدار سیگما (sigma)، تعداد گره‌ها (n)، تعداد یال‌ها (m)، میانگین درجه (avg_d)، میانگین وزن یال‌ها (avg_w)، اندازه بزرگ‌ترین مؤلفه (ns)، کسری از گره‌ها که در بزرگ‌ترین مؤلفه قرار دارند (S)، میانگین فاصله (L)، ضریب خوشه‌بندی (C)

نام‌گراف	نوع	sigma	n	m	avg_d	avg_w	ns	S	L	C
MQ2007-seg	بدون جهت	۰٫۳	۲۱	۸۴	۸	۰٫۳۴	۱۸	۰٫۸۵	۰٫۲۴	۰٫۶۷
MQ2008-seg	بدون جهت	۰٫۳	۲۱	۱۶	۱٫۵۲	۰٫۳۵	۸	۰٫۳۸	۰٫۲۸	۰٫۲۷

۵.۶ ضرایب خوشه‌بندی

هدف از خوشه‌بندی، استخراج بخش‌هایی از داده‌ها است که شباهت زیادی با هم دارند. به زبان دیگر در خوشه‌بندی، داده‌ها را به نحوی در گروه‌هایی تقسیم می‌کنیم که داده‌های مربوط به هر گروه ویژگی‌های نزدیک به هم داشته باشند و داده‌های موجود در دو گروه مختلف، ویژگی‌هایی با اختلاف زیاد داشته باشند.

- میانگین ضریب خوشه‌بندی: این معیار، خوشه‌بندی در یک شبکه را با میانگین‌گیری ضرایب خوشه‌بندی تمام گره‌های آن اندازه‌گیری می‌کند. به عبارت ساده‌تر ضریب خوشه‌بندی احتمال متوسط این است که دو همسایه از یک گره خودشان با هم همسایه باشند و شبکه ای با میانگین ضریب خوشه‌بندی بالا و فاصله متوسط کوچک اغلب شبکه «دنیای کوچک» نامیده می‌شود .[۱۳] با محاسبات انجام شده میانگین ضریب خوشه‌بندی برای گراف اول تقریبا دو برابر گراف دوم است. اما با توجه به معیارهای بدست آمده، میانگین فاصله در گراف اول از گراف دوم کوچک‌تر است. بنابراین می‌توان گفت گراف اول یک شبکه از جنس «دنیای کوچک» است.

- ضریب خوشه‌بندی محلی: با کمک این معیار می‌توان تعیین کرد که گره‌ها تا چه میزان تمایل به شرکت در یک اجتماع را دارند. به عبارت دیگر معیار ضریب خوشه‌بندی محلی نشان می‌دهد که که محیط اطراف یک گره تا چه میزان همبند بوده و به یک اجتماع شبیه است. هر چه محیط اطراف یک گره همبندتر باشد، آن گره قابل اطمینان‌تر است. زمانی که یک گره با اجتماعات متعدد در ارتباط است، دارای همسایگی با درجه همبندی پایین می‌باشد و دارای درجه اطمینان کم‌تری است. در گراف‌های مورد بررسی ما ضریب خوشه‌بندی محلی برای بالاترین درجه، کوچک و برای پایین‌ترین درجه، بزرگ است.

۷ نتیجه‌گیری

در این پژوهش دو مجموعه داده عمده در حوزه تجمیع رتبه‌بندی، یعنی MQ2007-agg و MQ2008-agg با استفاده از نظریه گراف، را مورد مطالعه و بررسی تطبیقی، قرار گرفته است. برای تحلیل این دادگان ابتدا آن‌ها را به یک گراف ویژگی تبدیل کرده و سپس با استفاده از معیارها و الگوریتم‌های تحلیل گراف سعی در مقایسه و تحلیل این دو مجموعه داده داشتیم. نتایج کلی بررسی گراف‌ها در جدول ۱ نمایش داده شده است.

همچنین هیچ کدام از شبکه‌ها، از نوع شبکه‌های بدون مقیاس نیستند و تنها شبکه متناظر با دادگان MQ2007 از نوع شبکه دنیای کوچک است. هر چند باید توجه داشت این نتیجه‌گیری‌ها کاملاً وابسته به مقدار متغیر سیگما هستند.

مراجع

[1] U. Cheramangalath, R. Nasre, and Y. N. Srikant, Distributed Graph Analytics. Springer International Publishing, 2020. doi: 10.1007/978-3-030-41886-1.

[2] J. Y. Yeh and C. J. Tsai, “A Graph-based Feature Selection Method for Learning to Rank Using Spectral Clustering for Redundancy Minimization and Biased PageRank for Relevance Analysis,” Comput. Sci. Inf. Syst., vol. 19, no. 1, pp. 141–164, Jan. 2022, doi: 10.2298/CSIS201220042Y.

[3] J. Y. Yeh and C. J. Tsai, “Graph-based Feature Selection Method for Learning to Rank,” ACM Int. Conf. Proceeding Ser., pp. 70–73, Nov. 2020, doi: 10.1145/3442555.3442567.

[4] H. Gao, L. Wu, P. Hu, Z. Wei, F. Xu, and B. Long, “Graph-augmented Learning to Rank for Querying Large-scale Knowledge Graph,” arXiv, p. arXiv:2111.10541, Nov. 2021, doi: 10.48550/ARXIV.2111.10541.

[5] B. Geng, L. Yang, and X.-S. Hua, “Learning to Rank with Graph Consistency,” Aug. 2009. Accessed: Jan. 23, 2023. [Online]. Available: https://www.microsoft.com/en-us/research/publication/learning-to-rank-with-graph-consistency/

[6] J. Shi and X. Y. Tian, “Learning to Rank Sports Teams on a Graph,” Appl. Sci. 2020, Vol. 10, Page 5833, vol. 10, no. 17, p. 5833, Aug. 2020, doi: 10.3390/APP10175833.

[7] H. Gao et al., “Graph-augmented Learning to Rank for Querying Large-scale Knowledge Graph,” arXiv, p. arXiv:2111.10541, Nov. 2021, Accessed: Jan. 22, 2023. [Online]. Available: https://ui.adsabs.harvard.edu/abs/2021arXiv211110541G/abstract

[8] H. Wu and F. J. Meng, “Research on the Application of Personalized Course Recommendation of Learn to Rank Based on Knowledge Graph,” Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST, vol. 331, pp. 19–30, 2020, doi: 10.1007/978-3-030-62205-3_2/COVER.

[9] Y. Su et al., “Reducing Bug Triaging Confusion by Learning from Mistakes with a Bug Tossing Knowledge Graph,” Proc. - 2021 36th IEEE/ACM Int. Conf. Autom. Softw. Eng. ASE 2021, pp. 191–202, 2021, doi: 10.1109/ASE51524.2021.9678574.

[10] H. Hosseini and E. Bagheri, “Learning to rank implicit entities on Twitter,” Inf. Process. Manag., vol. 58, no. 3, p. 102503, May 2021, doi: 10.1016/J.IPM.2021.102503.

[11] A. H. Keyhanipour, “Graph-based comparative analysis of learning to rank datasets,” Int. J. Data Sci. Anal., pp. 1–23, Jun. 2023, doi: 10.1007/S41060-023-00406-8/METRICS.

[12] M. Newman, Networks: A Introduction, Second edi. Oxford University Press, 2018.

[13] Y. Li, Y. Shang, and Y. Yang, “Clustering coefficients of large networks,” Inf. Sci. (Ny)., vol. 382–383, pp. 350–358, Mar. 2017, doi: 10.1016/J.INS.2016.12.027.

[14] T. Qin and T.-Y. Liu, “Introducing LETOR 4.0 Datasets,” Jun. 2013, doi: 10.48550/arxiv.1306.2597.

بررسی و تحلیل دادگان تشخیص صفحات اسپم درمحیط وب بر اساس نظریه گراف

مهدیه رعیتی[۱]، امیرحسین کیهانی‌پور[۲]

[۱] کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
mahdieh.raeyati@ut.ac.ir
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران
keyhanipour@ut.ac.ir

چکیده

نظریه گراف که به مدل‌سازی روابط موجود بین عناصر مختلف مسئله مورد بررسی می‌پردازد، ابزار مفیدی را برای ساده‌سازی بخش‌های یک سیستم فراهم می‌کند. پیچیده‌تر شدن مسائل دنیای پیرامونی، به‌کارگیری نظریه گراف را به یک ضرورت تبدیل نموده است. این مقاله قصد دارد مجموعه دادگان عرضه شده به‌منظور شناسایی تشخیص صفحات اسپم در محیط وب را از منظر گراف مورد بررسی قرار دهد. برای این منظور، ابتدا گراف شباهت ویژگی‌های مجموعه داده، ایجاد می‌شود و سپس، گراف حاصل به‌لحاظ شاخص‌های ساختاری مختلف، مورد بررسی قرار خواهد گرفت. برای ارزیابی روش پیشنهادی، گراف شباهت به‌ازای دو دسته از ویژگی‌های متنی و پیوندی به‌ازای مجموعه داده WEBSPAM-UK2007 ایجاد گردید و بر اساس شاخص‌های فوق مورد مقایسه تحلیلی قرار گرفت. نتایج به‌دست آمده نشان می‌دهد که علیرغم بزرگ‌تر بودن و تراکم نسبی بالاتر گراف شباهت ویژگی‌های مبتنی بر متن، نسبت به گراف شباهت ویژگی‌های مبتنی بر پیوند، بر اساس شاخص‌های ضریب خوشه‌بندی، گراف شباهت ویژگی‌های مبتنی بر پیوند، انسجام نسبی بیشتری را دارا می‌باشد. این موضوع با توجه به اندازه نسبی بزرگ‌ترین مؤلفه همبند نیز تأیید می‌شود. این رویکرد، امکان مقایسه تحلیلی دادگان مختلف را فراهم می‌آورد. علاوه بر آن، می توان از نتایج این پژوهش به‌منظور طراحی دادگان جدید نیز استفاده نمود.

کلمات کلیدی: نظریه گراف، دادگان تشخیص صفحات اسپم، ویژگی‌های گراف، شاخص کندال.

۱ مقدمه

بازیابی اطلاعات وب با چالش‌های متعددی مواجه است. یکی از این چالش‌ها که بعضاً عدم توجه به آن، منجر به کاهش کیفیت نتایج جستجو و در نتیجه عدم رضایت کاربر می‌شود، عدم توجه به موضوع تشخیص و حذف

صفحات اسپم[1] از فرآیند بازیابی اطلاعات می‌باشد. بطور خلاصه، صفحات اسپم، شامل محتوای غیر مفید یا هرزی هستند که یا اصولا امکان تامین نیاز اطلاعاتی کاربر از طریق آنها فراهم نیست و یا اینکه تامین نیاز کاربر را با دشواری‌های مختلف، مواجه می‌کنند. این قبیل سایت‌ها و صفحات، غالبا با هدف دستکاری رتبه‌بندی نتایج جستجو و جلب توجه کار به صفحات هدف، طراحی می‌شوند و ممکن است محتوای قابل مشاهده توسط کاربر با محتوای واقعی این صفحات، متفاوت باشد. به منظور شناسایی صفحات اسپم، مجموعه‌های داده مختلفی طراحی شده است که از نظر ویژگی‌ها و مشخصات، بسیار متفاوت می‌باشند. در این پژوهش در نظر است با مدل‌سازی این دادگان با استفاده از نظریه گراف، چارچوبی برای مقایسه تحلیلی این دادگان فراهم آید. نظریه گراف بواسطه امکان مدل‌سازی روابط پیچیده بین عناصر مساله مورد بررسی، مورد اقبال وسیع محققان قرار گرفته است. بصورت خلاصه، یک گراف (شبکه) در ساده‌ترین شکل خود مجموعه‌ای از گره‌ها است که از طریق یالهای ارتباط دهنده، به یکدیگر متصل شده‌اند. این یال‌های عملا بیانگر روابط بین گره‌ها. در این مقاله به بررسی مجموعه دادگان مربوط به تشخیص صفحات اسپم با استفاده از این روش مدل‌سازی، می‌پردازیم. گره‌های این گراف، معادل ویژگی‌های عرضه شده در مجموعه دادگان مورد بررسی هستند و یالهای آن، میزان شباهت ویژگی‌ها را نشان می می‌دهند. در واقع با تبدیل مجموعه داده به گراف ویژگی، ویژگی‌های مهم و تعیین کننده و همچنین ارتباط بین ویژگی‌ها، به طور دقیق و مؤثر، قابل مشاهده خواهند بود. مراحل کلی روش پیشنهادی به شرح زیر خواهد بود:

- تعیین گره‌ها و یال‌های گراف
- تعیین معیار وزن‌دهی یال‌ها (شاخص کندال)
- ایجاد گراف ویژگی با استفاده از ثابت sigma
- تحلیل گراف و بررسی ویژگی‌های آن (اعم از توزیع درجه، معیارهای مرکزیت، قطر شبکه و ضرایب خوشه‌بندی محلی و سراسری)

در ادامه این نوشتار، ابتدا به مرور کاربردهای نظریه گراف در حوزه بازیابی اطلاعات وب، خواهیم پرداخت و سپس، چارچوب نظری روش پیشنهادی، بیان خواهد شد. پس از آن، نتایج بدست آمده از اجرای روش پیشنهادی روی یک مجموعه دادگان شناسایی صفحات اسپم و نیز تحلیل این نتایج ارائه می‌شود. در پایان نیز جمع‌بندی این پژوهش و ارائه رویکردهای توسعه آن، مطرح می‌گردد.

۲ مروری بر کارهای دیگران

نظریه گراف بدلیل غنای نظری و نیز قابلیت مدلسازی روابط پیچیده بین عناصر مساله، بصورت گسترده در حوزه بازیابی اطلاعات مورد استفاده قرار گرفته است. از جمله کاربردهای جالب توجه این نظریه در بازیابی اطلاعات وب، می‌توان به موضوع تعبیه گراف[2] به منظور طراحی الگوریتم‌های رتبه‌بندی کارآمد اشاره

[1] Spam
[2] Graph Embedding

نمود [۱]-[۴]. رویکرد دیگری که بر اساس کاربرد نظریه گراف، توسعه یافته است، مربوط به بکارگیری شبکه پیچشی گراف[۳] در طراحی روش‌های کارآمد در زمینه اطلاعات و به خصوص در مورد رتبه‌بندی بازیابی نتایج جستجوهای کاربران می‌باشد [۵]-[۹]. در زمینه بازیابی معنایی اطلاعات[۴] نیز از توانمندی‌های نظریه گراف برای بررسی روابط پیچیده بین عناصر داده، در قالب تولید گراف دانش[۵] استفاده شده است. بر این اساس، امکان ارتقای کیفیت بازیابی اطلاعات به ویژه در زمینه رتبه‌بندی نتایج جستجو، نسبت به روش‌های کلاسیک، فراهم خواهد آمد. از جمله این پژوهش‌ها می‌توان به [۱۰]-[۱۳] اشاره نمود. در [۱۴]، [۱۵] ایده تولید گراف شباهت ویژگی‌های دادگان به منظور بدست آوردن ویژگی‌های گرافی مطرح شده است و از این ویژگی‌ها به منظور ارائه یک روش یادگیری رتبه‌بندی[۶] استفاده شده است. از سوی دیگر در [۱۶] از نظریه گراف به منظور مقایسه تحلیلی دادگان موجود در حوزه یادگیری رتبه‌بندی استفاده شده است. در این روش نیز گراف شباهت ویژگی‌های موجود در مجموعه داده، به عنوان بازنمایی ثانویه از مجموعه دادگان مورد بررسی، تولید شده و به ازای کل گراف مجموعه‌ای از ویژگی‌های ساختاری استخراج گردیده است. بدین ترتیب، چارچوبی برای مقایسه مشخصات این دادگان فراهم آمده است.

در پژوهش فعلی با الهام از سه مقاله اخیر، از همین رویکرد برای تهیه چارچوبی برای مقایسه دادگان تشخیص صفحات اسپم در محیط استفاده شده است که بر اساس نظریه گراف، طراحی شده است. مشابه پژوهش‌های قبلی، با استفاده از روش پیشنهادی، امکان مقایسه تحلیلی انواع دادگان حوزه شناسایی صفحات اسپم، فراهم می‌شود.

۳ معرفی مجموعه داده

مجموعه داده WEBSPAM-UK2007[۷] بر اساس خزش[۸] صورت گرفته از دامنه uk. بدست آمده است و شامل فهرستی از سایت‌ها است که بصورت اسپم یا غیر اسپم، برچسب‌گذاری شده‌اند. مجموعه ویژگی uk-2007-05.link_based_features، شامل ویژگی‌های مبتنی بر لینک برای میزبان‌ها است که هم در صفحه اصلی و هم در صفحه با حداکثر رتبه صفحه[۹] در هر میزبان اندازه‌گیری می‌شود. ویژگی‌هایی نظیر درجه، درجه خروجی، رتبه صفحه، ضریب طبقه‌بندی، رتبه اعتماد ، رتبه صفحه کوتاه شده و ... .

[3] Graph Convolution Network
[4] Semantic Information Retrieval
[5] Knowledge Graph
[6] Learning to Rank
[7] https://chato.cl/webspam/datasets
[8] Crawl
[9] maximum page rank

۴ ایجاد گراف ویژگی

۱.۴ تعیین گره‌ها و یال‌ها

گراف ویژگی بر اساس ویژگی‌های موجود در مجموعه داده (ستون های مجموعه داده) ایجاد می‌شود؛ بنابراین گره‌ها، نام ستون‌های مجموعه داده هستند. پس از حذف دو ستون اول شامل شناسه و نام میزبان، - که ویژگی‌های غیر عددی و غیر مرتبط با سایر ویژگی‌ها هستند - بین هر دو جفت گره، یک یال ایجاد می‌کنیم. هر یال نشان دهنده ارتباط ویژگی‌های نقاط انتهایی خودش است. بنابراین در پایان این مرحله، یک گراف کامل خواهیم داشت.

۲.۴ تعیین معیار وزن‌دهی یال‌ها (شاخص کندال)

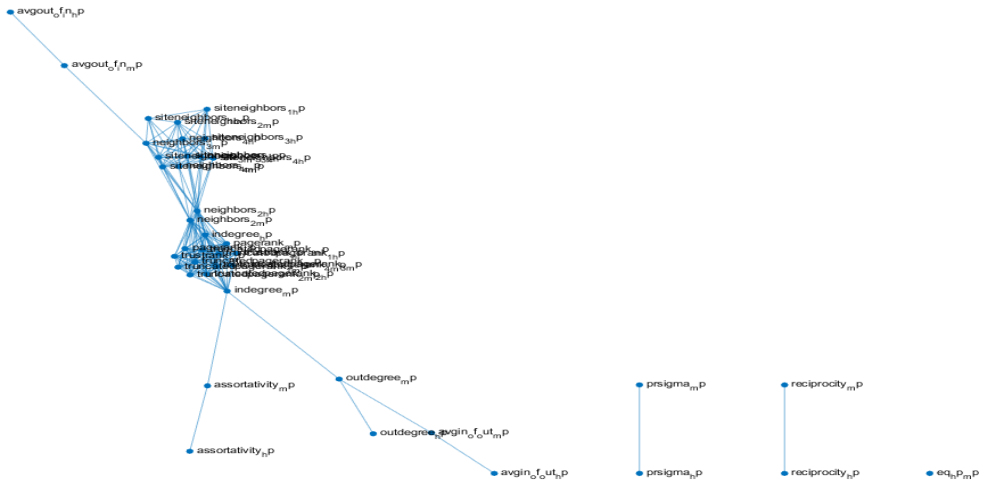
شاخص کندال، یک شاخص مناسب برای سنجش میزان ارتباط و همبستگی دو متغیر می‌باشد. لذا می‌توانیم برای ایجاد گراف ویژگی، از این آماره استفاده کنیم. شاخص کندال، عددی در بازه $[-۱, ۱]$ است. هرچه این عدد به یک یا منفی یک نزدیکتر باشد، میزان هماهنگی یا ناهماهنگی دو متغیر، بیشتر است؛ یعنی دو متغیر، تاثیر زیادی روی هم می‌گذارند و موجب تشدید یا تضعیف یکدیگر می‌شوند. بنابراین برای مشخص کردن میزان اهمیت و سنگین بودن یک یال، کافیست شاخص کندال را برای دو ستون متناظر دو گره در مجموعه داده ، محاسبه کنیم و قدر مطلق این مقدار را به عنوان وزن آن در نظر بگیریم . لذا هرچه وزن یالی به یک نزدیکتر باشد به معنی ارتباط قوی گره‌های انتهایی آن و هرچه به صفر نزدیکتر باشد به معنای ارتباط ضعیف‌تر است.

۳.۴ حذف یال‌های اضافی با استفاده از ثابت سیگما

گراف ایجاد شده در مرحله قبل، حاوی یال‌های اضافی است. ثابت سیگما، محدوده لازم برای حذف یا عدم حذف یال های گراف را مشخص می‌کند. اگر مقدار سیگما برابر با n باشد، تمام یال‌هایی که وزنشان از n کم‌تر باشد حذف خواهند شد. به همین ترتیب، هرچقدر ثابت سیگما بزرگ‌تر باشد، فیلتر سنگین‌تری روی گراف اعمال خواهد شد و فقط اتصال گره‌هایی که ارتباط بسیار قوی‌تری دارند حفظ خواهد شد. در این مقاله، مقدار سیگما، ۰٫۵ در نظر گرفته شده است. زیرا مقادیر کم‌تر از ۰٫۵، همبستگی اندکی دارند که بررسی آن ها، ضرورتی ندارد.

۵ تحلیل گراف

این گراف، شامل ۴۱ گره و ۲۰۲ یال است. میانگین درجه آن ۹٫۸ و میانگین وزن یال‌ها ۰٫۶۷ می‌باشد. همان‌طور که در شکل ۱ قابل مشاهده است، گراف از ۴ مؤلفه عمده تشکیل شده است به‌طوری‌که بزرگترین مؤلفه، ۰٫۸۷ = ۳۶/۴۱ گره‌ها را در بر دارد.



شکل ۱: گراف ویژگی استخراج شده از مجموعه ویژگی

۱.۵ توزیع درجه

در نمودار ۱، هیستوگرام توزیع درجه گراف نشان داده شده است. همانطور که در نمودار ۱ پیداست، توزیع درجه، از الگوی قانون توان پیروی نمی‌کند؛ زیرا اکثریت گره‌ها، درجه پایین ندارند و تعداد گره‌های درجه بالا، نسبتا زیاد است و به طور کلی، رفتار نمودار، نزولی (یا صعودی) نیست.

۲.۵ ضرایب خوشه‌بندی

فرمول محاسبه ضریب خوشه‌بندی برای کل شبکه به صورت زیر است [۱۷]:

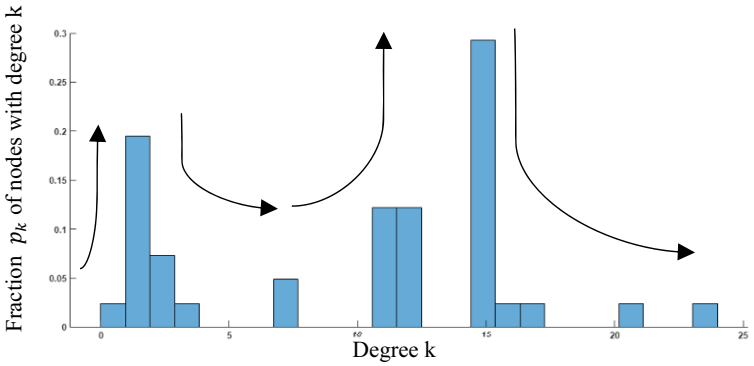
$$c = \frac{\text{۳ × تعداد مثلث‌ها در شبکه}}{\text{تعداد رئوس سه‌گانه متصل}} \quad (۱)$$

که در آن «سه‌گانه متصل» به‌معنای یک رأس منفرد با دو یال متصل به خودش است به‌گونه‌ای که اگر یال سومی به آنها اضافه شود، مثلث تشکیل خواهد شد [۱۸].

روش دوم: یک تعریف جایگزین از ضریب خوشه‌بندی، که به طور گسترده نیز استفاده می‌شود ، تعریف ضریب خوشه‌بندی محلی به صورت زیر است [۱۸]:

$$c_i = \frac{\text{تعداد مثلث‌های متصل به رأس } i}{\text{تعداد سه‌گانه با مرکز رأس } i} \quad (۲)$$

برای رئوس با درجه ۰ یا ۱ که صورت و مخرج هر دو صفر هستند، $c_i = ۰$ خواهد بود. سپس ضریب



نمودار ۱. هیستوگرام توزیع درجه گراف

خوشه‌بندی برای کل شبکه، میانگین مقادیر c_i خواهد بود [۱۸]:

$$C = \frac{۱}{n} \sum_i c_i \qquad (۳)$$

در این گراف، ضریب خوشه‌بندی سراسری با استفاده از معادله ۱ مقدار ۰٫۲۹۰۲ و با استفاده از معادله ۳ مقدار ۰٫۵۹۰۷۴ است.

همان‌طور که مشخص است، میانگین ضریب خوشه‌بندی محلی برای درجات ۱۵ تا ۲۴ اکیداً نزولی است. به‌طور کلی در اکثر شبکه‌های دنیای واقعی انتظار بر این است که گره‌های متعلق به مؤلفه‌های کوچک، درجات پایینی داشته باشند؛ زیرا گره‌های آن‌ها، محدوده انتخاب کوچک‌تری برای اتصال به گره‌های دیگر دارند؛ در حالی که مؤلفه‌های بزرگتر می‌توانند درجه بالاتری داشته باشند. با این وجود، معمولاً ضریب خوشه‌بندی محلی گره‌ها در مؤلفه‌های کوچک، بزرگتر است، زیرا هر مؤلفه ، به‌صورت جدا از بقیه شبکه و به‌عنوان یک شبکه کوچک‌تر عمل می‌کند [۱۹].

۳.۵ معیارهای مرکزیت

۱.۳.۵ مرکزیت درجه

گره‌های neighbors_2_hp و neighbors_2_mp در این گراف، بیشترین درجه‌ها را دارند (به ترتیب ۲۴ و ۲۱). بنابراین بیشترین مرکزیت درجه را خواهند داشت. بدیهی است که هیستوگرام مربوط به این مرکزیت، دقیقاً مشابه هیستوگرام توزیع درجه آن است.

۲.۳.۵ مرکزیت بینابینی

در این پژوهش، برای محاسبه مرکزیت بینابینی، از معکوس وزن یال‌ها استفاده شده است؛ زیرا وزن هر یال نشان دهنده میزان وابستگی و هماهنگی گره‌های دو سر آن است و هر چقدر معکوس این مقدار کم‌تر باشد، احتمال بالا رفتن مرکزیت بینابینی بیشتر است.

همانطور که انتظار می‌رفت، گره‌هایی که بخش‌های جدای گراف را به هم متصل می‌کنند، مرکزیت بینابینی بیشتری دارند. بیشترین مرکزیت بینابینی، مربوط به گره ۱ (indegree_mp) است. این گره، تنها راه اتصال ۶ گره پایین بزرگ‌ترین مؤلفه، به تمام گره‌های قسمت بالایی آن است. رتبه‌های بعدی متعلق به گره‌های ۲ و ۳ (neighbors_2_hp و neighbors_2_mp) است. این دو گره گلوگاه‌های ارتباطی قسمت بالا و پایین خودشان هستند. با اینکه گره ۱، نسبت به گره های ۲ و ۳ درجه به مراتب کمتری دارد، اما مرکزیت بینابینی آن بسیار بیشتر است. علت این است که گره ۱، تنها راه ارتباط بین تمام گره‌های بخش های بالا و پایین خودش است؛ در حالی که گره های ۲ و ۳، هر دو واسط ارتباطی بخش های بالا و پایین خودشان هستند و اگر هر کدام از آن‌ها از گراف حذف شود، دیگری می‌تواند نبودش را جبران کند.

گره‌های ۴ و ۵ (neighbors_3_mp و outdegree_mp) در جایگاه بعدی بینابینی قرار دارند. این دو نیز مثل موارد قبلی، گلوگاه ارتباطی هستند اما از آنجایی که واسط رسیدن به گره‌های کم‌تری از گراف هستند ، نسبت به سه گره قبلی، اهمیت کم‌تری دارند.

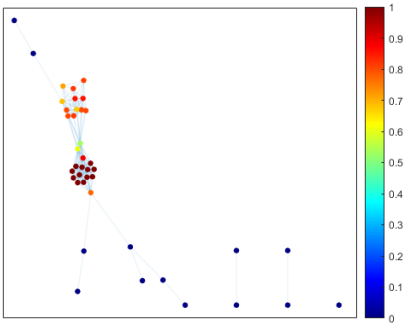
در نمودار ۴، مرکزیت در اکثر گره‌های گراف، مقدار کمی است. اما در انتهای توزیع، چند گره با مرکزیت بالا وجود دارند. در واقع نمودار مرکزیت بینابینی این گراف، مستعد پیروی از قانون توان (power law) است.

۳.۳.۵ مرکزیت بردار ویژه

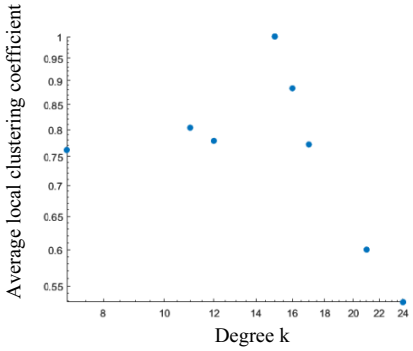
به‌منظور محاسبه مرکزیت برداروِیژه، می‌بایست وزن یال‌ها را به عنوان شاخصی برای اهمیت ارتباطات گره‌ها در نظر بگیریم. در واقع، نتیجه مرکزیت بردار ویژه، در صورتی که وزن یال‌ها را در نظر بگیریم، با زمانی که وزن‌ها را لحاظ نکنیم، متفاوت خواهد بود. در حالت اول، ماتریس مجاورت برای محاسبه مرکزیت بردار ویژه، با مقادیر وزن‌ها پر می‌شود و ارزش یک ارتباط را وزن آن تعیین خواهد کرد اما زمانی که گراف را بدون وزن در نظر بگیریم، صرفا اتصال به گره‌های درجه بالا، اهمیت خواهد داشت.

زمانی‌که تمام یال‌ها، به یک اندازه ارزش داشته باشند، عنصر تعیین کننده‌ی میزان اهمیت گره و همسایگانش، تنها «درجه» خواهد بود، لذا گره‌هایی که خودشان یا همسایگان نزدیکشان بیشترین درجه را داشته باشند، بیشترین مرکزیت را خواهند داشت؛ اما زمانی‌که وزن یال‌ها متفاوت است، برخی از اتصالات مهم‌تر هستند؛ بنابراین علاوه بر درجه، وزن اتصالات با همسایگان نیز تعیین کننده خواهند شد و همانطور که در شکل اول نمایان است، گره‌هایی که با اتصالات محکم‌تری به گره های مهم‌تر متصل هستند، مرکزیت بردار ویژه بالاتری خواهند داشت.

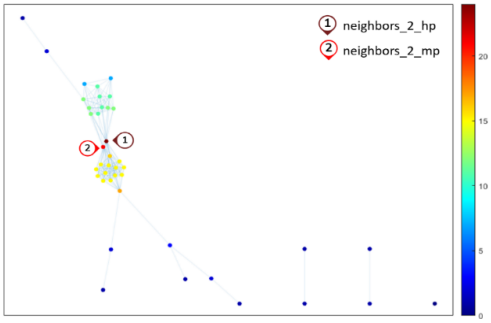
اما چرا بخش میانی گراف، نسبت به hub های شبکه که بیشترین درجات را دارند، مرکزیت بیشتری



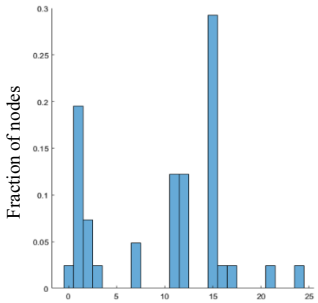
شکل ۲. ضرایب خوشه‌بندی محلی



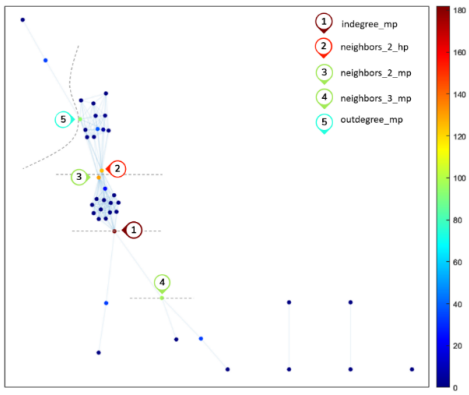
نمودار ۲. خوشه بندی محلی به عنوان تابعی از درجه



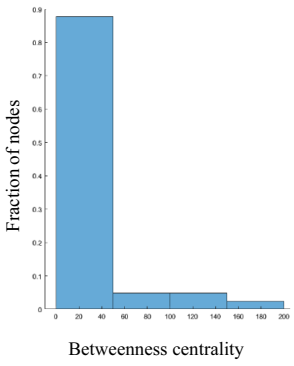
شکل ۳. مرکزیت درجه گراف



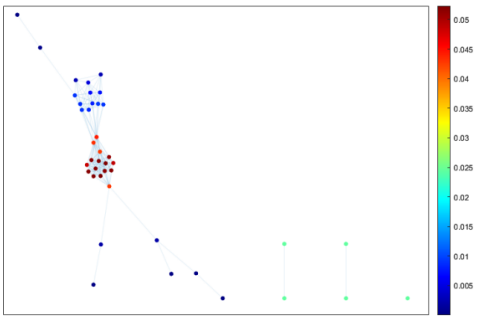
نمودار ۳. هیستوگرام مرکزیت درجه گراف



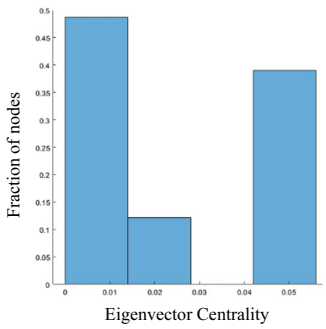
شکل ۴. مرکزیت بینابینی گراف



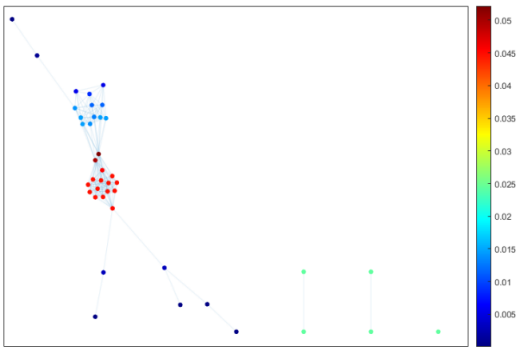
نمودار ۴. هیستوگرام مرکزیت



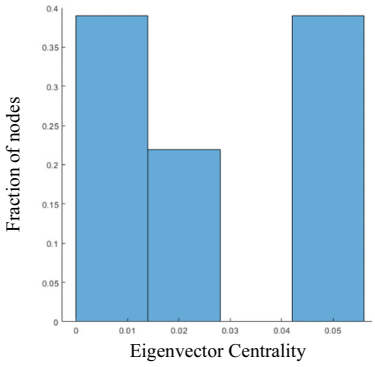
شکل۵. مرکزیت بردار ویژه گراف **با** در نظر گرفتن وزن یال‌ها



نمودار۵. هیستوگرام مرکزیت برداروِیژه گراف **با** در نظر گرفتن وزن یال‌ها



شکل۶. مرکزیت بردار ویژه گراف، **بدون** در نظر گرفتن وزن یال‌ها



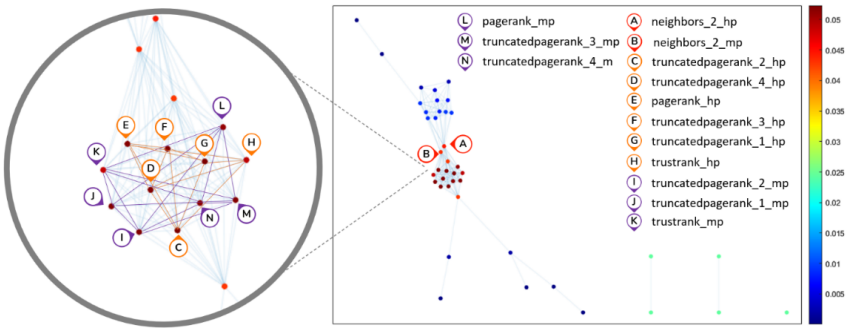
نمودار۶ . هیستوگرام مرکزیت بردار ویژه گراف

دارند؟ برای پاسخ به این سؤال، لازم است کیفیت اتصال گره ها را بررسی کنیم.

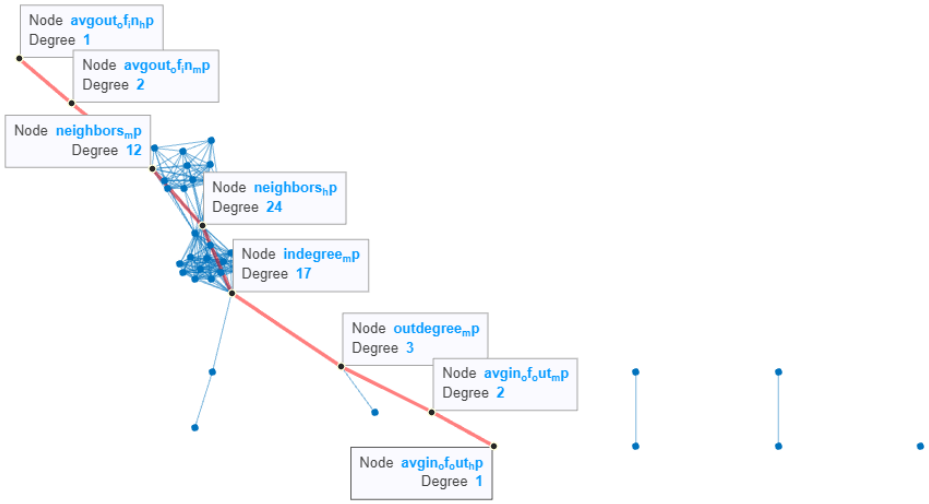
۴.۵ قطر شبکه

همان‌طور که در شکل ۸ پیداست، طولانی‌ترین فاصله، متعلق به دو گره avgin_of_out_hp و avgout_of_in_hp می‌باشد که با ۶ واسطه به یکدیگر متصل شده اند. مجموع این مسیر (اندازه قطر گراف) ۴٫۰۹۰۵ می‌باشد.

مرکزیت بینابینی، نسبت تعداد دفعاتی است که یک گره یا یک یال بر روی کوتاهترین مسیر میان گره‌های مختلف یک گراف قرار می‌گیرد. بررسی شکل ۸ نیز نشان می‌دهد که قطر گراف از نقاطی که بیشترین مرکزیت بینابینی را دارند (neighbors_2_hp, neighbors_3_mp indegree_mp)، عبور کرده است.



شکل ۷. نمایی نزدیک‌تر از مرکزیت بردار ویژه گراف با در نظر گرفتن وزن یال‌ها



شکل ۸. قطر گراف

جدول ۱: خلاصه پژوهش. برخی از ویژگی‌های اندازه‌گیری شده عبارتند از: تعداد گره‌ها (n)، تعداد یال‌ها (m)، میانگین درجه (avg1)، میانگین وزن یال‌ها (avg2)، اندازه بزرگ‌ترین مؤلفه (ns)، کسری از گره‌ها که در بزرگ‌ترین مؤلفه قرار دارند (s)، ضرایب خوشه‌بندی (C1,C2).

ویژگی‌های مورد استفاده	نوع گراف	n	m	avg1	avg2	n_s	S	L	C1	C2
ویژگی‌های مبتنی بر پیوند	بدون جهت	41	202	9.8	0.67	36	0.87	1.2	0.29	0.59
ویژگی‌های مبتنی بر متن	بدون جهت	96	854	17.79	0.64	75	0.78	1.63	0.2	0.7

۶ نتیجه‌گیری

در این پژوهش، گراف‌های شباهت ویژگی‌ها متناظر با دو دسته از ویژگی‌های مبتنی بر متن و نیز مبتنی بر پیوند از مجموعه داده مجموعه WEBSPAM-UK2007 ایجاد گردید و از منظر خصوصیات ساختاری، مورد مطالعه و مورد بررسی قرار گرفت. نتایج کلی به دست آمده در جدول ۱ آمده است.

همان‌طور که مشاهده می‌شود، علیرغم اینکه گراف شباهت ویژگی‌های مبتنی بر متن، نسبت به گراف شباهت ویژگی‌های مبتنی بر پیوند، بزرگ‌تر و به لحاظ تعداد یالها، متراکم‌تر است، با این حال، بر اساس شاخص‌های ضریب خوشه‌بندی، گراف شباهت ویژگی‌های مبتنی بر پیوند، انسجام نسبی بیشتری را دارا می‌باشد. این موضوع با توجه به اندازه نسبی بزرگ‌ترین مولفه همبند نیز تأیید می‌شود.

از این اطلاعات می‌توان به‌منظور کاهش فضای ابعاد داده مسئله شناسایی صفحات اسپم و نیز طراحی الگوریتم‌های جدید در این حوزه، استفاده نمود. از سوی دیگر، استفاده از رویکرد پیشنهای به‌منظور بررسی مجموعه‌های داده دیگر در حوزه شناسایی صفحات اسپم و نیز تحلیل تطبیقی این مجموعه‌های داده بسیار مفید خواهد بود. ضمن اینکه از این نتایج می‌توان به منظور تهیه یک مجموعه داده شناسایی صفحات اسپم در محیط وب فارسی نیز بهره گرفت.

مراجع

[1] Y. Zhang, D. Wang, and Y. Zhang, “Neural IR meets graph embedding: A ranking model for product search,” Web Conf. 2019 - Proc. World Wide Web Conf. WWW 2019, pp. 2390–2400, May 2019, doi: 10.1145/3308558.3313468.

[2] S. Liu, W. Gu, G. Cong, and F. Zhang, “Structural Relationship Representation Learning with Graph Embedding for Personalized Product Search,” Int. Conf. Inf. Knowl. Manag. Proc., pp. 915–924, Oct. 2020, doi: 10.1145/3340531.3411936.

[3] S. Bin Yang and B. Yang, “Learning to rank paths in spatial networks,” Proc. - Int. Conf. Data Eng., vol. 2020-April, pp. 2006–2009, Apr. 2020, doi: 10.1109/ICDE48307.2020.00225.

[4] Q. Xu, M. Li, and M. Yu, “Learning to rank with relational graph and pointwise constraint for cross-modal retrieval,” Soft Comput., vol. 23, no. 19, pp. 9413–9427, Oct. 2019, doi: 10.1007/S00500-018-3608-9/METRICS.

[5] Y. Qi, J. Zhang, Y. Liu, W. Xu, and J. Guo, "CGTR: Convolution Graph Topology Representation for Document Ranking," Int. Conf. Inf. Knowl. Manag. Proc., pp. 2173–2176, Oct. 2020, doi: 10.1145/3340531.3412073.

[6] R. Sawhney, S. Agarwal, A. Wadhwa, and R. Shah, "Exploring the scale-free nature of stock markets: Hyperbolic graph learning for algorithmic trading," Web Conf. 2021 - Proc. World Wide Web Conf. WWW 2021, pp. 11–22, Apr. 2021, doi: 10.1145/3442381.3450095.

[7] Y. Zhang et al., "Learning to Rank Ace Neural Architectures via Normalized Discounted Cumulative Gain," Aug. 2021, doi: 10.48550/arxiv.2108.03001.

[8] T. Formal, S. Clinchant, J. M. Renders, S. Lee, and G. H. Cho, "Learning to Rank Images with Cross-Modal Graph Convolutions," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12035 LNCS, pp. 589–604, 2020, doi: 10.1007/978-3-030-45439-5_39/FIGURES/2.

[9] F. Feng, X. He, X. Wang, C. Luo, Y. Liu, and T. S. Chua, "Temporal Relational Ranking for Stock Prediction," ACM Trans. Inf. Syst., vol. 37, no. 2, Mar. 2019, doi: 10.1145/3309547.

[10] F. Bianchi, M. Palmonari, M. Cremaschi, and E. Fersini, "Actively learning to rank semantic associations for personalized contextual exploration of knowledge graphs," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10249 LNCS, pp. 120–135, 2017, doi: 10.1007/978-3-319-58068-5_8/TABLES/4.

[11] I. Muhammad, D. Bollegala, F. Coenen, C. Gamble, A. Kearney, and P. Williamson, "Document Ranking for Curated Document Databases Using BERT and Knowledge Graph Embeddings: Introducing GRAB-Rank," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12925 LNCS, pp. 116–127, 2021, doi: 10.1007/978-3-030-86534-4_10/COVER.

[12] C. C. Ni, K. Sum Liu, and N. Torzec, "Layered Graph Embedding for Entity Recommendation using Wikipedia in the Yahoo! Knowledge Graph," Web Conf. 2020 - Companion World Wide Web Conf. WWW 2020, pp. 811–818, Apr. 2020, doi: 10.1145/3366424.3383570.

[13] G. Maheshwari, P. Trivedi, D. Lukovnikov, N. Chakraborty, A. Fischer, and J. Lehmann, "Learning to Rank Query Graphs for Complex Question Answering over Knowledge Graphs," in The 18th International Semantic Web Conference (ISWC 2019), Springer, 2019, pp. 487–504. doi: 10.1007/978-3-030-30793-6_28.

[14] J. Y. Yeh and C. J. Tsai, "Graph-based Feature Selection Method for Learning to Rank," ACM Int. Conf. Proceeding Ser., pp. 70–73, Nov. 2020, doi: 10.1145/3442555.3442567.

[15] J. Y. Yeh and C. J. Tsai, "A Graph-based Feature Selection Method for Learning to Rank Using Spectral Clustering for Redundancy Minimization and Biased PageRank for Relevance Analysis," Comput. Sci. Inf. Syst., vol. 19, no. 1, pp. 141–164, Jan. 2022, doi: 10.2298/CSIS201220042Y.

[16] A. H. Keyhanipour, "Graph-based comparative analysis of learning to rank datasets," Int. J. Data Sci. Anal., pp. 1–23, Jun. 2023, doi: 10.1007/S41060-023-00406-8/METRICS.

[17] A.-L. Barabási and M. Pósfai, Network Science, First edit. Cambridge University Press, 2016.

[18] M. Newman, Networks: A Introduction, Second edi. Oxford University Press, 2018.

[19] M. Newman, “The structure and function of complex networks,” SIAM Rev., vol. 45, no. 2, pp. 167–256, 2003, doi: 10.1137/S003614450342480.

مطالعه‌ی ابزارهای برتر شنود شبکه و مقایسه کاربردی Wireshark و Cain and Abel

سارا سعادت[۱]، هایده باقری پور[۱]

[۱]دانشجوی دکتری رشته مهندسی فناوری اطلاعات، پردیس بین‌المللی ارس دانشگاه تهران
{ssaadat,bagheripou}@ut.ac.ir

چکیده

این مقاله مطالعه‌ای بر روی بهترین ابزارهای نفوذ شبکه می‌باشد که از بین آنها Wireshark و Cain and Abel انتخاب‌شده‌اند و اینکه چگونه می‌توان حفره‌های امنیتی و انجام حملاتی مانند شکستن رمز عبور، حمله مرد میانی، شنود ترافیک کاربران و غیره را با این ابزارها آشکار کرد. آزمایش‌ها برای شواهد عملی از طریق ایجاد آزمایشگاه مجازی انجام شده‌است. هدف از این مقاله برای نشان دادن این مهم بود که چگونه می‌توان با آشکار کردن حفره‌های امنیتی مختلف در سیستم مبتنی بر ویندوز، سیستم شخص را به‌راحتی هک کرد. نتایج نشان‌می‌دهد که در صورت کم‌توجهی، سوءاستفاده از یک سیستم یا کشف رمز عبور چقدر ساده است و به‌راحتی می‌توان به امنیت و ایمنی سیستم خدشه وارد کرد. از آنجایی که سیستم‌ها هرگز نمی‌توانند همیشه از حملات در امان باشند، بنابراین دانستن این تهدیدات و استفاده از مکانیسم‌های امنیتی مناسب به‌گونه‌ای که مورد سوء استفاده قرار نگیرد برای افراد مفید خواهد بود.

کلمات کلیدی: شنود شبکه، نفوذ به شبکه، هک، ابزارهای نفوذ، تهدیدات سایبری، حملات رمز عبور، Wireshark، Cain and Abel.

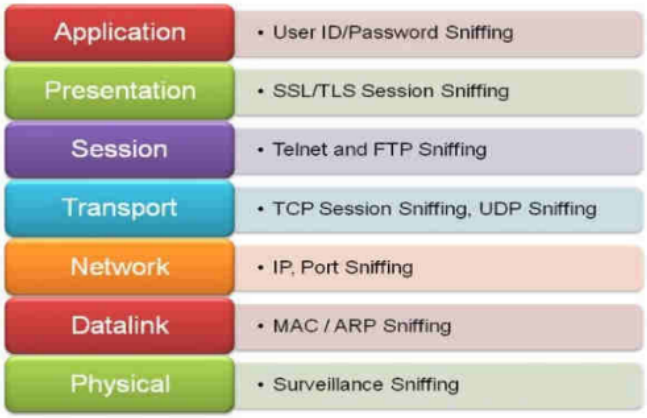
۱ مقدمه

یک شبکه، از مجموعه‌ای از گره‌ها مانند هاب‌ها، پل‌ها، سوئیچ‌ها، رهیاب‌ها[۱]، فایروال‌ها، شکل‌دهنده‌های بسته[۲] تشکیل شده است. هاب‌ها به اتصال دو دستگاه کمک می‌نمایند. پل‌ها و سوئیچ‌ها در لایه ۲ ISO-OSI (ارتباط بین سیستم‌های باز) عمل می‌کنند. رهیاب‌ها نقش تحویل بسته‌ها را از مبدأ به مقصد انجام می‌دهند. فایروال‌ها با فیلترکردن ترافیک بین فرستنده و گیرنده از شبکه‌ها محافظت می‌کنند. بستر شبکه به‌صورت

[1]Router

[۲]packet shapers: شکل‌دهی ترافیک که به شکل‌دهی بسته نیز معروف است، یک روش مدیریت ازدحام است که انتقال داده‌های شبکه را با به تاخیر انداختن جریان بسته‌های کمتر مهم یا کمتر دلخواه تنظیم می‌کند.

۷*۲۴ در حال استفاده است و در معرض انواع مختلفی از حملات مانند ARP[۳] و DDOS[۴] (انکار سرویس توزیع‌شده) است. ازاین‌رو نظارت بر عملکرد آن نقش حیاتی در حفظ شبکه ایفا می‌کند. ابزارهایی مانند Wireshark و Cain and Abel در این مقاله مورد تجزیه‌وتحلیل قرار می‌گیرند. ترافیک شبکه توسط Wireshark قابل‌ردیابی و تفسیر است و با ابزار Cain and Abel حملاتی مانند آشکارسازی رمز عبور و مسمومیت ARP را می‌توان تجزیه‌وتحلیل کرد. اقدامات پیشگیرانه بر اساس خروجی ابزارهای نظارتی مانند Wireshark و سایر ابزارهای نظارتی انجام می‌شود. شنود شبکه به‌صورت کلی شامل گرفتن، رمزگشایی، بازرسی و تفسیر اطلاعات داخل یک بسته شبکه باهدف سرقت اطلاعات است.



شکل ۱: شنود در لایه‌های مختلف OSI [۱]

معمولاً شناسه‌های کاربران، رمزهای عبور، جزئیات شبکه، اطلاعات کارت‌های اعتباری نمونه اطلاعات مهمی هستند که در شبکه مورد تبادل قرار می‌گیرند. شنود به‌طورکلی به‌عنوان یک نوع حمله «غیرفعال» نامیده می‌شود که در آن مهاجمان می‌توانند در شبکه به‌صورت مسکوت از اطلاعات مهم سوءاستفاده کنند [۱].

۲ ادبیات موضوعی

ابزارهای متعددی در حال حاضر به‌منظور شنود، اسکن و آنالیز شبکه مورداستفاده قرار می‌گیرند که در این مقاله نمونه‌هایی از آنها را قید کرده‌ایم [۲، ۳].

[۳] پروتکل ارتباطی«Address Resolution Protocol» یا به‌اختصار پروتکل ARP، برای یافتن آدرس MAC سیستم‌های شبکه است.

[۴] حملات DDoS یا حمله محروم‌سازی از سرویس، یکی از رایج‌ترین و قدرتمندترین حملات سایبری به شمار می‌رود که سرورها و سرویس‌های آنلاین را مورد هدف قرار می‌دهد.

جدول ۱: ویژگی‌های ابزارهای نفوذ به شبکه [۲]

SNO	TOOLS	FEATURES
1	ENDACE	Deep Packet Analyzer
2	Wireshark	Network Protocol Analyzer
3	Tcpdump [2]	Network Sniffer
4	Dsniff	Passive sniffs the network
5	Etherpeek	Protocol Analyzer
6	Sniffit [3]	Network Analyzer
7	Etherflood [4]	White hat hacking purpose
8	ETHERCAP	Packet sniffer
9	Insider	Network Scanner
10	Pof [5]	Identify the Operating system
11	NetworkMiner	Forensic Analyzer
12	Ettercap	Sniffs dynamic connections
13	KISMET	Passive sniffer
14	Cain and Abel	Cracking passwords
15	NetStumbler [6]	Active sniffer
16	Ntop	Determines network status
17	Ngrep	Packet sniffer
18	EtherApe [7]	Network traffic monitor
19	KisMAC	Network discovery tool
20	Aircrack-ng	Detection of network packets
21	SUITE	Creates encrypted packets

۳ بهترین ابزارهای شنود شبکه

۱.۳ Wireshark

Wireshark یک تحلیل‌گر بسته است و برای عیب‌یابی، تجزیه‌وتحلیل شبکه استفاده می‌شود. این پروژه که در ابتدا Ethereal نام داشت، در می 2006 به دلیل مشکلات مربوط به علامت تجاری به Wireshark تغییر نام داد. Wireshark یک رابط کاربری تعاملی است که از pcap برای ضبط بسته‌ها استفاده می‌نماید. بر روی سیستم‌های عامل مختلف نظیر unix و solaris و در مایکروسافت ویندوز اجرا می‌شود. ابزاری است که کاربران می‌توانند از منوی "Capture" آن برای ضبط تصاویر استفاده‌کننده. می‌تواند بسته‌ها را ضبط کرده و انتخاب‌های مختلفی را برای برآوردن تنظیمات و شرایط تحلیل‌گران ارائه دهد [۴].

Wireshark همچنین ویژگی‌های بسیاری را ارائه می‌دهد. از ethernet، IEEE 802.11، PPP و Loopback پشتیبانی می‌کند. Wireshark شامل یک رابط کاربری تعاملی و همچنین یک نسخه خط فرمان است. Wireshark داده‌های ترافیکی با کد رنگی را برای نشان‌دادن پروتکل مورداستفاده برای انتقال نمایش می‌دهد. این ابزار همچنین شامل گزینه‌های مختلف فیلتر است که داده‌های نمایش‌داده‌شده را محدود می‌کند. مهاجم می‌تواند از این ابزار در ترکیب با Cain and Abel برای انجام Session hijacking استفاده نماید [۵].

علاوه بر این Wireshark با ضبط و تحلیل بسته‌های داده‌ای که از طریق رابط شبکه عبور می‌کنند، عمل می‌نماید و به کاربر اجازه می‌دهد تا ترافیک را به طور زنده، ضبط یا فایل‌های پیگیری بسته‌های قبلی را تجزیه‌وتحلیل نماید. این نرم‌افزار از محدوده وسیعی از پروتکل‌ها از جمله HTTP، TCP، UDP، DNS، FTP و بسیاری دیگر پشتیبانی می‌کند و با قابلیت پشتیبانی از ترافیک رمزگذاری شده مانند SSL/TLS، Wireshark درک بهتری از ارتباطات امن را ارائه می‌دهد.

با تجزیه و تحلیل ترافیک شبکه، می‌توان از توانایی‌های Wireshark برای بهبود کارایی شبکه استفاده کرد. با شناسایی الگوها و روندهای ترافیک، متخصصان می‌توانند شبکه را بهینه‌سازی و عملکرد بهتری را فراهم نمایند.

Wireshark قادر به تجزیه‌وتحلیل بسته‌های VoIP (Voice over Internet Protocol) است. این ویژگی، امکان بررسی و مانیتورینگ ارتباطات تلفنی اینترنتی فراهم می‌سازد. همچنین Wireshark قادر به مشاهده پیام‌های DNS (Domain Name System) است. این قابلیت به شما اجازه می‌دهد تا درخواست‌های DNS مورد ارسال و دریافت را بررسی نمایید و به تجزیه‌وتحلیل مسائل احتمالی مرتبط با آن بپردازید.

برای شناسایی ترافیک شبکه، ابزار Wireshark باید بر روی سیستم شما نصب شود تا بسته‌ها را ضبط کند. در ابتدای اجرای برنامه باید کارت شبکه را انتخاب و سپس شروع به ضبط ترافیک کرد.

■ ویژگی‌های پیشرفته Wireshark

- تحلیل پروتکل:

Wireshark می‌تواند طیف وسیعی از پروتکل‌های شبکه، از جمله TCP/IP، UDP، ICMP، HTTP، FTP، DNS، و بسیاری دیگر را تشریح کند که این امکان را می‌دهد که جزئیات هر بسته، مانند آدرس IP مبدأ و مقصد، شماره port و داده‌های بارگذاری را مشاهده کنید.

- فیلتر کردن:

Wireshark این امکان را می‌دهد که بسته‌هایی که در پنجره اصلی نمایش داده می‌شوند را فیلتر کنید. این می‌تواند برای محدودکردن ترافیکی که به تجزیه‌وتحلیل آن علاقه دارید مفید باشد. به‌عنوان‌مثال، می‌توانید بر اساس آدرس IP، شماره port، پروتکل یا کلمه کلیدی فیلتر کنید.

- کدگذاری رنگ:

Wireshark از کدگذاری رنگی برای برجسته‌کردن انواع مختلف ترافیک استفاده می‌کند. این می‌تواند به شما کمک کند تا به‌سرعت انواع بسته‌های موردعلاقه خود را شناسایی کنید. به‌عنوان‌مثال، بسته‌های TCP معمولاً با رنگ سبز، بسته‌های UDP به رنگ آبی و بسته‌های ICMP به رنگ صورتی نمایش داده می‌شوند.

- اطلاعات تخصصی:

Wireshark اطلاعات تخصصی بسیاری از بسته‌هایی را که می‌گیرد ارائه می‌دهد. این اطلاعات می‌تواند به شما کمک کند تا معنای بسته را بفهمید و مشکلاتی را که ممکن است دارید عیب‌یابی کنید.

- آمار:

Wireshark می‌تواند آماری در مورد ترافیک شبکه‌ای که می‌گیرد جمع‌آوری کند. از این آمار می‌توان برای شناسایی روندها و الگوهای ترافیک استفاده کرد.

- گراف‌ها:

Wireshark می‌تواند نمودارهایی از ترافیک شبکه‌ای را که می‌گیرد ایجاد کند. از این نمودارها می‌توان برای تجسم ترافیک و شناسایی مشکلات احتمالی استفاده کرد.

علاوه بر این ویژگی‌های پیشرفته، Wireshark تعدادی ویژگی دیگر نیز دارد که می‌تواند برای عیب‌یابی مشکلات شبکه مفید باشد، مانند توانایی دنبال‌کردن جریان‌های TCP، واکاوی بسته‌های VoIP و تجزیه‌وتحلیل ترافیک شبکه بی‌سیم.

■ نمونه‌هایی از نحوه استفاده از ویژگی‌های پیشرفته Wireshark:

- برای عیب‌یابی اتصال کند شبکه:

می‌توانید از Wireshark برای ضبط ترافیک شبکه استفاده کنید و سپس آن را برای علائم تراکم، از دست‌دادن بسته‌ها یا سایر مشکلات تجزیه‌وتحلیل کنید.

- برای بررسی یک نقض امنیتی:

می‌توانید از Wireshark برای ضبط ترافیک شبکه و سپس تجزیه‌وتحلیل آن برای فعالیت‌های مخرب، مانند آلودگی‌های بدافزار یا تلاش‌های دسترسی غیرمجاز استفاده کنید.

- برای بهینه سازی عملکرد شبکه:

می‌توانید از Wireshark برای ضبط ترافیک شبکه و سپس تجزیه‌وتحلیل آن برای شناسایی تنگناها و سایر مناطقی که شبکه می‌تواند بهبود یابد استفاده کنید.

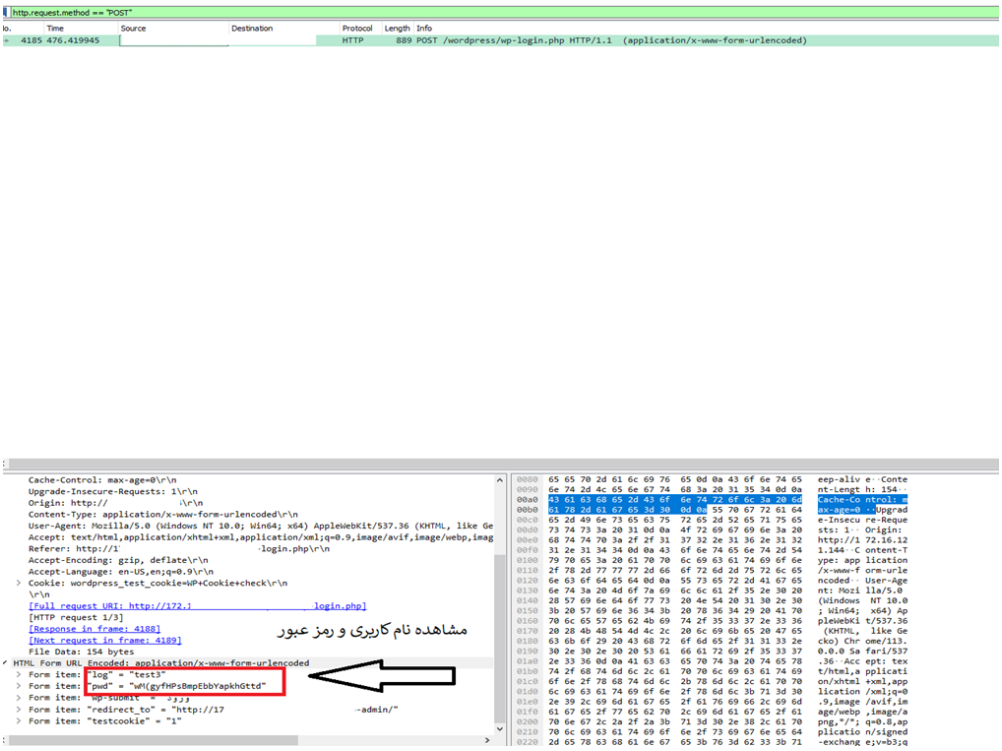
- برای توسعه پروتکل‌های شبکه جدید:

می‌توانید از Wireshark برای ضبط و تجزیه‌وتحلیل ترافیک ایجاد شده توسط پروتکل جدید خود استفاده کنید تا مطمئن شوید که مطابق انتظار کار می‌کند.

Wireshark یک ابزار قدرتمند است که می‌تواند برای اهداف مختلف استفاده شود. با یادگیری نحوه استفاده از ویژگی‌های پیشرفته آن، می‌توان درک عمیق‌تری از ترافیک شبکه به دست آورد و مشکلات شبکه را به طور مؤثرتری عیب‌یابی کرد.

۱.۱.۳ شنود شبکه با Wireshark

برای مشاهده رمز عبور در Wireshark، http را در فیلتر تایپ کرده و روی Apply کلیک کنید. این کار تمام بسته‌های http را فیلتر می‌کند. اگر روی فیلتر انجام شده روی پروتکل http، مجدد فیلتر متد post را اعمال کنید، در جزئیات ترافیک، نام کاربری و رمز عبور وارد شده برای آی پی مقصد به‌وضوح قابل‌مشاهده است. http.request.method == ”POST”



شکل ۲: مشاهده نام کاربری و رمز عبور از ترافیک ضبط شده

۲.۱.۳ جایگزین‌های Wireshark

ما ۷ جایگزین برای Wireshark فهرست کرده‌ایم که دارای ویژگی‌های مشابهی مانند Wireshark از جمله ساختاری، رایگان و منبع‌باز بودن هستند [۶، ۷].

جدول ۲: جایگزین‌های منبع باز Wireshark [۷]

ابزار	توضیحات ابزار
tcpdump	tcpdump از کتابخانه libpcap برای گرفتن بسته‌ها استفاده می‌کند.
Microsoft Network Monitor	Microsoft Network Monitor یک تحلیلگر بسته برای ضبط، مشاهده و تجزیه‌وتحلیل داده‌های شبکه و رمزگشایی پروتکل‌های شبکه که در حال حاضر توسعه آن متوقف شده است.
Intercepter-NG	Intercepter-NG یک ابزار شبکه چندمنظوره برای انواع مختلف بازیابی اطلاعات جالب از جریان شبکه و انجام انواع مختلف MiTM است.
apptalk.ninja	apptalk.ninja یک نرم‌افزار نظارت بر اپلیکیشن موبایل است.
netcat	Netcat (nc) یک ابزار شبکه کامپیوتری برای خواندن و نوشتن از طریق اتصالات شبکه با استفاده از TCP یا UDP است. Netcat به شکل یک پشتیبان قابل‌اعتماد طراحی شده است.
Ettercap	Ettercap یک مجموعه جامع برای حملات مرد میانی است.
Nethogs	Nethogs یک نرم‌افزار نظارت بر پهنای باند است.

https://appmus.com/alternatives-to/wireshark

۲.۳ Cain and Abel

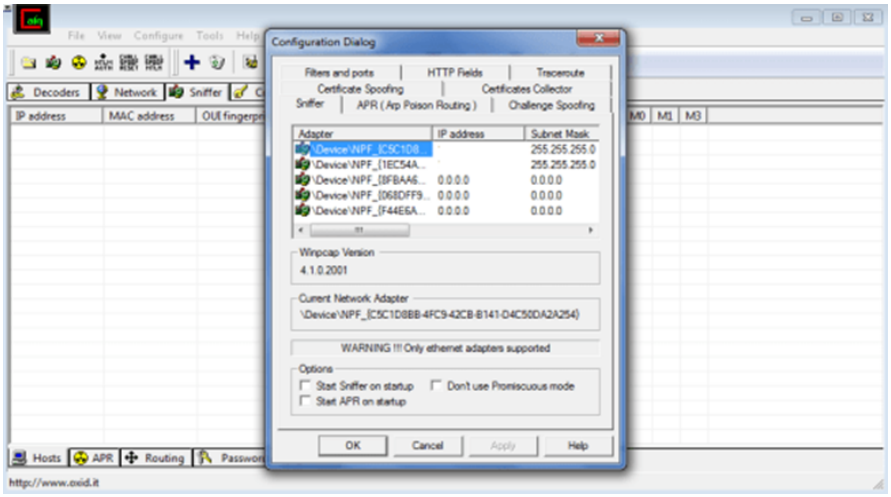
Cain and Abel یک ابزار بازیابی رمز عبور برای سیستم‌عامل‌های مایکروسافت است که اجازه بازیابی آسان با استراق سمع شبکه، آشکارسازی رمزهای عبور با استفاده از Dictionary، Brute-Force و حملات Cryptanalysis، ضبط مکالمات VoIP، رمزگشایی رمزهای عبور درهم، بازیابی کلیدهای شبکه بی‌سیم، کشف رمزهای عبور ذخیره شده و تجزیه‌وتحلیل پروتکل‌های مسیریابی را فراهم می‌کند. برنامه قابلیت exploit آسیب‌پذیری نرم‌افزاری را ندارد؛ ولی برخی از جنبه‌های امنیتی / ضعف موجود در پروتکل‌ها، استانداردها، روش‌های احراز هویت و حافظه پنهان را پوشش می‌دهد [۳، ۶، ۸]. همچنین می‌تواند پروتکل‌های رمزگذاری شده مانند SSH-1 و HTTPS را تجزیه‌وتحلیل کند و شامل فیلترهایی برای گرفتن اعتبار از سازوکارهای کنترلی مختلف است [۵].

۱.۲.۳ شنود شبکه با Cain and Abel

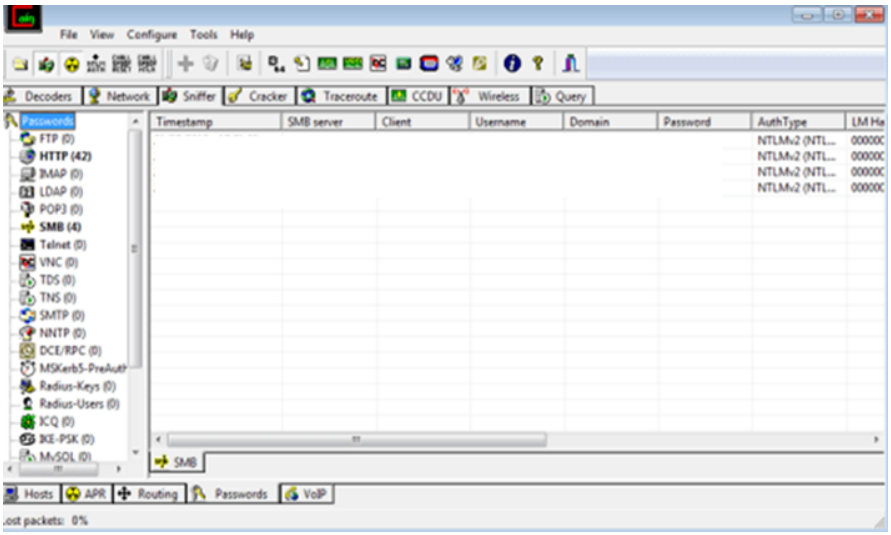
برای آشکارسازی پسوردهای رمزنگاری شده از حمله دیکشنری و brute-force معمولاً از این ابزار استفاده می‌شود و همچنین سایر حملاتی مانند DNS و ARP نیز از طریق آن قابل‌انجام است.

برای شنود رمزهای عبور در حال تبادل روی شبکه، ابتدا نرم‌افزار Cain and Abel را اجرا نموده، سپس در منوی بالایی نرم‌افزار گزینه Configure را انتخاب کرده و در مرحله بعد آداپتور شبکه مناسب را برای

شنود پسوردها به‌صورت متن ساده انتخاب می‌نماییم.



شکل ۳: نحوه تنظیمات در Cain and Abel



شکل ۴: آشکارسازی رمز عبور در Cain and Abel

۲.۲.۳ جایگزین‌های Cain and Abel

در جدول ۳، نه جایگزین برای ابزار Cain and Abel، معرفی شده است.

جدول ۳: جایگزین‌های منبع‌باز Cain and Abel

ابزار	توضیحات ابزار
Wireshark	Wireshark یک ابزار ردیابی شبکه منبع‌باز برای تجزیه‌وتحلیل ترافیک شبکه است.
Ophcrack	Ophcrack یک برنامه منبع‌باز رایگان (دارای مجوز GPL)[۵] است که رمزهای عبور ورود به سیستم ویندوز را با استفاده از هش‌های LM از طریق جداول رنگین‌کمان[۶] می‌شکند.
Reaver	reaver برای بازیابی رمزهای عبور WPA/WPA2 است و یک حمله brute force علیه پین‌های ثبت‌کننده الگوریتم محافظت شده Wifi (WPS) اجرا می‌کند.
Ettercap	Ettercap یک مجموعه جامع برای حملات مرد میانی است.
Kon-Boot (تجاری)	Kon-Boot برنامه‌ای است که فرایند احراز هویت سیستم‌عامل‌های مبتنی بر ویندوز را دور می‌زند.
Aircrack-ng	Aircrack-ng یک مجموعه نرم‌افزار شبکه است که از آشکارساز، ردیاب بسته، رمزگشای WEP و WPA/WPA2-PSK و ابزار تجزیه‌وتحلیل برای شبکه‌های محلی بی‌سیم 802.11 تشکیل شده است.
Offline NT Password and Registry Editor	chntpw یک ابزار نرم‌افزاری برای بازنشانی یا خالی‌کردن رمزهای عبور محلی است که توسط Windows NT، 2000، XP، Vista، 7، 8 و 8.1 استفاده می‌شود.
John the Ripper	John the Ripper یک ابزار نرم‌افزاری رایگان برای شکستن رمز عبور است.
Intercepter-NG	Intercepter-NG یک ابزار شبکه چندمنظوره برای انواع مختلف حملات مرد میانی یا MiTM است.

https://appmus.com/alternatives-to/cain-and-abel

۴ مقایسه کاربردی Wireshark و Cain and Abel

در جدول ۴ مقایسه کاربردی Wireshark و Cain and Abel ارائه شده است.

[۵] GPL یا General Public License که گاهی به آن GNU GPL نیز گفته می‌شود، رایج‌ترین مجوز نرم‌افزار رایگان است. این کار توسط ریچارد استالمن از بنیاد نرم‌افزار آزاد برای پروژه گنو نوشته شده است. این مجوز اجازه می‌دهد تا نرم‌افزار آزادانه مورداستفاده، اصلاح و توزیع مجدد قرار گیرد.

[۶] rainbow tables: جدول رنگین‌کمان یک جدول از پیش محاسبه شده برای ذخیره خروجی‌های یک تابع هش رمزنگاری است که معمولاً برای شکستن هش رمز عبور است.

جدول ۴: مقایسه کاربردی Wireshark و Cain and Abel

ویژگی‌ها	Wireshark	Cain and Abel
تولیدکننده	تیم Wireshark	توسط Massimiliano montro
رابط میانی	GUI and CLI	GUI
لایسنس نرم‌افزار	Freeware	GNU
سیستم‌عامل	لینوکس و ویندوز	فقط پلتفرم ویندوز
ویژگی اصلی	ابزار عالی آنالیز شبکه	
آسیب‌پذیری نرم‌افزار	قابلیت exploit آنها را دارد.	قابلیت exploit آنها را ندارد.
TCP/IP Stream	قابلیت بازیابی آن را دارد.	قابلیت بازیابی آن را ندارد.
تحلیل ترافیک	آنالیز جزئی ترافیک شبکه	قابلیت آنالیز جزئی را ندارد و صرفاً تعداد پکت‌های اخذ شده یا شنود شده را نشان می‌دهد.
پشتیبانی پروتکل‌های شبکه	طیف گسترده	محدود
سهولت کاربری	متوسط	آسان
پشتیبانی سیستم‌عامل اندروید	دارد	دارد
تحلیل جزئیات اطلاعات بسته	دارد	دارد
نظارت بر عملکرد شبکه	دارد	دارد
مشاهده فعالیت‌های در لحظه شبکه	دارد	ندارد
نظارت بر عملکرد برنامه‌های کاربردی	دارد	ندارد
نظارت بر عملکرد CPU و RAM	دارد	ندارد
نظارت بر عملکرد پروتکل HTTP	دارد	ندارد
دورزدن، بازیابی و شکستن رمز عبور	ندارد	دارد

۵ محدودیت‌ها و معایب Wireshark و Cain and Abel

۱.۵ معایب Wireshark

هرچند Wireshark یک ابزار قدرتمند است، اما استفاده از آن نیازمند دانش و تجربه است. همچنین تحلیل ترافیک شبکه ممکن است پیچیده و زمان‌بر باشد و نیازمند تخصص و آگاهی در زمینه پروتکل‌ها و مفاهیم شبکه است.

همچنین باید به محدودیت‌ها در استفاده از Wireshark توجه داشت. به‌عنوان یک ابزار بررسی ترافیک، Wireshark نمی‌تواند به طور کامل اطلاعات رمزنگاری شده را نمایش دهد و نیازمند دسترسی به کلیدها و رمزهای مربوطه است.

۲.۵ معایب Cain and Abel

- Cain and Abel می‌تواند موجب کندی ارتباطات شود. این امر به طور بالقوه می‌تواند حمله را آشکار

کند و کاربر را مشکوک نماید. در آزمایش‌ها، حدود ۳۰ درصد تفاوت بین یک اتصال معمولی و یک اتصال مسموم ARP پیدا کردیم، اما نتایج ممکن است برای سایرین متفاوت باشد. سرعت اضافه شده به دلیل گره اضافی است که بسته‌ها باید از آن عبور نمایند.

- به طور پیش‌فرض نمی‌تواند رمزهای عبور بسیاری از وبگاه‌ها را شناسایی کند. مگر اینکه وبگاهی از یک فیلد رمز عبور مانند "pass" یا "pw" استفاده کند، Cain و Abel آن را با پیکربندی پیش‌فرض تشخیص نخواهند داد. برای اجرا به دسترسی سطح مدیر نیاز دارد. این ابزار با برخی از ابزارهای کرک مانند Ophcrack که برای کرک کردن هش‌ها به هیچ حساب کاربری نیاز ندارند، تفاوت دارد.
- جعل ARP نیاز به دسترسی به شبکه دارد. هیچ کاری با ARP انجام نمی‌شود مگر اینکه کاربر به‌درستی به شبکه متصل باشد [۱۰].

۶ نتیجه‌گیری

ابزارهای متعددی برای شنود و آنالیز ترافیک شبکه مورداستفاده قرار می‌گیرند که ازاین‌بین دو نمونه از بهترین ابزارها مورد بررسی و مقایسه قرار گرفتند. ترافیک شنود شده در آزمایشگاه مورد تحلیل قرار گرفت و نتایج آن ارائه گردید.

- Wireshark ابزار بهتر برای آنالیز شبکه و رصد ترافیک شبکه برای مدیران
- Cain and Abel ابزار ساده‌تر برای آشکارسازی رمز عبور ها

Wireshark به‌عنوان یک تحلیل‌گر پروتکل شبکه منبع‌باز قدرتمند، در ضبط بسته‌های بلادرنگ، تجزیه‌وتحلیل عمیق پروتکل و طیف گسترده‌ای از پلتفرم‌های پشتیبانی شده خود برجسته است. پشتیبانی گسترده، مستندات جامع و رابط کاربرپسند، آن را به انتخابی ارجح برای مدیران شبکه و متخصصان امنیتی که به دنبال بینش دقیق شبکه هستند، تبدیل کرده است. به نظر می‌رسد برای آنالیز ترافیک شبکه ابزار Wireshark مناسب‌تر و جامع‌تر باشد درعین‌حال برای شنود رمز عبور که یکی مهم‌ترین علاقه‌مندی هکرها است، Cain and Abel ابزار مناسبی است. اگر به دنبال یک تحلیلگر بسته ساده و با کاربری آسان هستید، Cain and Abel انتخاب خوبی است. همچنین اگر بتوانید رمزهای عبور را بشکنید یا رمزهای عبور ذخیره شده را از مرورگرها بازیابی کنید، انتخاب خوبی است.

بااین‌حال، مهم است که توجه داشته باشید که Cain and Abel به‌اندازه Wireshark به طور فعال توسعه‌نیافته است و ممکن است از آخرین پروتکل‌های شبکه پشتیبانی نکند.

در کارهای آتی به مطالعه سایر ابزارها و ارائه شواهد شبکه‌ای آنالیز و نفوذ به شبکه در دست اقدام توسط این تیم است.

سپاس‌گزاری

از زحمات جناب آقای دکتر آراسته راد، استاد راهنمای گرامی و سرپرست محترم پژوهشگاه کمال قدردانی را داریم.

مراجع

[1] V. Singh، M. Kumar and L. Raj، "Efficient Method for Preventing Password Sniffing Using MD5 Algorithm"، International Journal of Advanced Engineering Research and Science (IJAERS)، Vol-3، Issue-3، March- 2016، ISSN: 2349-6495.

[2] M. Fathima K M and N. Santhiyakumari، "A Survey On Network Packet Inspection And ARP Poisoning Using Wireshark And Ettercap"، Proceedings of the International Conference on Artificial Intelligence and Smart Systems (ICAIS-2021)، IEEE Xplore Part Number: CFP21OAB-ART; ISBN: 978-1-7281-9537-7

[3] A. Avritzer, R. G. Cole and E. J. Weyuker، "Monitoring for Security Intrusion using Performance Signatures"، WOSP/SIPEW'10، January 28–30، 2010، San Jose، California، USA. Copyright 2010 ACM 978-1-60558-563-5/10/01

[4] S. Dilip Sarve, S. Mahadik, "Comparative Study on Packet Sniffing Tools", International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), Volume 2, Issue 1, July 2022, Copyright to IJARSCT DOI:10.48175/IJARSCT-5697403

[5] Z. Balogh, S. Koprda and J. Francisti, "LAN security analysis and design", IEEE 12th International Conference on Application of Information and Communication Technologies, October 2018 DOI:10.1109/ICAICT.2018.8746912

[6] N. Kaur and J. Singh، "ETHICAL HACKING IN WINDOWS ENVIRONMENT"، IJESRT INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES and RESEARCH TECHNOLOGY، ISSN: 2277-9655، DOI: 10.5281/zenodo.46485، February 2016.

[7] https://appmus.com/vs/wireshark-vs-cain-and-abel

[8] http://www.wireshark.org/

[9] http://www.oxid.it/cain.html

[10] http://www.cs.toronto.edu/~arnold/427/15s/csc427/tools/CainAndAbel/index.html

پیشرفت مطلق یا هدفمند هوش مصنوعی در اندیشه مقام معظم رهبری

حمید محسنی [۱]، کاظم فولادی قلعه [۲]

[۱] دکتری حکمت متعالیه از مؤسسه آموزشی و پژوهشی امام خمینی (ره)، قم
h.mohseni1297@mailfa.com
[۲] استادیار گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
kfouladi@ut.ac.ir

چکیده

از منظر برخی اندیشمندان و متفکران در آینده نه‌چندان دور هوش مصنوعی در مسئله حکمرانی دنیا و جوامع نقشه بسزایی خواهد داشت. به همین دلیل اخیراً مقام معظم رهبری بر پیشرفت در حوزه هوش مصنوعی تأکید کرده‌اند. اما برای مواجهه درست و دقیق با دیدگاه معظم له، می‌بایست اندیشه وی دراین‌باره تبیین و بررسی شود. ازاین‌رو مسئله اصلی تحقیق حاضر این است که آیا نگرش واقعی رهبری در حوزه هوش مصنوعی به‌طور مطلق و در هر شرایطی بوده یا هدفمند و جهت‌دار است؟ با تأمل و واکاوی اندیشه مقام معظم رهبری مشخص شد همان‌طور که ایشان بر اصل ضرورت پیشرفت در حوزه فناوری هوش مصنوعی تأکید کرده‌اند بر هدفمندی و جهت گذاری صحیح هوش مصنوعی نیز تأکید دارند. اصل توحیدمحوری یکی از جنبه‌های هدفمندی در پیشرفت هوش مصنوعی است. هدف مهم دیگر تحقیق حاضر این بود که مسئله هوش مصنوعی یک فناوری صرف نبوده، بلکه می‌تواند تأثیرات مهم فرهنگی، دینی تمدنی و حکمرانی داشته باشد. ازاین‌رو پیشرفت این نوع فناوری در نظام و تمدن اسلامی می‌بایست هدفمند و بر محور توحید باشد. افزون براین از منظر رهبری پیشرفت هر نوع علم و فناوری مبتنی بر مباحث فکری و فلسفی است. درنتیجه، با تبیین نگرش واقعی رهبری بسیاری از ابهامات برای مسئولان و قانون‌گذاران و محققان در مواجهه با پیشرفت هوش مصنوعی برطرف خواهد شد.

کلمات کلیدی: ضرورت پیشرفت، اصل هدفمندی، اصل توحید، مقام معظم رهبری.

۱ مقدمه

از منظر برخی محققان، هوش مصنوعی تنها جنبه‌ی فنی و مهندسی دارد؛ به‌همین دلیل با این نوع فناوری تنها مواجهه ابزاری دارند. در این رویکرد، بیشتر فواید و منافع ابزاری هوش مصنوعی در نظر گرفته می‌شود (ویتبای، ۱۴۰۱). اما از منظر دیگر متفکران، به‌زودی هوش مصنوعی همه حیات و تلاش‌های بشری را تحت

تأثیر خود قرار خواهد داد. تحولات دوران‌ساز ناشی از هوش مصنوعی در جامعه، اقتصاد، سیاست، فرهنگ، علوم انسانی، حکمرانی اثرات بسیاری خواهد گذاشت (کیسینجر و همکاران، ۱۴۰۱). به‌طورکلی همین هوش مصنوعی امروز (هوش مصنوعی محدود[1]) در زندگی بسیاری از انسان‌ها تأثیرگذار است (Russell & Norvig, 2020). بنابراین با پیشرفت روزافزون هوش مصنوعی به‌زودی همه ابعاد زندگی در جوامع بشری تحت شعاع این فناوری نوین قرار خواهد گرفت.

ازاین‌رو، در آینده نه‌چندان دور هوش مصنوعی در مسئله حکمرانی دنیا و جوامع نقشه بسزایی خواهد داشت. به‌همین دلیل مقام معظم رهبری اخیراً بر پیشرفت در حوزه هوش مصنوعی تأکید کرده‌اند: «پیشنهاد می‌کنم یکی از مسائلی که مورد تکیه و توجّه و تعمیق واقع می‌شود، مسئله‌ی هوش مصنوعی باشد که در اداره‌ی آینده‌ی دنیا نقش خواهد داشت؛ ... باید کاری کنیم که حدّ اقل به ده کشور اوّل دنیا در این مسئله برسیم» (بیانات، دیدار جمعی از نخبگان و استعدادهای برتر علمی کشور، ۱۴۰۰/۰۸/۲۶). بنابراین نگرش مقام معظم رهبری در بحث فناوری هوش مصنوعی، پیشرفت در این زمینه بوده و ایران اسلامی نمی‌بایست در دست‌یابی به این نوع فناوری‌ها عقب بماند. اما می‌بایست دیدگاه رهبری به‌طور دقیق و واقع‌بینانه بررسی شود. زیرا از یک‌سو رهبری در عبارت مذکور به‌ظاهر ضرورت پیشرفت هوش مصنوعی را به‌طور مطلق مطرح کرده‌اند. از سوی دیگر می‌بایست روشن شود اندیشه واقعی مقام معظم رهبری درباره پیشرفت فناوری‌های نوین و هوش مصنوعی چیست؟ آیا نگرش در حوزه پیشرفت فناوری‌های نوین –به‌طور عام– و فناوری هوش مصنوعی –به‌طور خاص– هدف‌مند و جهت‌دار است؟ به‌تحلیل دیگر، مسئله اصلی تحقیق حاضر این است که در نگرش عمیق و ژرف می‌بایست بررسی کرد که آیا منظور رهبری از پیشرفت در حوزه هوش مصنوعی به‌طور مطلق و در هر شرایطی بوده یا هدف‌مند و جهت‌دار است؟ بنابراین در این تحقیق نگرش واقعی آیت‌الله خامنه‌ای در حوزه پیشرفت فناوری هوش مصنوعی تبیین و واکاوی می‌شود.

۲ پیشینه تحقیق

در راستای مسئله بحث حاضر، تحقیقات مستقل، جامع و کامل که نگرش واقعی در حوزه پیشرفت فناوری هوش مصنوعی از منظر رهبری را واکاوی کرده باشد، مشاهده نشد. اما برخی تحقیقات که به‌نوعی با مسئله‌ی تحقیق حاضر ارتباط دارند را می‌توان در ادامه اشاره کرد. سند «الگوی اسلامی ایرانی پیشرفت» توسط برخی از متفکران تنظیم‌شده است. در این سند تنها پیشرفت در حوزه اقتصاد به‌طور خاص مبتنی بر مبانی نظری اسلامی برجسته شده است؛ ولی مسئله پیشرفت علم و فناوری مورد مداقه قرار نگرفته است (https://www.olgou.ir/index.php/fa). مقاله «نقشه راه رهبری برای تولید علم و فناوری، توسعه و پیشرفت»، تا حدودی به اهداف پژوهش حاضر نزدیک است؛ در این مقاله سعی شده است محورهای پیشرفت در حوزه علم و فناوری از منظر مقام معظم رهبری تبیین شود، ولی به نظر می‌رسد به‌طور دقیق و منسجم و کامل اندیشه مقام رهبری دراین‌باره تبیین نشده است (تاجریان، ۱۳۸۸). در تحقیق «فناوری‌های نوظهور و تأثیر آنها بر تمدن نوین اسلامی» کمی مفصل‌تر بحث تأثیر فناوری‌ها به‌خصوص تأثیر کاربردی و ابزاری

[1] Artificial Narrow Intelligence: ANI

فناوری‌های نوظهور بر تمدن نوین اسلامی به‌طور کلی توضیح داده‌شده است، ولی اصلاً به‌طور مصداقی و عینی به بحث هوش مصنوعی به‌عنوان یکی از فناوری‌های نوظهور اشاره نشده است (قاسمی، و نصیرلو، ۱۴۰۰). در مقاله «نقش هوش مصنوعی در فرهنگ نوین تمدن اسلامی»، که در واقع گزارشی در حدود ۱۳ صفحه است، سعی شده است با رویکردی خوش‌بینانه و با بیان مواردی کلی، استفاده از هوش مصنوعی در راستای تمدن و فرهنگ اسلامی توجیه شود (سهرابی مقدم چافجیری، و اکبرنژاد دموچالی، ۱۴۰۱).

همچنین برخی مراکز دیدگاه‌های رهبری درباره علم و فناوری را جمع‌آوری کرده‌اند ولی چندان به تحقیق و واکاوی نگرش معظم له نپرداخته‌اند (شورای عالی انقلاب فرهنگی، ۱۳۸۹؛ همچنین: مؤسسه فرهنگی حدیث لو و قلم، ۱۳۹۰) بدین‌سان عمده بحث و تمرکز اصلی کاوش حاضر تحلیل پیشرفت مطلق و یا هدفمند در حوزه هوش مصنوعی با استفاده از اندیشه مقام معظم رهبری خواهد بود.

۳ تبیین مفاهیم و اصطلاحات

۱.۳ ارتباط علم با فناوری

پیش از ورود به بحث واکاوی مسئله، تبیین ارتباط علم و فناوری شایسته به نظر می‌رسد. زیرا بحث اصلی تحقیق حاضر درباره فناوری و به‌طور خاص فناوری هوش مصنوعی از منظر مقام معظم رهبری است، اما این مسئله بی‌ارتباط با مسائل حوزه علم نیست. زیرا به باور رهبری علم با فناوری ارتباط اساسی و جدی دارد (بیانات در دیدار اساتید دانشگاه‌ها، ۱۳۹۳/۰۴/۱۱). به بیان دقیق‌تر فناوری از دل دانش و علم بیرون می‌آید؛ ازاین‌رو دانش، پایه فناوری‌های پیشرفته است (بیانات در دیدار رؤسای دانشگاه‌ها و مؤسسات آموزش عالی، ۱۳۸۵/۰۵/۲۳). در نتیجه اندیشه‌ای که مقام معظم رهبری درباره علم و دانش دارند، فناوری را نیز دربر می‌گیرد.

۲.۳ معنای پیشرفت و فرق آن با توسعه

در اندیشه رهبری مفهوم «پیشرفت» با «توسعه» فرق می‌کند (اصطلاح «توسعه» در ادبیات غربی مورد توجه است، ولی در اندیشه رهبری اصطلاح «پیشرفت» مورد تأکید است) (بیانات در دیدار رئیس‌جمهور و اعضای هیأت دولت، ۱۳۹۲/۰۶/۰۶). به‌بیان‌دیگر، در اندیشه رهبری اصطلاح پیشرفت بر واژه توسعه ترجیح دارد، زیرا کلمه توسعه بار ارزشی و معنای خاص خود را دارد. این اصطلاح التزاماتی با خود همراه دارد که نمی‌توان در نظام اسلامی این التزامات را پذیرفت (بیانات در نخستین نشست اندیشه‌های راهبردی، ۱۳۸۹/۰۹/۱۰)، اما مفهوم پیشرفت مفهومی است که می‌تواند اهداف نظام اسلامی را تا حدود زیادی در خود جمع کند (بیانات در دیدار جوانان استان خراسان شمالی، ۱۳۹۱/۰۷/۲۳). افزون بر این، توسعه در فرهنگ غربی یک یا دو بعدی است؛ ولی پیشرفت در مفهوم اسلامی چند بعدی است که سبک زندگی، معنویت و رستگاری انسان را نیز شامل می‌شود (بیانات در دیدار جوانان استان خراسان شمالی، ۱۳۹۱/۰۷/۲۳).

ازاین‌رو در اندیشه رهبری مفهوم پیشرفت تنها در بعد دانش و فناوری خلاصه نمی‌شود، بلکه به همراه پیشرفت فناوری در جنبه‌های تولید ثروت، اقتدار ملی، عزت بین‌المللی نیز می‌بایست پیشرفت کرد. افزون بر

این به‌همراه این‌ها پیشرفت در اخلاق و معنویت و امنیت اجتماعی و اخلاقی نیز ضروری است. همچنین به اعتقاد رهبری اگر پیشرفت با عدالت همراه نباشد، این نوع پیشرفت موردنظر اسلام نیست (بیانات در دیدار زائران و مجاوران بارگاه حضرت علی‌بن‌موسی الرضا، ۱۳۸۸/۰۱/۰۱). ازاین‌رو نگرش رهبری به‌لحاظ مفهوم و معنای پیشرفت تنها در بعدی فناوری صرف خلاصه نمی‌شود.

۴ نگرش مقام معظم رهبری به فناوری هوش مصنوعی

۱.۴ اصل ضرورت پیشرفت

بنا بر اندیشه آیت‌الله خامنه‌ای یکی از وظایف اصلی و ضروری جامعه ما این است که دنبال فناوری‌های نوین باشیم و می‌بایست هر فناوری که موجب استقلال، عدم وابستگی و عزت کشور است را به‌دست آوریم (بیانات در دیدار جمعی از مسئولان جهاد دانشگاهی، ۱۳۸۳/۰۴/۰۱)، بلکه نگرش مقام معظم رهبری براین است که اصل پیشرفت و «تحول» یک سنت و قاعده الهی و قرآنی است؛ زیرا خداوند متعال در قرآن کریم می‌فرماید: «إِنَّ اللَّهَ لا يغَيرُ ما بِقَوْمٍ حَتَّى يغَيرُوا ما بِأَنْفُسِهِم» (رعد، ۱۳)؛ یعنی کلید تحولات و تحولات بزرگ در دست انسان‌ها است (بیانات در دیدار دانشگاهیان سمنان، ۱۳۸۵/۰۸/۱۸). در راستای مسئله حاضر نیز رهبری تأکید می‌کنند جامعه ما امروز در بحث فناوری‌های نوین همچون علوم شناختی و فناوری‌های مرتبط با آن، و فناوری هوش مصنوعی نمی‌بایست عقب بماند: «در زمینه‌ی هوش مصنوعی مثلاً ما چهاردهم هستیم در دنیا- اگر چنانچه یک ذرّه غفلت کنیم و خوابمان ببرد، بسرعت سقوط خواهیم کرد و پنجاه سالِ دیگر خواهیم شد پنجاهم، خواهیم شد صدم، یعنی دنیا از ما جلو می‌افتد و می‌رود. این نکته مهمّی است و باید همه به این توجّه کنند» (بیانات در دیدار مسئولان و محققان ستاد توسعه علوم شناختی، ۱۳۹۷/۱۱/۰۳). افزون بر این، اخیراً رهبری به‌طور مستقل در مقوله هوش مصنوعی تأکید کردند: «پیشنهاد می‌کنم یکی از مسائلی که مورد تکیه و توجّه و تعمیق واقع می‌شود، مسئله‌ی هوش مصنوعی باشد که در اداره‌ی آینده‌ی دنیا نقش خواهد داشت؛ ... باید کاری کنیم که حدّاقل به ده کشور اوّل دنیا در این مسئله برسیم» (بیانات، دیدار جمعی از نخبگان و استعدادهای برتر علمی کشور، ۱۴۰۰/۰۸/۲۶).

بنابراین تا بدین جا دیدگاه رهبری درباره اصل ضرورت پیشرفت در حوزه فناوری‌های نوین و هوش مصنوعی تبیین شد. بنابراین اصل و نگرش، دیدگاه کسانی که با هر نوع فناوری و یا تحول مخالف هستند و یا برخی که اصل فناوری‌های نوین را در تضاد با آموزه‌های اسلامی می‌دانند، رد می‌شود. افزون بر این، اصل ضرورت پیشرفت جامعه اسلامی در حوزه فناوری‌های نوین و هوش مصنوعی نمایان می‌شود.

اما همان‌طور که گذشت می‌بایست دیدگاه واقعی رهبری در حوزه پیشرفت هوش مصنوعی تبیین شود که به‌طور مطلق بوده یا اینکه ایشان پیشرفت درزمینه‌ی فناوری هوش مصنوعی را هدفمند و جهت‌دار می‌داند؟

۲.۴ اصل هدفمندی فناوری

با دقت و تأمل در اندیشه رهبری مشخص می‌شود اصل مهم در پیشرفت فناوری این است که می‌بایست در این حوزه هدف‌گذاری و جهت‌گیری صحیح داشت. همان‌طور که وی به پیشرفت در حوزه فناوری تأکید

کرده‌اند، همچنین تأکید دارند که این پیشرفت می‌بایست هدفمند باشد: «شما بایستی خودتان، هدف‌های خودتان را در این دانش معیّن کنید؛ در همه‌ی بخش‌های علوم شناختی، اوّل شما هدف‌گذاری کنید تا ببینیم ما چه می‌خواهیم و دنبال چه هستیم» (بیانات، دیدار مسئولان و محققان ستاد توسعه علوم شناختی، ۱۳۹۷/۱۱/۰۳). ازاین‌رو ولی فقیه نظام اسلامی راهبرد کلانی که در حوزه پیشرفت فناوری‌های نوین ترسیم می‌کنند، هدف‌گذاری مستقل در این عرصه است.

مسئله هدفمندی فناوری هوش مصنوعی یک دغدغه بین‌المللی است. ازاین‌رو برخی اندیشمندان غربی و سازمان‌های بین‌المللی سعی دارند به‌نوعی جهت‌گیری فناوری‌ها هوش مصنوعی را به‌دست گیرند. به‌طور نمونه اخیراً یونسکو به این فکر افتاده است تا چارچوب‌های نظارتی بین‌المللی و ملی را فراهم آورد تا این فناوری نوظهور به‌طور کلی به‌نفع بشریت باشد؛ و افزون بر این در برخی مفاد این سند توصیه می‌کند که هرگونه پیشرفت هوش مصنوعی می‌بایست بر اساس ارزش‌های اخلاقی هدایت شود (https://en.unesco.org/artificial-intelligence/ethics).

البته رهبری تصریح می‌کنند غربی‌ها برای اینکه فرهنگ مدنظر خودشان را به دیگر کشورها وارد کنند ممکن است در بین شاخصه‌های توسعه و پیشرفت، مفاد فرهنگی را که جزو شاخصه‌های پیشرفت نیست، بگنجانند. افرادی که این شاخصه‌ها را تهیه می‌کنند اغلب دانشمند هستند ولی بسیاری از آنها افراد وابسته هستند. یعنی دشمن در شبکه و ناتوی فرهنگی و در مجموعه خودشان بسیار از این دانشمندان و متفکران را دارند (بیانات در دیدار دانشگاهیان سمنان، ۱۳۸۵/۰۸/۱۸)، تا به‌وسیله آنها اهداف فرهنگی و تمدنی موردنظرشان را از طریق شاخص پیشرفت به دیگران تحمیل کنند.

برای اثبات این مدعای رهبر انقلاب می‌توان شاهد مثال واقعی آورد: توصیه‌نامه یونسکو که در حوزه اخلاق هوش مصنوعی است اما در آن به‌نوعی فرهنگ فمینیستی گنجانده‌شده است. به‌طور نمونه در مقدمه این سند و در بندهای ۶ و ۸ بخش‌های 88b و 90 به اصطلاح «برابری جنسیتی»[۲] اشاره می‌کند که پیشرفت هوش مصنوعی می‌بایست در راستای ارزش‌های برابر جنسیتی باشد. در مقابل رهبر انقلاب پیش از این در بیاناتی -در بحث کرامت زنان- به استعمال این واژه از سوی برخی در داخل کشور واکنش نشان داده و استفاده از این واژه را نکوهش و نقد کرده است. زیرا به باور معظم له، افرادی که در غرب به‌دنبال برابر جنسیتی بودند، امروزه دچار فسادهای گریبان‌گیری شده‌اند و نمی‌توانند از آن رهایی پیدا کنند (بیانات، دیدار با مداحان، ۱۳۹۵/۱۲/۲۹). از این رو برنامه پیشرفت هوش مصنوعی در نظام اسلامی می‌بایست در حوزه زنان بنا بر فرهنگ و مبانی دین اسلام و در راستای کرامت زنان تهیه و تنظیم شود.

افزون براین از سوی برخی محققان، نگرانی‌های اخلاقی، حقوقی، امنیتی، سلامت و درمان، و اشتغال درباره اعتماد به هوش مصنوعی مطرح‌شده است که ضرورت کنترل و هدایت این نوع فناوری را نمایان می‌سازد. زیرا ممکن است حجم وسیعی از داده‌ها از ناحیه هوش مصنوعی دست‌کاری شود. در این صورت این امر می‌تواند در یادگیری ماشینی و نحوی ارتباط فرد با دیگران تأثیر بگذارد. یعنی هوش مصنوعی می‌تواند در چگونگی فکر و استدلال ما به‌عنوان اشخاص انسانی تأثیر بگذارد (Boddington, 2017: pp.

[2] Gender equality

(3-2. بنابراین نگرانی‌های بسیار مهم حقوقی و اخلاقی از ناحیه هوش مصنوعی متوجه انسان است. ازاین‌رو برای جلوگیری از عملی شدن این موارد می‌بایست پیشرفت فناوری هوش مصنوعی هدفمند و محدود به یک سری بایدها و نبایدهای اخلاقی و حقوقی باشد.

همچنین در بسیاری از مراکز دانشگاهی و تحقیقاتی جهان ابتکارات زیادی درزمینه‌ی اخلاقی، اجتماعی و جنبه‌های حقوقی هوش مصنوعی در حال انجام است؛ از جمله این مراکز اختصاصی، Leverhulme مرکز آینده اطلاعات در کمبریج است. مأموریت آنها در مرکز اطلاعات آینده لوورهولم (CFI) ایجاد یک جامعه‌ی بین‌رشته‌ای جدید از محققان است که ارتباط‌های قوی بین فناوران و سیاست‌گذاران داشته باشند. همچنین هدف اصلی آنها این است که بهترین فرصت‌های هوش مصنوعی در طول قراردادهای آینده را فراهم آورند (http://lcfi.ac.uk). مطالعه صدساله هوش مصنوعی (AI100) در دانشگاه استنفورد، پژوهش بلندمدت دیگری است که هدف آن مطالعه و پیش‌بینی چگونگی تأثیرات هوش مصنوعی در تمام جنبه‌های نحوه کار، زندگی و بازی افراد است (https://ai100.stanford.edu).

این پروژه‌ها نشان می‌دهد محققان از مشکلات احتمالی هوش مصنوعی آگاه هستند. همچنین تحقیقاتی تحت عنوان هوش مصنوعی باز (OpenAI) سعی دارند کدهای متن‌باز را ارائه دهند. آن‌ها بر این باور هستند که این راه بهترین شیوه برای مبارزه با خطرات مخرب هوش مصنوعی است (http://open.ai). محققان هوش ماشینی مؤسسه (MIRI) هدف خود را «همسوسازی هوش مصنوعی پیشرفته با منافع انسانی» عنوان می‌کنند (https://intelligence.org). شرکت‌های بزرگ و کوچک‌تر نیز ابتکاراتی دارند، مانند مشارکت در هوش مصنوعی به نفع مردم و جامعه، با همکاری آمازون، دیپ‌مایند، فیس‌بوک، گوگل، آی. بی. ام و مایکروسافت (https://www.partnershiponai.org). همچنین برخی افراد تحقیقاتی مانند پژوهش در زمینه‌ی بررسی سوگیری در هوش مصنوعی را دنبال می‌کنند (Boddington, 2017: p. 3).

اما به‌طور کلی در نگرش رهبر انقلاب خروجی علم بدون جهت‌گیری صحیح، استعمار است. علم اگر جهت‌گیری صحیح نداشته باشد، منجر می‌شود که فناوری بمب اتم از آن تولید شود. از منظر رهبری می‌بایست ما مراقبت کنیم که علم ما به این سمت حرکت نکند؛ و این مراقبت آن است که جهت‌گیری علم را خودمان هدایت کنم (بیانات در دیدار رؤسای دانشگاه‌ها، پژوهشگاه‌ها، مراکز رشد و پارک‌های علم و فناوری، ۱۳۹۴/۰۸/۲۰).

بنا بر نگرش رهبری ذات تکنولوژی –همانند فناوری هسته‌ای، نانو، یا صنایع الکترونیک و آیرودینامیک– بد نیست. بلکه بدی و خوبی به نحوه استفاده از آن برمی‌گردد. اگر افرادی از این نوع فناوری‌ها برای آسیب زدن به انسان‌ها، زورگویی، تسلط به دیگران، ظلم و پایمال کردن حقوق دیگران استفاده کنند، در این صورت بدی به استفاده‌کنندگان برمی‌گردد. اما اگر افرادی از این ابزارها با مبانی الهی، در جهت کرامت انسانی، عدم ظلم، در جهت اهداف ضد استکبار استفاده کنند و ارزش‌های الهی را ترویج دهند، در این صورت ابزارها خوب هستند (بیانات در دیدار نخبگان جوان دانشگاهی، ۱۳۸۷/۰۶/۰۵). به بیان دیگر، در جهت‌گیری و اهداف، استفاده انسان‌هاست که به فناوری ارزش می‌دهد. از منظر ایشان می‌بایست جهت‌گیری‌ها در استفاده از فناوری، درست و مبتنی بر ارزش‌های الهی باشد.

بنابراین علم دو جنبه دارد. علم می‌تواند در خدمت ارزش‌ها قرار بگیرد و یا می‌تواند در خدمت اهداف

حیوانی قرار بگیرد. بستگی دارد که مدیریت علم دست چه کسانی باشد. اگر علم در دست انسان‌های دنیاطلب و سلطه‌طلب باشد، -همان‌طور که امروز در دنیا مشاهده می‌شود- علمی ابزاری برای استعمار، استثمار، تحقیر ملت‌ها و ترویج فحشا و مواد مخدر است؛ ولی اگر مدیریت علم در دست انسان‌های صالح باشد، به دیگران زیان نمی‌رساند. اگر کسی که انرژی هسته‌ای را کشف کرد اهل تقوا بود، و اگر کسانی که آن را به کار گرفتند اهل فضیلت بودند، هرگز حادثه هیروشیما پیش نمی‌آمد. بنابراین از منظر رهبری ادعای برخی در سکولاریزه‌سازی علم، یک مغالطه و فریب بسیار بزرگ است. ازاین‌رو ارزش‌ها در علم دخیل هستند. بنا بر نگرش آیت‌الله خامنه‌ای، آموزه‌های اسلامی با ارزش‌های حیوانی، با فساد و سوءاستفاده از علم مشکل دارد، نه با دانش، تحقیق و فناوری. ازاین‌رو معنویت همراه با علم می‌تواند نتایج دانش و پژوهش را در جهت معنویت حرکت دهد (بیانات در دیدار جمعی از مسئولان جهاد دانشگاهی، ۱۳۸۳/۰۴/۰۱). همچنین معظم له در عبارت دیگری تأکید می‌کند دانشگاه می‌بایست علم و دانش و تحصیل علم را در جهت ارزش‌های اسلامی و اخلاقی قرار دهد. ازاین‌رو دانشگاه در جهت‌گذاری ارزشی علم می‌بایست از حوزه علمیه و علوم دینی استفاده کند (بیانات در دیدار طلّاب و دانشجویان، ۱۳۷۳/۰۹/۲۷).

به تحلیل دیگر از منظر مقام رهبری پیشرفت فناوری هوش مصنوعی می‌بایست، پیشرفت در جهت ارزش‌های اسلامی باشد و این نوع پیشرفت صحیح است. همچنین پیشرفت صحیح و در راستای ایران اسلامی لوازمی دارد. لازمه اول پیشرفت، بحث نظری است (بیانات در دیدار دانشگاهیان سمنان، ۱۳۸۵/۰۸/۱۸). در بیان دیگری ایشان تصریح می‌کنند: «ما احتیاج داریم به فکر، احتیاج داریم به فلسفه، تا بتوانیم علم را، فناوری را، مدیریت کشور را، مسائل گوناگون جامعه را به پیش ببریم و حل کنیم. فکر قبل از علم مورد نیاز است» (بیانات در دیدار جمعی از اساتید دانشگاه‌ها، ۱۳۹۰/۰۶/۰۲).

همچنین لازمه دیگر پیشرفت آن است که پیش از اینکه در فناوری نوین و پیچیده‌ای همچون هوش مصنوعی پیشرفت کنیم، می‌بایست معیار و الگوی پیشرفت آن مشخص شود (بیانات در دیدار دانشگاهیان سمنان، ۱۳۸۵/۰۸/۱۸). مسئله الگوی اسلامی-ایرانی پیشرفت از نکات مهمی است که رهبری در بسیاری از بیاناتشان بر روی آن تأکید کرده‌اند. این نکته نیز مؤید مهمی بر همین هدفمندی پیشرفت فناوری هوش مصنوعی است که در اینجا بیش از این مجال پرداختن بدان نیست.

بنابراین نمی‌بایست در بحث فناوری هوش مصنوعی همین‌طور بدون جهت‌گیری و هدف‌گذاری حرکت کرد؛ بلکه می‌بایست در راستای ارزش‌ها و اصول اسلام هدف‌گذاری صورت گیرد. افزون براین، بنا بر نگرش رهبری درباره اصل هدفمندی و جهت‌گیری صحیح و تعیین الگوی پیشرفت و بنا بر نیازمندی فناوری به مباحث فکری و فلسفه، ضرورت و اهمیت تحقیق حاضر در رویکرد نظری به حوزه هوش مصنوعی نیز مشخص می‌شود.

۳.۴ اصل توحید

تا بدین‌جا مشخص شد که از منظر رهبری می‌بایست در حوزه هوش مصنوعی پیشرفت کرد این پیشرفت می‌بایست هدفمند و جهت‌دار باشد. اما هدف و جهت اصلی فناوری این است که می‌بایست بر محور اصل مهم دین اسلام یعنی توحید باشد.

در همین راستا مقام معظم رهبری در تبیین الگوی اسلامی ایرانی پیشرفت تأکید می‌کند که اولین چیزی که در محتوای اسلامی پیشرفت می‌بایست موردتوجه قرار گیرد، مسئله توحید و مبدأ است: «انّا لله و انّا الیه راجعون». مهم‌ترین مشکل دنیای غرب جدایی از خدا و اعتقاد به خدا است. اگر مسئله مبدأ حل شود بسیاری از مسائل حل خواهد گشت. وقتی انسان به‌گونه‌ای به توحید معتقد باشد و این اعتقاد را در زندگی خود بسط دهد، مشکل اساسی بشریت حل خواهد شد (بیانات در نخستین نشست اندیشه‌های راهبردی، ۱۳۸۹/۰۹/۱۰).

افزون بر این، مقام معظم رهبری مفهومی کاربردی از توحید ارائه می‌دهند. توحید تنها به‌معنای اعتقاد به اینکه خدا یکی است و دوتا نیست، نمی‌باشد. توحید پایه یا زمینه اساسی یک جهان‌بینی است که زندگی را می‌سازد. عقیده به توحید یعنی جامعه توحیدی به وجود آید، جامعه‌ای که بر مبنای توحید شکل بگیرد و اداره بشود. اگر توحید بدین معنا نبود دشمنی با انبیا به وجود نمی‌آمد. انبیا شکل جامعه را مورد اعتراض قرار دادند. یک شکل جدید و هندسه جدیدی برای شیوه زندگی بشر ارائه کردند. آن شکل جدید همان حیات طیبه است. حیات طیبه یعنی زندگی با ایمان. از سوی دیگر، زندگی به امکانات مادی، به علم و به فناوری احتیاج دارد. منتها اگر چنانچه این‌ها بدون ایمان شد، این حیات نیست، مرده است. حیات آن‌وقتی است که تحرکات زندگی و عوامل زندگی و فناوری با ایمان همراه بشود و نور پیدا کند (بیانات در دیدار طلاب حوزه‌های علمیه استان تهران، ۱۳۹۶/۰۶/۰۶). ازاین‌رو اصل توحید می‌تواند در جهت‌گیری و پیشرفت هدفمند فناوری تأثیر بگذارد.

همچنین وی تأکید می‌کند می‌بایست پیشرفت‌های علوم شناختی و هوش مصنوعی بر محور توحید بوده و انسان‌ها را به خداوند نزدیک کند: «حواستان باشد جوری حرکت بکنید، با مبنائی حرکت بکنید که ... آشنایی با این علوم [شناختی] و وارد شدن در این عرصه ما را با خدا بیشتر آشنا کند، جوانهای ما را با توحید و با معرفت الهی بیشتر آشنا کند؛ سعی‌تان این باشد» (بیانات، دیدار مسئولان و محققان ستاد توسعه علوم شناختی، ۱۳۹۷/۱۱/۰۳). اما پیشرفت در برخی فناوری‌های نوین و هوش مصنوعی می‌تواند مخالف مباحث توحیدی و الهی باشد. در ادامه جهت روشن شدن تأثیر نگرش هدفمند توحیدی، به برخی نمونه‌های غیرتوحیدی و الهی اشاره می‌شود.

بلی ویتبای یکی از محققان هوش مصنوعی تصریح می‌کند در حال حاضر تقاضا برای «دوست‌دخترهای مجازی» بسیار زیاد است. آن‌ها شخصیت‌های رایانه‌ای هستند که می‌توانند برخی نقش‌های یک همدم خانم را بازی کنند. -بیشترین تقاضا در میان مردان ژاپنی وجود دارد-. ترکیب فناوری‌های موجود، امکان ایجاد همدم‌های مصنوعی تقریباً واقعی در آینده نزدیک را فراهم کرده است. پیش‌بینی می‌شود با ترکیب توان هالیوود برای تولید تصویرهایی کاملاً شبیه انسان با توان هوش مصنوعی خودکار و نیمه‌خودکارسازی عامل‌ها به تحولات جالبی منجر شود. یکی از صنایعی که می‌تواند بستر این تحولات باشد، صنعت سرگرمی جنسی است. این حوزه یکی از جاها و احتمالاً تنها جایی است که بازسازی حساب‌شده ویژگی انسانی موردپژوهش است. ازاین‌رو کاربردهای زیادی برای هوش مصنوعی متصور است (ویتبای، ۱۴۰۱، صص ۱۱۲-۱۱۳). نمونه افراطی از این نوع رابطه احساسی را می‌توان در برخی فیلم‌های غربی یافت. فیلم «هر» (Her) محصول ۲۰۱۳ درباره رابطه عاطفی بین یک مرد و یک سیستم عامل ساخته‌شده است. این فیلم به‌طور واضح عاشق شدن

یک انسان به هوش مصنوعی را به تصویر کشیده است (https://www.aparat.com/v/TPU4n).

ازاین‌رو برخی محققان هوش مصنوعی برای رونق صنعت هوش مصنوعی توصیه می‌کنند که می‌بایست این فناوری در صنعت هالیوود و در زندگی واقعی با صنعت جنسی آمیخته شود. در این صورت فناوری هوش مصنوعی می‌تواند بازار گسترده و سود فراوان داشته باشد. هوش مصنوعی می‌تواند به روش‌های گوناگون وارد این صنعت شود. یعنی ترکیب فناوری هوش مصنوعی با توان تولید شخصیت‌های مصنوعی با نمود کاملاً واقعی، فرصتی است که صنعت جنسی از دست نخواهد داد. ویتبای بیان می‌کند به‌راحتی می‌توان واکنش لحظه‌ای و احساسی به این مسئله نشان داد. ولی این مسئله ترکیبی از فناوری‌های توسعه‌یافته و گرایش‌های اجتماعی موجود است (ویتبای، ۱۴۰۱، ص ۱۱۳).

اما بنا بر نگرش مقام معظم رهبری پیشرفت فناوری می‌بایست بر محور توحید و معارف الهی و آموزه‌های اسلام باشد و این فناوری موجب گمراهی جوان‌ها نشود.

۵ نتیجه‌گیری و جمع‌بندی

امروزه مسئله فناوری‌های نوین همچون هوش مصنوعی، همه جنبه‌های زندگی جوامع بشری را تحت تأثیر خود قرار داده و در اداره جامعه نقش بسزایی خواهد داشت. ازاین‌رو رهبر حکیم به دلیل اهمیت این موضوع به ضرورت پیشرفت در زمینه‌ی هوش مصنوعی تأکید کرده‌اند. اما ممکن است برخی از ظاهر عبارت ایشان در باب ضرورت پیشرفت هوش مصنوعی این‌گونه برداشت کنند که دیدگاه رهبری پیشرفت در حوزه هوش مصنوعی به‌طور مطلق است.

به بیان دیگر، به‌طور کلی دو رویکرد بین مهندسان و فلاسفه و اندیشمندان نسبت به مقوله هوش مصنوعی وجود دارد. یک رویکرد، نگرش مهندسی-ابزاری به سامانه‌های هوش مصنوعی است که در این نگرش جنبه‌های فنی مهندسی و ابزارگونه آن بیشتر مورد توجه است. رویکرد دیگر، رویکرد نظری، فلسفی، علوم انسانی و تمدنی به مسئله هوش مصنوعی است. در رویکرد مهندسی نگرش خوش‌بینانه به این فناوری وجود دارد، هرچند ممکن است به برخی مضرات و خطرات آن نیز اشاره شود، ولی بیشتر منافع این فناوری موردتوجه است. اما در رویکرد فلسفی و تمدنی با اعتراف به اینکه منافع و مزایایی از ناحیه هوش مصنوعی برای جوامع وجود دارد، تأکید می‌شود که خطرات مهمی نیز از این ناحیه متوجه انسان‌هاست. برای جلوگیری از خطرات و چالش‌های فرهنگی، دینی، اخلاقی، امنیتی و اقتصادی، می‌بایست پیشرفت هوش مصنوعی هدفمند بوده و جهت‌گیری صحیحی داشته باشد. ازاین‌رو در نگرش واقعی مقام رهبری همان‌طور که ضرورت پیشرفت مورد تأکید است، هدفمندی و جهت‌گیری صحیح این نوع فناوری‌ها نیز مورد اهتمام است. جهت‌گیری صحیح آن است که این نوع فناوری در راستای توحید و معارف الهی منجر به هدایت افراد جامعه شود.

هدف مهم تحقیق حاضر بیان این نکته بود که مسئله هوش مصنوعی یک فناوری صرف نبوده، بلکه می‌تواند تأثیرات مهم فرهنگی، دینی، تمدنی و حکمرانی داشته باشد. ازاین‌رو، پیشرفت این نوع فناوری در نظام و تمدن اسلامی می‌بایست هدفمند و بر محور توحید باشد. افزون بر این از منظر رهبری پیشرفت هر نوع علم و فناوری مبتنی بر مباحث فکری و فلسفی است. از این رو در ایران اسلامی نیز می‌بایست محققان در

مراکز علمی، دانشگاهی و تحقیقاتی پیش از تولید فناوری‌های نوین و هوش مصنوعی درزمینه مسائل نظری، تمدنی، فلسفی و بنیادین آن پژوهش کرده و پیشرفت فناوری مبتنی براین نوع مباحث فکری و بنیادین باشد.

درنتیجه با تبیین این مسئله بسیاری از ابهامات برای مسئولان و قانون‌گذاران و محققان در مواجهه با پیشرفت هوش مصنوعی برطرف خواهد شد. همچنین با تبیین این نگرش، پژوهشگران، معیار، شاخصه‌ها و اصول مهمی در بررسی اسناد بین‌المللی (همچون قانون جامع هوش مصنوعی اتحادیه اروپا و سند اخلاقی هوش مصنوعی یونسکو) و یا تنظیم و تصویب و اجرای آن در کشور، خواهند داشت. بنابراین در ضمن تبیین نگرش واقعی رهبری در حوزه هوش مصنوعی، هم ضرورت ورود عالمان دینی، فلاسفه و اندیشمندان علوم انسانی به حوزه هوش مصنوعی تبیین شد؛ و هم اهمیت تحقیق در حوزه هوش مصنوعی با رویکرد نظری، فلسفی، تحلیلی و انتقادی نمایان گشت. ازاین‌رو محققان می‌توانند با رویکرد نظری و فلسفی و علوم انسانی در هدفمندی صحیح و پیشرفت فناوری هوش مصنوعی بر محور توحید نقش‌آفرینی کنند. در این صورت زمینه ایجاد فناوری هوش مصنوعی بر اساس مبانی و اصول اسلامی فراهم خواهد شد. درنتیجه با توجه به مبانی پیشرفت از منظر رهبری می‌توان امید این را داشت که پیشرفت هوش مصنوعی در راستای تمدن اسلامی و بر محور توحید و هدایت انسان‌ها خواهد بود. البته اصول و مبانی مهم دیگری نیز در اندیشه رهبری در راستای پیشرفت فناوری نوین و هوش مصنوعی همچون عدالت، استقلال و عدم وابستگی (با راهکار مراحل سه‌گانه پیشرفت فناوری)، حکمرانی و کنترل مستقل فناوری و پیشرفت مبتنی بر فرهنگ، دین و ایمان و در راستای کمال و سعادت انسان‌ها یافت می‌شود. تبیین و واکاوی این مبانی نیازمند به پژوهش مفصل و مستقل است. اما در این مقاله بنا بر اندیشه مقام معظم رهبری سه اصل مهم ضرورت پیشرفت، هدفمندی و توحید محوری در حوزه فناوری هوش مصنوعی تبیین و تثبیت شد.

مراجع

[۱] قرآن کریم.

[۲] تاجریان، علیرضا. «نقشه راه رهبری برای تولید علم و فناوری، توسعه و پیشرفت»، راهبرد یاس، شماره ۲۰، زمستان ۱۳۸۸.

[۳] سهرابی مقدم چافجیری، ایمان، و اکبرنژاد دموچالی، حسین. «نقش هوش مصنوعی در فرهنگ نوین تمدن اسلامی»، جستارنامه فرهنگ و هنر اسلامی، دوره اول، شماره دوم، پائیز ۱۴۰۱.

[۴] شورای عالی انقلاب فرهنگی. منشور انقلاب اسلامی (۱)، علم و فناوری، اسفند ۱۳۸۹.

[۵] قاسمی، حاکم، و نصیرلو، سودابه. «فناوری‌های نوظهور و تأثیر آنها بر تمدن نوین اسلامی»، مطالعات بنیادین تمدن نوین اسلامی، دوره ۴، شماره ۱، بهار و تابستان ۱۴۰۰. ص ۱-۴۰.

[۶] قربانی، سعید. «علم و فناوری دفاعی از دیدگاه امام خامنه‌ای»، تهران، یاران شاهد، ۱۳۹۲.

[۷] کیسینجر، هنری، و همکاران. «عصر هوش مصنوعی و آینده بشریت»، ترجمه رحمن قهرمان پور، تهران، روزنه، ۱۴۰۱.

[۸] مؤسسه فرهنگی حدیث لو و قلم. «روشنای علم: مروری بر بیانات حضرت آیت‌الله العظمی خامنه‌ای (مدظله‌العالی) رهبر معظم انقلاب پیرامون دانش و تولید علم»، تهران، انقلاب اسلامی، ۱۳۹۰.

[۹] ویتبای، بلی. «هوش مصنوعی به زبان ساده»، ترجمه حسین مجدفر، و آوا بهرامی، چ ۳، تهران، سبزان، ۱۴۰۱.

[۱۰] پایگاه اطلاع‌رسانی دفتر حفظ و نشر آثار حضرت آیت‌الله‌العظمی سیدعلی خامنه‌ای (مدظله‌العالی). http://www.khamenei.ir

[۱۱] وب‌سایت مرکز الگوی ایرانی اسلامی پیشرفت. https://www.olgou.ir

[12] Boddington, Paula. “Towards a Code of Ethics for Artificial Intelligence”, Springer International Publishing, 2017.

[13] Russell, S., & Norvig, P. “Artificial Intelligence: A Modern Approach”, 4th Ed., Prentice Hall, 2020.

[14] UNESCO. “Recommendation on the ethics of artificial intelligence”, 2021, URL: https://en.unesco.org/artificial-intelligence/ethics, retrieved: 2022 Feb. 6.

سایبودینامیک، قوانین جریان اطلاعات در چرخه‌ی سایبرنتیک

محمدعلی شکوهیان‌راد[۱]، سمانه کاتبی کوشالی[۲]

[۱]مدرس دانشگاه تهران و پژوهشگر ارشد آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
cm@shokoohian.ir
[۲]دانش‌آموخته‌ی دکتری شیمی - فیزیک، دانشگاه کاشان
sahab135@gmail.com

چکیده

تلقی انسان از جهان و ارکان سازنده‌ی آن در طول تاریخ، چنین بوده که صرفاً ماده و انرژی سازندگان پایه‌ی جهان هستند. لذا دانش‌هایی که بتوانند ماهیت، کارکرد، قوانین حاکم و نحوه‌ی کنترل ماده و انرژی را توضیح دهند، برای فهم جهان کفایت می‌کنند. اما عصر اطلاعات که با وقوع انقلاب صنعتی سوم آغاز شد، فضای فهم و ادراک از جهان را به‌سمت مؤلفه‌ی نوینی سوق داد که در گذر زمان اثبات شد حتی ماده و انرژی نیز تحت سیطره‌ی آن هستند: اطلاعات. همچنین به‌دلیل استیلای اطلاعات بر ماده و انرژی، دانش سایبرنتیک –دانش تخصصی کنترل جریان اطلاعات– نیز بر دانش فیزیک سلطه دارد. به‌تدریج مشخص گردید اطلاعات در حالی که می‌تواند ماده و انرژی را کنترل نماید، به‌دلیل ماهیت متفاوتی که دارد از قوانین حاکم بر ماده و انرژی پیروی نمی‌کند. این مهم آغاز یکی از بزرگترین انقلاب‌های علمی جهان شد که مبنای اکثر دانش‌ها را از ماده و انرژی به اطلاعات تغییر داد؛ تغییری که بر پایه‌ی دانش سایبرنتیک رقم خورد و کماکان ادامه دارد. از سوی دیگر، ثبات‌مندی و پایداری بسیار بالای جریان اطلاعات حاکی از قانون‌مندی روند آن است. بدین سبب جریان‌مندی اطلاعات، قطعاً از قوانین مشخصی پیروی می‌کند؛ قوانینی که در دانش فیزیک مطالعه نشده و باید کشف شوند. در این راستا، طی نسبت‌شناسی میان مؤلفه‌ی گرما در پویایی ماده و انرژی که قوانین ترمودینامیک بر پایه‌ی آن تدوین شده، با مؤلفه‌ی سایبر که جریان اطلاعات را در چرخه‌ی سایبرنتیک ایجاد و کنترل می‌نماید، برای نخستین بار «قوانین پویایی جریان اطلاعات» با عنوان سایبودینامیک مورد مطالعه قرار گرفت.

کلمات کلیدی: سایبرنتیک؛ سایبودینامیک؛ قوانین جریان اطلاعات؛ مثلث اطلاعات، ماده و انرژی (مثلث اِما).

۱ مقدمه

دانش سایبرنتیک، دانشی است که اساساً بر مؤلفه‌ی اطلاعات تمرکز دارد؛ به همین دلیل است که به‌عنوان دانش اعمال کنترل از طریق جریان اطلاعات شناخته می‌شود. از سوی دیگر، موضوع کنترل، مقوله‌ای است

که به‌دلیل ماهیت کشف و اصلاح خطا، خودش باید فاقد هرگونه خطا باشد. به‌همین دلیل است که حوزه‌ی کنترل، حوزه‌ای است که نیازمند ثبات و پایداری است و از هر عاملی که برهم‌زننده‌ی پیش‌بینی‌پذیری است حذر دارد. به‌عبارت دیگر زمانی می‌توان به درستی اعمال کرد و خطاهای احتمالی را در هر فرایند مدنظر، کشف و اصلاح نمود که خود ساز و کار کنترلی دچار خطا و عدم پایداری نباشد.

بنابر این دانش سایبرنتیک، در حوزه‌ی کنترل از طریق جریان اطلاعات از ثبات و پایداری بسیار بالایی برخوردار است، تا آنجا که در زمره‌ی معدود دانش‌هایی است که مبانی فلسفی و نظری آنها طی حدود دو قرن گذشته، مردود اعلام نشده، بلکه بر همان مسیر اولیه تکمیل گردیده است. این ثبات و پایداری درونی دانش سایبرنتیک، قطعاً حاصل استوار شدن این دانش بر قوانینی است که در نسبت با عالم، همسو و منطبق هستند. به‌عبارت دیگر اگر صحبت از کنترل بر اساس جریان اطلاعات می‌شود، ثبات آن بابت ثباتی است که جریان اطلاعات از آن برخوردار است. از این رو می‌توان اذعان داشت جریان‌مندی اطلاعات از قوانین مشخصی پیروی می‌کند.

اما آیا قوانین اطلاعات، استخراج شده است؟ آیا قوانین حاکم بر اطلاعات، همان قوانین حاکم بر ماده و انرژی است که دانش فیزیک مطرح می‌کند؟ چه نسبتی میان قوانین حاکم بر جریان اطلاعات با قوانین حاکم بر جریان ماده و انرژی برقرار است؟ نوآوری پژوهش حاضر از آن جنبه است که نخستین متن علمی در زبان فارسی است که تلاش دارد بخشی از قوانین جریان اطلاعات را الگو نموده و تشریح کند.

بدین منظور، پژوهش حاضر ابتدا ماده و انرژی و قوانین حاکم بر جریان‌مندی آن را طبق دانش فیزیک بررسی کرده و سپس در نسبت با آن به معرفی جریان اطلاعات، نسبت جریان اطلاعات به جریان ماده و انرژی و نهایتاً تدوین و تشریح بخشی از قوانین حاکم بر جریان اطلاعات می‌پردازد.

۲ پیشینه‌ی پژوهش

بر اساس مطالعات انجام شده، نخستین فردی که پیرامون قانون‌مندی و نظریه‌پذیری اطلاعات صحبت کرده، یک فیزیک‌دان اروپایی به نام لئو زیلارد است. زیلارد مقاله‌ای در مورد شیطان ماکسول با عنوان «درباره‌ی کاهش آنتروپی در یک سیستم ترمودینامیکی با مداخله‌ی موجودات هوشمند» نوشته است. وی دیدگاهی را معرفی کرد که اکنون موتور زیلارد نامیده می‌شود و در تاریخچه‌ی دانش برای درک شیطان ماکسول مهم تلقی شد. این مقاله همچنین اولین معادله‌ی آنتروپی منفی و اطلاعات را ارائه کرده است (لئو زیلارد، ۱۹۲۹). به این ترتیب، زیلارد را می‌توان به‌عنوان یکی از بنیانگذاران نظریه‌ی اطلاعات معرفی کرد.

دومین مطالعات مهم در باب قانون‌پذیری اطلاعات توسط لئون بریلوئین[1] –فیزیک‌دان فرانسوی– انجام شده است. وی از اولین کسانی است که تلاش نموده از طریق جریان اطلاعات و قوانین حاکم بر آن، مسائل فیزیکی را بررسی نماید. بریلوئین از نظریه‌پردازانی است که تلاش داشته تا بتواند از منظر مباحث فیزیکی، با کنترل جریان اطلاعات در محیط و ایجاد آنتروپی منفی، بر مسأله‌ی آنتروپی که به افول و زوال تدریجی سیستم‌ها اشاره دارد، غلبه نماید. وی در خصوص سایبرنتیک اعتقاد دارد «ما با تلقی اطلاعات به‌صورت مجزا

[1] Léon Nicolas Brillouin

[تا پیش از سایبرنتیک]، راه نادرستی را انتخاب کرده‌ایم. ضروری است که همیشه این دو را به‌صورت مجموعه بررسی کنیم، یعنی اطلاعات به‌علاوه‌ی آنتروپی منفی» (کلاود شانون، ۱۹۴۸).

بریلوئین در یکی از مهم‌ترین آثار خود پیرامون سایبرنتیک با عنوان «زندگی، ترمودیناک و سایبرنتیک»، نظر خود درباره‌ی نگاه وینر به موضوع ایجاد آنتروپی منفی از طریق جریان اطلاعات را چنین بیان می‌نماید: «اگر اطلاعات به‌معنای آنتروپی منفی است» –همانطور که وینر پیشنهاد کرده است– چگونه می‌خواهیم این متغیر و مداخله‌گر جدید را در آنتروپی اندازه‌گیری کنیم؟ وینر تعاریف عملی و عددی را پیشنهاد می‌کند که ممکن است برای ساده‌ترین مسائل ممکن از این نوع به کار رود. این یک میدان کاملاً جدید برای تحقیق و یک ایده‌ی تحول‌آفرین را نشان می‌دهد» (لئون بریلوئین، ۱۹۴۹).

بریلوئین در کتاب «دانش و نظریه‌ی اطلاعات»[۲] که در سال ۱۹۵۶ میلادی منتشر شد، با مبحث کنترل محیط از طریق کنترل جریان اطلاعات به‌واسطه‌ی ایجاد آنتروپی منفی، تعیین تکلیف نموده و آن را کاملاً واقعی و ممکن دانسته است. وی در این کتاب، برای بیان آنتروپی منفی از طریق اطلاعات، اصطلاح «نِگِنتروپی»[۳] را مطرح می‌کند[۴] که ابتناء بر اصلی دارد که خودش پایه‌گذاری نموده است: «اصل نگنتروپی اطلاعات»[۵] که سه سال پیش از این (۱۹۵۳ میلادی) در مقاله‌ای با همین عنوان آن را تشریح کرده است (لئون بریلوئین، ۱۹۵۳). این فیزیک‌دان رابطه‌ی میان آنتروپی منفی و اطلاعات را چنین تشریح کرده است: «آنتروپی معمولاً به‌عنوان اندازه‌گیری میزان بی‌نظمی در یک سیستم فیزیکی توصیف می‌شود. به بیانی دقیق‌تر، آنتروپی میزان خلأ اطلاعات در مورد ساختار واقعی سیستم را اندازه‌گیری می‌کند. این فقدان اطلاعات، امکان وجود تنوع زیادی از ساختارهای متمایز میکروسکوپی را مطرح می‌کند که ما در عمل قادر به تشخیص آنها از یکدیگر نیستیم. از آنجایی که هر یک از این ریزساختارهای مختلف واقعاً در هر زمان معیّن قابل تحقق است، فقدان اطلاعات مربوط به بی‌نظمی واقعی در درجات پنهان آزادی است» (لئون بریلوئین، دانش و نظریه‌ی اطلاعات).

از مهم‌ترین مطالعاتی که تلاش نموده قوانین اطلاعات را شناسایی و از طریق جریان‌مندی اطلاعات، آنتروپی سیستم را تحت کنترل درآورد متعلق به نوربرت وینر[۶] است که پدر دانش سایبرنتیک می‌باشد. وینر در این خصوص بیان می‌دارد: «ما در نوعی زندگی مستغرق هستیم که در آن دنیا به‌طور کلی، از اصل دوم ترمودینامیک پیروی می‌کند: درهم‌آشفتگی افزایش و نظم کاهش می‌یابد (نوربرت وینر، ۱۳۶۶). زمانی که من ساختمان یک موجود زنده را با ماشین مقایسه می‌کنم، حتی برای یک لحظه مقصودم این نیست که فرآیندهای ویژه‌ی فیزیکی، شیمیایی و روحانی زندگی، بدان معنایی که عادتاً آنها را می‌شناسیم، همانند فرآیندهایی هستند که درون ماشین‌ها روی می‌دهند. منظور من صرفاً آن است که هر دو می‌توانند در محل

---

[2] Science and Information theory

[3] Negentropy

[۴] می‌توان پیشینه‌ی اصطلاح نگنتروپی بریلوئین را در اصطلاح «آنتروپی منفی»(Negative Entropy)،که توسط اروین شرودینگر مطرح شده است، جستجو نمود اما تعاریف بریلوئین حاکی از آن است که نگنتروپی، دقیقاً همان آنتروپی منفی شرودینگر نیست و پدیده‌ی اطلاعات در آن نقش بسیار جدی یافته است.

[5] Negentropy Principle of Information

[6] Norbert Wiener

خود، نمونه‌ای از فرایندهای پادآنتروپیک باشند» (همان).

۳ ادبیات پژوهش

۱.۳ قوانین ماده و انرژی در ترمودینامیک

ماده و انرژی، دو حوزه‌ی اصلی مورد مطالعه در دانش فیزیک هستند و کلیت این دانش بر آنها تمرکز دارد، به‌گونه‌ای که هدف دانش فیزیک، کشف روابط میان ماده و انرژی و ارائه‌ی الگوی دقیق محاسباتی برای آنها است. در فیزیک کلاسیک و شیمی عمومی، ماده به هر جزء یا ماهیتی گفته می‌شود که دارای جرم است و با داشتن حجم، فضا را اشغال می‌کند (پِنروس، ۱۹۹۱). همچنین انرژی خاصیت کمی است که به یک جسم یا یک سیستم فیزیکی منتقل می‌شود و در انجام کار و به شکل گرما و نور قابل تشخیص است (پائولو بوسوتی، ۲۰۲۳).

رابطه‌ای که فیزیک میان ماده و انرژی در نظر می‌گیرد چنین است که انرژی، فعال‌کننده‌ی ماده است و همانطور که بیان شد، این فعال‌شوندگی از علائم کمّی برخوردار و قابل تشخیص است که اهم آن گرما است. به‌عبارت دیگر، انتقال انرژی به ماده به‌گونه‌ای که گرمای آن را افزایش دهد، اثر فیزیکی انرژی بر ماده است که از طریق پایش دما اندازه‌گیری می‌شود. بنابر این می‌توان گرما را مؤلفه‌ی پویایی ماده از طریق انرژی دانست. به‌همین سبب است که قوانین ماده، انرژی و ارتباطات میان آنها از طریق مؤلفه‌ی مهم دما مورد مطالعه قرار می‌گیرد.

به‌صورت مشخص، مبحثی که قوانین ماده و انرژی در نسبت با دما را در دانش فیزیک و شیمی مورد مطالعه قرار می‌دهد، ترمودینامیک است. ترمودینامیک، علم ماکروسکوپی است که ارتباط‌های خواص تعادلی یک سیستم و تغییرات آن را در خلال فرآیندها مطالعه می‌کند (ایرا لوین، ۱۳۸۶، ص۱). همانطور که بیان شد، دما خاصیت کلیدی در ترمودینامیک است که بدین سبب گاهی ترمودینامیک به‌عنوان مطالعه‌ی رابطه‌ی دما با خواص ماکروسکوپی ماده نیز تعریف می‌شود (ایرا لوین، ۱۳۸۶، ص۳). پس به‌طور کل می‌توان دانش فیزیک را دانش مطالعه‌ی ماده، انرژی و خواص و قوانین حاکم بر آنها دانست که یکی از اهم قوانین شناخته شده در مبحث ترمودینامیک مطرح شده است که مؤلفه‌ی اصلی آن دما (سنجش میزان گرما) است.

۲.۳ اطلاعات، کنترل‌کننده‌ی ماده و انرژی

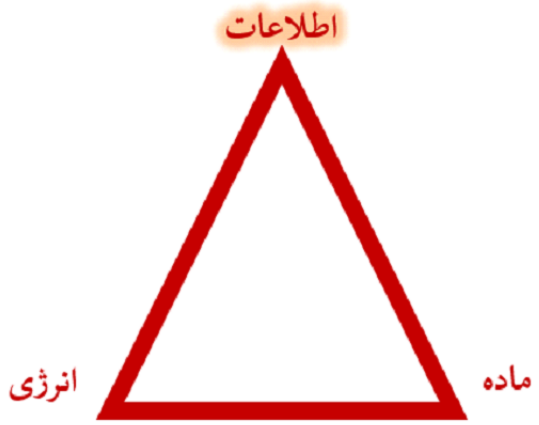
اطلاعات را می‌توان عمیق‌ترین مؤلفه‌ای دانست که تاکنون بشر به فهم و توانایی استفاده‌ی گسترده از آن دست یافته است، زیرا کاربرد اطلاعات در عصر حاضر صرفاً در راستای بهبود یا تکامل نیست، بلکه می‌تواند پدیده‌ها را از بنیان دگرگون سازد. **از این رو اطلاعات، مؤلفه‌ای است که نه فقط باعث طراحی و اجرای جدید پدیده‌ها می‌شود، بلکه سرشت ذاتی آنها یعنی هستی‌شناسی‌شان را به‌طور بنیادین تغییر می‌دهد.** بدین معنا اطلاعات، جهان ما را نه فقط بازطراحی و بازمهندسی، بلکه به واقع مجدداً هستی‌شناختی می‌کند. فضای اطلاعات به‌قدری عمیق و همه‌جا حاضر شده است که جهان امروز در اینفوسفِر قرار گرفته و این مسأله تا آنجا پیش رفته که قطع شدن ارتباط انسان‌ها –خصوصاً نسل‌های جدید– با اینفوسفِر همانند

بیرون افتادن ماهی از درون آب است.

این موضوع حتی برای دانش فیزیک نیز که تماماً در حیطه‌ی ماده و انرژی تعریف شده، مصداق یافته است؛ آنجا که بشر متوجه شد ماده و انرژی ذیل اطلاعات کار می‌کنند. به‌عبارت دیگر ماده، انرژی و قوانین حاکم بر آنها تحت تأثیر جریان اطلاعات هستند. بنابراین با کنترل جریان اطلاعات، می‌توان جریان ماده و انرژی را نیز کنترل نمود.

اگر مؤلفه‌ی اطلاعات را که یک مؤلفه‌ی سایبرنتیکی است، به دو مؤلفه فیزیکی ماده و انرژی اضافه کنیم، به‌گونه‌ای که ارجحیت اطلاعات بر ماده و انرژی لحاظ شود؛ یک مثلث شکل می‌گیرد که به **«مثلث اطلاعات، ماده و انرژی»** (به اختصار، مثلث اِما) شهرت دارد، به‌گونه‌ای که رأس فوقانی آن جایگاه اطلاعات و دو رأس تحتانی آن محل استقرار ماده و انرژی است (شکل ۱).

مبنای شکل‌گیری مثلث اِما از آنجا است که پردازش اطلاعات، به انرژی نیاز دارد تا در سطح ماده نسبتاً قابل مشاهده باشد، یعنی تجسم و فشرده‌سازی آن. عناصر اصلی مادی مانند زمین، هوا، آتش و آب... همگی از انرژی ساخته شده‌اند، اما شکل‌های مختلف آنها توسط اطلاعات تعیین می‌شود. انجام هر کاری نیاز به انرژی دارد. برای مشخص کردن آنچه انجام می‌شود نیاز به اطلاعات است. انرژی و اطلاعات ذاتاً (بدون جناس) در هم تنیده شده‌اند. بنابراین اطلاعات، ماده و انرژی در یک خود ارجاعی «درهم تنیده» در نظر گرفته می‌شود (اینّا سِمِتسکی، ۲۰۱۰).



شکل ۱: مثلث اطلاعات، ماده و انرژی (به اختصار، مثلث اِما)

هر چند در مثلث اِما، به‌علت وجود رابطه‌ی $E = mc^2$ که مبنای تبدیل ماده و انرژی به یکدیگر است، ماده و انرژی با یکدیگر هم‌طراز هستند؛ اما جایگاه اطلاعات به‌دلیل توضیحاتی که بیان شد، فرای ماده و انرژی است و ماده و انرژی تحت تأثیر اطلاعات هستند.

۳.۳ آنتروپی سایبرنتیکی، کنترل‌کننده‌ی آنتروپی فیزیکی

همانگونه که فیزیک، دانش شناخت ماهیت و روابط محاسباتی ماده و انرژی است؛ سایبرنتیک نیز دانش شناخت ماهیت و قوانین جریان‌مندی اطلاعات است. از سوی دیگر بیان شد اطلاعات، ماده و انرژی را کنترل می‌کند. از این رو دانش سایبرنتیک نیز توانایی کنترل دانش فیزیک را دارا است. اروین شرودینگر (فیزیکدان) در خصوص برتری جریان اطلاعات بر فیزیک در موجودات زنده می‌گوید: «ماده‌ی زنده، در حالی که قوانین شناخته‌شده‌ی فیزیک را نقض نمی‌کند، ممکن است تابع قوانین دیگری از فیزیک باشد که هنوز ناشناخته هستند». در این طرز فکر، شرودینگر تنها نبود و پایه‌گذاران دیگر مکانیک کوانتومی مانند نیلز بور و ورنر هایزنبرگ نیز احساس کردند که ماده‌ی زنده، نیازمند فیزیک جدیدی است (پل دیویس، ۱۳۹۹). لذا در حالی که جهان تحت تأثیر قوانین فیزیک کار می‌کند، تابع قوانین دیگری است که فیزیک بر آنها سیطره ندارد؛ قوانینی که مرتبط با حوزه‌ی جریان اطلاعات است. اما موضوع بسیار مهم این است که هنوز در هیچ دانشی، قوانین اطلاعات، پویایی اطلاعات و چرخه‌های اطلاعاتی به‌صورت جامع بررسی نشده است.

اکنون این پرسش مطرح می‌شود که منظور از قوانین اطلاعات چیست؟ مگر قوانین حاکم بر اطلاعات با قوانین حاکم بر ماده و انرژی متفاوت است؟ با یک مثال می‌توان پاسخ داد. بدیهی است که ماده و انرژی، هر چه بیشتر مصرف شوند، از مقدارشان کاسته می‌شود تا آنکه به اتمام برسند. آیا مصداقی از ماده یا انرژی سراغ دارید که در اثر مصرف، افزایش یابد؟ یعنی مصداقی از انرژی می‌شناسید که هر چه بیشتر مصرف کنیم، بیشتر شود یا نوعی از ماده که در صورت استفاده‌ی بیشتر، افزایش یابد؟ لذا کاهش مقدار در اثر مصرف شدن، یکی از قوانین حاکم بر ماده و انرژی است.

اما برخلاف ماده و انرژی، اطلاعات در اثر مصرف شدن بیشتر می‌شود. برای مثال وقتی اطلاعات موجود روی یک سیستم را در ذخیره‌ساز خود کپی می‌کنیم تا مورد استفاده قرار دهیم، عملاً با ایجاد یک نسخه‌ی همانند از نسخه‌ی اولیه، آن را دو برابر کرده‌ایم؛ آن هم با همان کیفیت و و یژگی‌های نسخه‌ی اولیه.

بنابراین قوانین حاکم بر اطلاعات متفاوت است از قوانین حاکم بر ماده و انرژی. لذا قوانینی که دانش فیزیک برای ماده و انرژی ارائه کرده است، نمی‌تواند روابط و قوانین حاکم بر اطلاعات را توضیح دهد. این در حالی است که بیان شد اطلاعات، ماده و انرژی را کنترل می‌کند. بنابر این اولاً همانگونه که دانش فیزیک، قوانین را برای ماده و انرژی توصیف کرده است؛ دانش سایبرنتیک نیز قوانین را برای اطلاعات توصیف می‌کند؛ و ثانیاً خود دانش فیزیک، تحت تأثیر دانشی است که قوانین حاکم بر اطلاعات را توضیح می‌دهد که دانش سایبرنتیک است. یک مثال دیگر برای فهم دقیق‌تر و عمیق‌تر این گزاره:

سه بسته کاغذ را در نظر بگیرید، سه بسته‌ای که از تمامی جهات فیزیکی مانند، مواد اولیه‌ی تولید، زمان تولید، شرایط نگهداری، مقدار و ... کاملاً یکسان هستند. بسته‌ی اول در واقع یک کتاب علمی صد صفحه‌ای است، بسته‌ی دوم شامل صد صفحه مجله‌ی سرگرمی است و بسته‌ی سوم حاوی صد صفحه روزنامه‌ی باطله.

پرسش این است: آیا آنتروپی این سه بسته کاغذ از منظر دانش فیزیک، با یکدیگر تفاوت دارند؟ قطعاً پاسخ شما خیر است. این بدین معنا است که در روال عادی طبیعت، آنتروپی هر سه بسته‌ی کاغذ یکسان است و همزمان و هماهنگ دچار زوال می‌شوند. حال پرسش دوم این است: زمانی که قصد مطالعه‌ی یک

متن علمی را دارید، کدام یک از کاغذها را انتخاب می‌کنید؟ کتاب علمی، مجله‌ی سرگرمی یا روزنامه‌های باطله؟ به‌طور کلان‌تر، از هر کدام از بسته کاغذهای مذکور در چه زمانی و چه اموری استفاده می‌کنید؟ تبعاً پاسخ‌تان چنین است که از کتاب حاوی متن علمی برای مطالعات علمی و کسب دانش، از مجلات سرگرمی برای سپری کردن اوقات فراغت و از روزنامه‌های باطله برای نظافت یا بسته‌بندی اشیاء استفاده می‌کنیم. اکنون پرسش مهم این است که مگر هر سه بسته‌ی کاغذهای مذکور از حیث شرایط و ویژگی‌های فیزیکی، یکسان نیستند؟ پس چرا در انتخاب کاربرد آنها نسبت به شرایط مختلف، تصمیمات مختلفی اخذ می‌کنید؟

حتماً پاسخ‌تان این است که به‌دلیل تفاوت‌شان در محتوایی که ارائه می‌کنند.

بله! تنها تفاوت میان این سه دسته کاغذ صد صفحه‌ای، اطلاعاتی است که ارائه می‌کنند. به‌عبارت دیگر، تفاوت در تصمیم‌گیریِ ما، حاصل از تفاوت در اطلاعاتِ مندرج در این سه منبع است. دقیقاً اختلاف در اطلاعات منابع است که باعث می‌شود کتاب علمی را برای مدت بسیار طولانی در کتابخانه نگه دارید و به منفی شدن آنتروپی آن کمک کنید اما روزنامه‌های باطله را حتی نه برای مطالعه، بلکه برای نظافت سطوح استفاده کنید که در واقع آنتروپی آن را سریع‌تر می‌کنید.

در مثال فوق به‌وضوح مشخص است که علی‌رغم یکسان بودن آنتروپی فیزیکیِ (آنتروپی ماده و انرژی) سه بسته کاغذ، با دخالت متغیر اطلاعات، سرنوشت متفاوتی برای آنها رقم می‌خورد. از این رو با مفهومی متفاوت و بسیار اثرگذار مواجه هستیم که**آنتروپی اطلاعات** نام دارد و از آنجا که اطلاعات و تمامی مسائل مرتبط با آن در دانش سایبرنتیک مورد مطالعه و بررسی قرار می‌گیرد، مؤلفه‌ی دیگری علاوه بر آنتروپی فیزیکی مطرح می‌شود که آن را **آنتروپی سایبرنتیکی** آنتروپی سایبرنتیکی می‌نامیم.

همچنین مثال فوق نشان داد که آنتروپی سایبرنتیکی، کاملاً بر آنتروپی فیزیکی اثرگذار است. دقیقاً به‌دلیل آنتروپی سایبرنتیکی است که از سویی، یک کتاب قدیمی که در حال پوسیدن و زوال فیزیکی است (آنتروپی فیزیکی) را با روش‌های مختلف ترمیم نموده و نگهداری می‌کنیم تا از بین نرود (آنتروپی منفی فیزیکی) زیرا اطلاعات آن ارزشمند است و باید حفظ شود؛ ولی از سوی دیگر، انبوهی از کاغذهایی که محتوای چاپ شده روی آنها باطل شده است (آنتروپی سایبرنتیکی) علی‌رغم سالم بودن خود کاغذها (آنتروپی منفی فیزیکی) به خمیر تبدیل می‌کنیم (آنتروپی فیزیکی) تا بتوان از کاغذ بازیافت شده، مجدداً برای چاپ اطلاعات و محتوای جدید استفاده نمود. **نکته‌ی بسیار مهم این است که مبتنی بر مثلث اِما، از آنجا که اطلاعات بر ماده و انرژی برتری و استیلا دارد؛ در نتیجه آنتروپی سایبرنتیکی، کنترل‌کننده‌ی آنتروپی فیزیکی است.**

۴.۳ نسبت‌شناسی قوانین سایبودینامیک با قوانین ترمودینامیک

بیان شد بخشی از دانشمندان سایبرنتیک، خصوصاً آن دسته که عموماً از منظر فیزیک و مهندسی به سایبرنتیک نگریسته‌اند؛ تزریق اطلاعات به سیستم را به‌مثابه آنتروپی منفی برای آن سیستم در نظر گرفته و بدین نحو، کارکرد کنترلی را برای جریان اطلاعات، اثبات و احراز نموده‌اند. این نگاه، در حالی که از سویی اتکا بر قوانین ترمودینامیک دارد، از سوی دیگر تعبیری مبتنی بر سایبرنتیک و پویایی اطلاعات را به‌جای دیدگاه فیزیکی ارائه می‌نماید. در پژوهش حاضر برای نخستین بار، نه فقط مفهوم آنتروپی منفی بلکه هر

جدول ۱: چهار حالت بر اساس ماتریس دو در دو

x	سیستم الف	سیستم ب
کنترل‌کننده	کنترل‌کننده سیستم الف	کنترل‌کننده سیستم ب
کنترل‌شونده	کنترل‌شونده سیستم الف	کنترل‌شونده سیستم ب

چهار قانون ترمودینامیک از منظر سایبرنتیک تشریح شده است؛ مبحثی که آن را سایبودینامیک[۷] به‌معنای «پویایی جریان اطلاعات» می‌نامیم. قوانین پویایی جریان اطلاعات (سایبودینامیک) به‌صورت ذیل بازتعریف می‌شود:

۱.۴.۳ قانون یکم سایبودینامیک: تعادل جریان اطلاعات میان سیستمی

گزاره: اگر دو سیستم با سیستم سومی در تعادل کنترلی به‌واسطه‌ی جریان اطلاعات باشند، خود آن دو سیستم نیز با یکدیگر در حالت تعادل جریان اطلاعات هستند.

اثبات: همواره شکل‌گیری کنترل سایبرنتیکی، نیازمند شکل‌گیری چرخه‌ی سایبرنتیک است. لذا حتماً از میان دو سیستم، یکی از آنها کنترل‌کننده و دیگری کنترل‌شونده است که به‌ترتیب سیستم‌های الف و ب می‌نامیم. حال سیستم سومی به چرخه‌ی سایبرنتیک اضافه می‌شود که سیستم پ نام دارد. بدیهی است که سیستم مذکور نسبت به هر کدام از دو سیستم الف و ب، یا باید نقش کنترل‌کننده داشته باشد یا کنترل‌شونده و نمی‌تواند نسبت به یک سیستم، همزمان در هر دو نقش ظاهر شود. از آنجا که دو سیستم موجود است و نسبت به هر سیستم، دو نقش قابل احراز؛ در نتیجه چهار حالت بر اساس ماتریس دو در دو شکل می‌گیرد (جدول ۱).

اگر سیستم پ، کنترل‌کننده‌ی سیستم الف باشد: از آنجا که سیستم الف نیز کنترل‌کننده‌ی سیستم ب بوده و میان آنها چرخه‌ی سایبرنتیک از قبل به‌صورت بدون نقص و پایدار برقرار شده؛ در نتیجه سیستم الف نیز در تعادل اطلاعاتی با سیستم ب است. زیرا اگر جز این باشد، از طریق جریان اطلاعات ارسالی به کنترل‌شونده‌ی خود (سیستم الف) بر عملکرد آن به‌گونه‌ای اثر خواهد گذاشت که نهایتاً سیستم الف که نقش کنترل‌کننده‌ی سیستم ب را دارا است، از تعادل با آن سیستم خارج می‌گردد. پس مادامی که سیستم الف با سیستم ب در تعادل چرخه‌ی سایبرنتیک است، به‌معنای این است که سیستم پ با سیستم الف در تعادل چرخه‌ی سایبرنتیک می‌باشد؛ در نتیجه میان سیستم پ و سیستم ب نیز **تعادل سایبوسایبرنتیک** (سایبرنتیک مرتبه‌ی دوم) وجود دارد.

اگر سیستم پ، کنترل‌کننده‌ی سیستم ب باشد: از آنجا که سیستم ب کنترل‌شونده‌ی سیستم الف است ابتدا باید مشخص شود سیستم پ با سیستم الف چه نسبتی دارد؟ اگر میان سیستم پ و سیستم الف، نسبت کنترل‌کننده – کنترل‌شونده برقرار باشد که تکرار حالت قبل است و در واقع سیستم پ از طریق

[7] Cybodynamics

سایبوسایبرنتیک بر سیستم ب کنترل دارد. اما اگر نسبت سیستم پ به سیستم الف از نوع کنترل‌شونده – کنترل‌کننده باشد، روند بدین صورت است که سیستم پ در راستای کنترل سیستم الف، سیستم ب را کنترل می‌نماید. در این حالت سیستم پ به سیستم داخلی سایبوسایبرنتیک سیستم الف تبدیل می‌شود و از آنجایی که سیستم پ از سویی با سیستم الف به‌عنوان کنترل‌کننده‌اش و از سوی دیگر با سیستم ب به‌عنوان کنترل‌شونده‌اش در تعادل چرخه‌ی سایبرنتیک است؛ در نتیجه سیستم‌های الف و ب نیز با یکدیگر در تعادل جریان اطلاعات هستند.

اگر سیستم پ، کنترل‌شونده‌ی سیستم الف باشد: در این صورت بنابر اینکه سیستم الف، سیستم ب را نیز کنترل می‌نماید، مشخصاً سیستم الف در جایگاه کنترل‌کننده‌ی مطلق قرار می‌گیرد. حال باید مشخص شود نسبت سیستم پ به سیستم ب چگونه است؟ اگر سیستم پ کنترل‌کننده‌ی سیستم ب باشد، حالت قبل رخ می‌دهد که تشریح شد. اما اگر سیستم پ کنترل‌شونده‌ی سیستم ب باشد، در این صورت سیستم الف در حال کنترل سیستم ب بوده و سیستم ب نیز سیستم پ را کنترل می‌نماید. در مجموع کنترل سایبوسایبرنتیک بدین صورت شکل می‌گیرد که سیستم ب، سیستم داخلی کنترل سایبوسایبرنتیک سیستم الف بر سیستم پ است. لذا از آنجا که سیستم ب به‌عنوان کنترل‌شونده در تعادل چرخه‌ی سایبرنتیک با سیستم الف بوده و به‌عنوان کنترل‌کننده نیز چرخه‌ی سایبرنتیک با سیستم پ دارد؛ در نتیجه سیستم‌های الف و پ با یکدیگر در تعادل جریان اطلاعات هستند.

اگر سیستم پ، کنترل‌شونده‌ی سیستم ب باشد: بنابر اینکه سیستم ب توسط سیستم الف کنترل می‌شود، دقیقاً حالت قبل واقع می‌شود. در نتیجه تعادل جریان اطلاعات میان سیستم الف و پ به‌واسطه‌ی جایگاه سیستم ب برقرار است.

۲.۴.۳ قانون دوم سایبودینامیک: توان اقدام کنترل‌شونده

گزاره: همواره میزان توان اقدام کنترل‌شونده نسبت به کنترل‌کننده، برابر است با اختلاف میزان اقدام انجام شده و میزان اطلاعات دریافتی از کنترل‌کننده.

اثبات: در چرخه‌ی سایبرنتیک، کنترل‌شونده از سمتی، اطلاعات را از کنترل‌کننده دریافت می‌کند و از سمت دیگر، اقدام متناظر با اطلاعات دریافتی را انجام می‌دهد که این اقدام، به‌صورت کنش بر محیط ظاهر می‌شود. از سوی دیگر بیان شد که میزان کیفی و کمّی اقدام کنترل‌شونده، اولاً به توان محاسباتی آن وابسته است که کاملاً درونی است و هیچ راهی برای کنترل‌کننده نسبت به اطلاع مستقیم از آن وجود ندارد، مگر رصد محیط و تغییراتی که در آن بر حسب اقدام کنترل‌شونده حاصل می‌گردد. ثانیاً به میزان انرژی دریافتی کنترل‌شونده از محیط باز می‌گردد. برآیند دو گزاره‌ی مذکور، مشخص می‌سازد که توان اقدام بالقوه‌ی کنترل‌شونده در راستای اطلاعات دریافتی از کنترل‌کننده چه میزان است. لذا اختلاف کیفی و کمّی میان اطلاعات دریافتی از کنترل‌کننده و اقدام صورت گرفته از کنترل‌شونده، بیانگر توان اقدام کنترل‌شونده است.

جدول ۲: نُه حالت حاصل از جایگشت سه حالت کوچکتر، مساوی و بزرگتر از منظر تناسب ریاضی با دوگانه‌ی کیفی و کمّی

x	کوچکتر	مساوی	بزرگتر
کیفی	به لحاظ کیفی کوچکتر	به لحاظ کیفی مساوی	به لحاظ کیفی بزرگتر
کمی	به لحاظ کمی کوچکتر	به لحاظ کمی مساوی	به لحاظ کیفی بزرگتر

در اینجا از جایگشت سه حالت کوچکتر، مساوی و بزرگتر از منظر تناسب ریاضی با دوگانه‌ی کیفی و کمّی، نُه حالت حاصل می‌شود که محل سنجش توان اقدام کنترل‌شونده در نسبت با مطالبات کنترل‌کننده درون چرخه‌ی سایبرنتیک است.

۱-۱) به‌لحاظ کیفی و کمّی، کوچکتر: در این حالت، توان اقدام کنترل‌شونده، هم از حیث کیفیت و هم از حیث کمیّت آن، کمتر از حد مطلوب کنترل‌کننده است. بدین معنا که اقدام صورت گرفته، نه عمق لازم را دارا است و نه گستره‌ی لازم را. جارو برقی هوشمندی را در نظر بگیرید که کنترل‌کننده (انسان) به آن برنامه داده اتاق ۱۰ متر مربعی را ظرف ۵ دقیقه، از هرگونه کثیفی و ذرات بزرگتر از دو میلی‌متر پاک نماید. حالت جاری چنین است که جارو پس از اتمام ۵ دقیقه، هم بخشی از مساحت را جارو نکرده باشد و هم در آن بخشی که جارو کرده است، همچنان ذرات بزرگتر از دو میلی‌متر یافت شود.

۱-۲) به‌لحاظ کیفی، کوچکتر و کمّی، مساوی: بدان معنا است که اقدام کنترل‌شونده از حیث گستره‌ی اقدام در محیط، در حد مورد انتظار کنترل‌کننده است اما بخش‌های تحت تأثیر از عمق لازم اثرپذیری برخوردار نیستند. به‌تعبیر دیگر کنترل‌شونده توانسته انتظارات کمی را برآورده سازد اما ضعیف‌تر از کیفیت مطلوب. مصداق این وضعیت در مثال جاروی هوشمند، اینگونه است که برنامه‌ی جاروی اتاق ۱۰ متری رأس مدت ۵ دقیقه پایان می‌یابد اما کماکان در فضای اتاق، ذرات بزرگتر از ۲ میلی‌متر وجود دارد.

۱-۳) به‌لحاظ کیفی، کوچکتر و کمّی، بزرگتر: در این حالت، کنترل‌شونده توانسته گستره‌ی اقدام را پوشش دهد اما فاقد کیفیت مطلوب می‌باشد. مانند اینکه جاروبرقی هوشمند، اتاق ۱۰ متری را درزمان کمتر از ۵ دقیقه جارو نماید اما همچنان ذرات بزرگتر از ۲ میلی‌متر در فضا یافت شود.

۱-۲) به‌لحاظ کیفی، مساوی و کمّی، کوچکتر: توان اقدام کنترل‌شونده با عمق فرمان کنترل‌کننده، برابری دارد اما به‌لحاظ کمّی وضعیت مطلوب را دارا نیست. برای مثال جاروبرقی هوشمند می‌تواند ۱۰ متر مربع را کاملاً از ذرات بزرگتر از ۲ میلی‌متر پاک نماید اما در مدت زمانی بیش از ۵ دقیقه.

۲-۲) به‌لحاظ کیفی و کمّی، مساوی: چنانچه توان اقدام کنترل‌شونده در نسبت با مطلوبات کنترل‌کننده، از هر دو حیث کیفی و کمّی در وضعیت برابر باشد، در وضعیت فعلی قرار می‌گیرد. بدان معنا است که جاروی هوشمند، فضای ۱۰ متری را دقیقاً رأس ۵ دقیقه به‌گونه‌ای جارو کند که هیچ ذره‌ی بزرگتر از ۲ میلی‌متر روی زمین باقی نمانده باشد.

۳-۲) به‌لحاظ کیفی، مساوی و کمّی، بزرگتر: کنترل‌شونده قادر است اطلاعات دریافتی از کنترل‌کننده را با کیفیت مطلوب و گستره‌ای فراتر از سطح انتظار کنترل‌کننده محقق سازد. البته لازم به‌ذکر است که کنترل‌شونده دقیقاً باید معادل اطلاعات دریافتی از کنترل‌کننده اقدام کند و اگر توان کاهش آن را دارد، اقدام به کاهش ننماید مگر آنکه اطلاعاتی در این خصوص دریافت نموده باشد. برای نمونه، جاروی هوشمند فضای ۱۰ متری اتاق را می‌تواند در زمان کمتر از ۵ دقیقه از ذرات بزرگتر از ۲ میلی‌متر پاکسازی کند اما مادامی که برای استفاده از این توانمندی مخیر نشده است، در همان مدت ۵ دقیقه باید کار را به اتمام رساند.

۳-۱) به‌لحاظ کیفی، بزرگتر و کمّی، کوچکتر: یعنی نسبت به آنچه مطلوب کنترل‌کننده است، توان اقدام کنترل‌کننده از حیث عمق اثر بیشتر بوده اما گستره‌ی آن کمتر است. البته زمانی مجاز به اقدام فراتر از حد مطلوب است که کنترل‌کننده فرمان آن را صادر نموده باشد. نظیر جاروی هوشمندی که می‌تواند در اتاق ۱۰ متری، ذرات کوچکتر از ۲ میلی‌متر را نیز جارو نماید (در صورت دریافت فرمان) اما در زمانی بیش از ۵ دقیقه.

۳-۲) به‌لحاظ کیفی، بزرگتر و کمّی، مساوی: کنترل‌شونده می‌تواند عمق اثری فراتر از حد مطلوب کنترل‌کننده را در صورت درخواست وی، دقیقاً در گستره‌ی مقرر ارائه نماید. مانند زمانی که جاروی هوشمند بتواند علاوه بر ذرات ۲ میلی‌متری و بزرگتر از آن، ذرات کوچکتر از ۲ میلی‌متر را نیز از فضای ۱۰ متری اتاق دقیقاً در زمان ۵ دقیقه جارو نماید.

۳-۳) به‌لحاظ کیفی و کمّی، بزرگتر: نسبت توان اقدام کنترل‌شونده با اطلاعات دریافتی از کنترل‌کننده، هم از حیث عمق اثر و هم گستره‌ی اثرگذاری بیشتر است. منتها برای عملیاتی‌سازی هر دو باید از کنترل‌کننده فرمان دریافت کند. بدین معنا است که جاروبرقی هوشمند می‌تواند علاوه بر ذرات بزرگتر از ۲ میلی‌متر، ذرات کوچکتر را نیز به‌گونه‌ای جارو نماید که فضای ۱۰ متری در زمان کمتر از ۵ دقیقه پاکسازی شود.

۳.۴.۳ قانون سوم سایبودینامیک: هدر رفت توان اقدام کنترل‌شونده

گزاره: در چرخه‌ی سایبرنتیک، کنترل‌شونده نمی‌تواند تمامی توان خود را به اقدام در راستای اطلاعات دریافتی از کنترل‌کننده تبدیل نماید.

اثبات: توان اقدام کنترل‌شونده از برآیند توان محاسباتی آن و میزان انرژی ستاده از محیط حاصل شده است. اولاً محاسبات از دو بخش پردازش و ذخیره‌سازی تشکیل شده است. پردازش نسبت به اطلاعات دریافتی از کنترل‌کننده و سایر مواردی که نیازمند پردازش اطلاعاتی هستند، می‌باشد. از سویی هیچ سیستم هوشمندی، توان محاسبات صد در صدی محیط را ندارد. به‌تعبیر دیگر ادراک هر پدیده‌ی هوشمند از محیط، مطابق ظرفیت پردازشی‌اش است، نه دقیقاً تمامی شئون و کیفیاتی که در محیط وجود دارد. از این رو بدیهی است اگر بخشی از مطلوبات کنترل‌کننده، یا اصلاً توسط کنترل‌شونده پردازش نشود یا دچار نقص و خطا گردد. در نتیجه بخشی از توان پردازشی کنترل‌شونده، درگیر خطا است ولو آنقدر کم که قابل اغماض بوده و

بر اصل فرایند کنترل در چرخه‌ی سایبرنتیک اثرگذار نباشد. ازسوی دیگر، فرایند ذخیره‌سازی نیز از تضمین مطلق برخوردار نیست و ممکن است در بخش‌های مختلف آن نظیر ذخیره‌سازی، بازخوانی و بازیابی و ... دچار اشکال گردد که در نتیجه بخشی یا تمام توان محاسباتی را دچار اختلال می‌نماید.

اما آنچه بیان شد، تمام دلیل نیست. یکی از مشکلات پر تکرار در سیستم‌های هوشمند، عقب ماندن توان اقدام نسبت به توان ادراک است. بدین معنا که ممکن است پدیده‌ی هوشمند (اعم از زیستی و غیر زیستی) از حیث ادراکی متوجه شود که باید چه کار کند اما عملگرهای مناسبی برای اجرا و عینیت‌بخشی به آن را نداشته باشد یا از تسلط کافی برای به‌کارگیری عملگرهایش برخوردار نباشد. برای نمونه، سیستمی که متولی ایجاد برش‌های بسیار کوچک و دقیق روی اجسام است، به‌لحاظ نرم‌افزاری می‌تواند در راستای دستور دریافت شده از کنترل‌کننده، میزان و محل برش را تعیین کند اما نمی‌تواند در عمل به‌صورت دقیق و کاملاً منطبق، اجرا نماید. لذا معمولاً میان دریافت انتزاعی یک فرمان با پیاده‌سازی آن، اختلاف وجود دارد، ولو قابل چشم‌پوشی.

از سمت دیگر، مسأله‌ی انرژی نیز بر توان اقدام کنترل‌شونده مؤثر است. اینکه کنترل‌شونده در چه زمانی، از چه طریقی، به چه میزانی، به کدام منابع انرژی دسترسی یابد؛ تأثیر مستقیم بر این دارد که چگونه و چه میزان بتواند در راستای اطلاعات دریافتی از کنترل‌کننده، اقدام متناسب صورت دهد. کوچکترین اخلالی در بخش انرژی کنترل‌شونده، به‌معنای اخلال در توان اقدام آن است و از آنجا که ذات فیزیکی انرژی، فاقد خطا نیست؛ در نتیجه همیشه میزانی از خطا بابت مسائل مرتبط به انرژی در توان اقدام کنترل‌شونده وجود دارد.

در مجموع آنکه همواره بخشی از توان اقدام کنترل‌شونده، به‌دلایلی که بیان شد بابت فرایند اقدام صرف می‌شود و به خروجی تبدیل نمی‌گردد، از این رو تمام توان اقدام کنترل‌شونده به خروجی در راستای چرخه‌ی سایبرنتیک تبدیل نمی‌گردد.

بر اساس آنچه بیان شد، مفهوم بهینگی برای توان اقدام کنترل‌شونده مطرح می‌شود، بدین معنا که چگونه می‌توان حداکثر بهره‌وری و خروجی را از یک کنترل‌شونده در چرخه‌ی سایبرنتیک دریافت نموده و ناتوانی کمّی و کیفی آن را به حداقل ممکن رساند؟ بخش مهمی از تمرکز هوش مصنوعی، دقیقاً در راستای ارائه‌ی پاسخ‌های کیفی و کمّی به پرسش فوق است و اساساً یکی از مهم‌ترین انگیزه‌های بشر برای جایگزینی ماشین هوشمند با انسان در امور روتین و حتی تخصصی، بابت این است که به‌طور میانگین، ماشین‌ها از بهینگی بالاتری نسبت به انسان در توان اقدام برخوردار هستند.

۴.۴.۳ قانون چهارم سایبودینامیک: پایداری چرخه

گزاره: چرخه‌ی سایبرنتیک در دو وضعیت، پایدار است:

- **الف) برقراری تناسب میان اطلاعات و اقدام**
- **ب) عدم وجود جریان اطلاعات: چرخه‌ی خاموش**

اثبات: برای اثبات، هر بخش به‌صورت مجزا مورد بررسی قرار می‌گیرد:

الف) استمرار و پایداری چرخه‌ی سایبرنتیک، حاصل ایجاد و ادامه یافتن مدار اطلاعات میان اجزای چرخه‌ی مذکور است. از سمت دیگر اساس وجود چرخه‌ی سایبرنتیک بر کنش و واکنش‌های میان کنترل‌کننده و کنترل‌شونده بنا شده است به‌گونه‌ای که کنترل‌کننده، اطلاعات مد نظر را برای کنترل‌شونده ارسال نموده و در مقابل آن، اقدام دریافت می‌کند. حال اگر میان اطلاعات ارسالی و اقدام دریافتی، تناسب کیفی و کمّی برقرار باشد؛ چرخه‌ی سایبرنتیک در وضعیتی پایدار و با ثبات قرار می‌گیرد. به‌عبارت دیگر ارسال اطلاعات از سوی کنترل‌کننده و اقدام متناسب آن ازسوی کنترل‌شونده، باعث جلوگیری از بروز بی‌نظمی و ناپایداری در چرخه‌ی سایبرنتیک گشته و مانع از زوال سیستم خواهد شد. پس تا زمانی که تناسب مذکور ادامه داشته باشد، شرایط چرخه نیز پایدار خواهد بود.

نکته‌ی مهم آن است که تفاوتی ندارد چرخه‌ی سایبرنتیک در پدیده‌های زیستی پیاده‌سازی شود یا غیر زیستی. در هر حال، چه کنترل‌شونده، ماشین باشد و چه انسان، شرایط قوانین سایبودینامیک از جمله قانون پایداری چرخه بر آن صادق است.

ب) مادامی که جریان اطلاعات وجود دارد، دائماً تمامی اجزا خصوصاً کنترل‌کننده و کنترل‌شونده در حال تغییر وضعیت هستند که باعث می‌شود نظمی پویا ایجاد گردد، نه ایستا. در این شرایط هر لحظه امکان دارد به‌دلیل وقوع خطا در عملکرد هر کدام از اجزای چرخه، جریان اطلاعات از استمرار خارج شده و متوقف گردد یا به سمت انحراف اطلاعاتی سوق یابد. لذا پایداری چرخه‌ی سایبرنتیک مختل شده و به‌سمت ناپایداری میل می‌کند. بنابر این، هر چند که فعالیت چرخه‌ی سایبرنتیک، به‌واسطه‌ی ثبات در جریان اطلاعات از ثبات و پایداری برخوردار است اما باید توجه داشت که این پایداری، نسبی است نه مطلق و هر لحظه امکان ناپایدار شدن چرخه وجود دارد. ولیکن اگر چرخه‌ی سایبرنتیک علی‌رغم تعریف ارتباط معنادار میان اجزا، هنوز فعال نشده و جریان اطلاعات در آن برقرار نشده باشد؛ در این حالت به‌دلیل آنکه یک نظم ایستا بر چرخه حاکم شده، احتمال میل چرخه‌ی سایبرنتیک به‌سمت ناپایداری به صفر می‌رسد، حالتی که چرخه‌ی خاموش یا غیرفعال نام دارد.

۴ نتیجه‌گیری

هر چند اطلاعات از ابتدای حیات بشر در زندگی نقش داشته و تا واپسین دقایق زیست بشر این نقش بی‌بدیل ادامه خواهد یافت؛ اما نقش اطلاعات در اعصار مختلف از حیث عمق و گستره‌ی اثرگذاری یکسان نبوده است. عصر حاضر، عصری است که مهم‌ترین عنصر سازنده‌ی تمدن، اطلاعات است. گزاره‌ای که پیش از این هرگز تا این حد جدیت و شمولیت نداشته است. لذا عصر حاضر از حیث نقش عظیم و ویژه‌ی اطلاعات در تمدن‌سازی، نقطه‌ی عطف تاریخ انسان است.

از سوی دیگر مشخص شد اطلاعات، علاوه بر اثر بی‌بدیلی که در حوزه‌ی کنترل محیط و بسترسازی حکمرانی دارد، تا آنجا که حتی ماده و انرژی را نیز تحت سیطره‌ی خود دارد، اما قوانین متفاوتی دارد.

لذا جهان امروز ما در حالی که از حکمرانی اطلاعاتی ساخته شده و تغییرات بنیادین در آن و همچنین در شناخت انسان نسبت به جهان بر اساس جریان‌سازی و جریان‌مندی اطلاعات صورت می‌پذیرد، اما عموم انسان‌ها اینگونه تصور می‌کنند که این تغییرات صرفاً وابسته به ماده و انرژی است و قوانین حاکم بر این دو، برای فهم جهان نوین کفایت می‌کند. از این رو بزرگترین و عمیق‌ترین غافل‌گیری راهبردی برای عموم ملت‌ها و دولت‌ها رخ داده است. اطلاعاتی شدن جهان حاضر، تلفیقی توأمان از تهدیدها و فرصت‌ها است. فرصت‌هایی از جنس انجام اموری که سابقاً با اتکا با ابعاد ماده و انرژی امکان‌ناپذیر یا سخت‌امکان‌پذیر بودند، اما امروز با توان انسان در کنترل جریان اطلاعات امکان‌پذیر شده‌اند که همزمان به‌دلیل بسترسازی نوین برای تهدیدات نوپدید، جنبه‌ی تهدیدآفرین نیز دارد.

بنابر این ضروری است شناخت ما از جهان پیرامونی و رخدادهایی که در آن واقع می‌شود و همچنین رخدادهایی که در رکن اطلاعات گزارش می‌شود اما در ارکان ماده و انرژی هنوز رصد نشده است، مبتنی بر مؤلفه‌ی اطلاعات به‌روز رسانی و کامل گردد تا بتوانیم ملت آینده باشیم و در آینده‌ی جهان، نقش تمدنی خود را به‌عنوان کانون انقلاب اسلامی در جهان ایفا نماییم.

مراجع

[۱] نوربرت وینر، «**استفاده‌ی انسانی از انسان‌ها**»، ترجمه‌ی مهرداد ارجمند، تهران، سازمان انتشارات و آموزش انقلاب اسلامی، ۱۳۶۶، ص ۳۰.

[۲] ایرا لوین، «**شیمی فیزیک**»، ترجمه‌ی غلامرضا اسلامپور، انتشارات فاطمی، ویرایش پنجم، ۱۳۸۶، تهران، جلد یکم،

[۳] پل دیویس، «**شبح در ماشین**»، مترجم: تورج حوری، انتشارات مازیار، ۱۳۹۹،

[4] Leo Szilard, **"Über die Entropieverminderung in einem thermodynamischen System bei Eingriffen intelligenter Wesen"**, 1929, Zeitschrift für Physik (in German), P 53.

[5] Claude Shannon, **"A Mathematical Theory of Communication"**, Bell System Technical Journal, July 1948, Pages 379-423 and October 1948, Pages 623-656.

[6] Léon Nicolas Brillouin, **"Life, Thermodynamics, and Cybernetics"**, American Scientist Journal, Year 1949, Vol 37, Page 554.

[7] Brillouin, Leon, **"Negentropy Principle of Information"**, J. of Applied Physics, Year 1953, Vol 24, Pages 1152–1163.

[8] Léon Nicolas Brillouin, **"Science and Information Theory"**, Courier Corporation, 2nd edition, Pages 159-161.

[9] R. Penrose, **"The mass of the classical vacuum"**, (1991), In S. Saunders; H.R. Brown (eds.). The Philosophy of Vacuum, Oxford University Press, Pages 21–26.

[10] Paolo Bussotti, **"Introducing the concept of energy: educational and conceptual considerations based on the history of physics"**, University of Udine, Italy, Proceedings of the 5th International Baltic Symposium on Science and Technology Education, BalticSTE 2023, Link: https://files.eric.ed.gov/fulltext/ED629206.pdf

[11] Inna Semetsky, **"Information and Signs: The Language of Images"**, Entropy Journal, Year 2010, Volume 12, Link: https://doi.org/10.3390/e12030528

نسبت قلمرو حکمرانی با فضای سایبر

علی لک‌زائی [۱]، کاظم فولادی قلعه [۲]

[۱] دانشجوی کارشناسی ارشد گرایش امنیت سایبری، دانشکده برق و کامپیوتر، دانشگاه تربیت مدرس؛ دستیار پژوهشی آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
lakzaei.ali@modares.ac.ir
[۲] استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛ سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
kfouladi@ut.ac.ir

چکیده

موضوع حکمرانی از مباحثی است که در شرایط کنونی ذهن دانشمندان و سیاست‌مداران را به شکل توأمان درگیر کرده است. حکمرانی، از آن حیث که هم دانش است و هم کنش، از گستره وسیعی برخوردار بوده و آنچه باعث اهمیت بیشتر آن شده است، نقش و تأثیر آن در پیشرفت و عقب‌ماندگی کشورها است؛ آنچه امروزه بر پیچیدگی الگوهای حکمرانی افزوده است، افزوده شدن فضای سایبر به‌عنوان عنصری تعیین‌کننده در این عرصه می‌باشد. از این رو تعیین نسبت قلمرو حکمرانی با فضای سایبر از اهمیت مضاعف برخوردار است و اتخاذ هر رویکردی در باب قلمرو حکمرانی مستقیما بر گستره حکمرانی و سیاست‌های اتخاذ شده در این زمینه و در نتیجه بر امنیت ملی و بلکه تمامی ساحت‌های زندگی فردی و اجتماعی هر کشوری اثرگذار است؛ از این رو پرسش اصلی مقاله حاضر نسبت قلمرو حکمرانی با فضای سایبر است. فرضیه مورد بررسی این است که نسبت قلمرو حکمرانی با فضای سایبر سه عرصه را در بر می‌گیرد. ۱- حکمرانی در فضای سایبر ۲- حکمرانی بر فضای سایبر ۳- حکمرانی با فضای سایبر، مهم‌ترین دست‌آورد مقاله این است که غفلت از هر یک از سه عرصه مذکور موجب ناقص دیده شدن نسبت قلمرو حکمرانی با فضای سایبر بوده و به‌جای فرصت‌سازی، چالش‌خیز، تهدیدساز و بحران‌آفرین خواهد بود.

کلمات کلیدی: حکمرانی در فضای سایبر، حکمرانی بر فضای سایبر، حکمرانی با فضای سایبر، قلمرو حکمرانی، سایبرنتیک.

۱ مقدمه

تعریف واژه سایبرنتیکس [۱] در لغت‌نامه آکسفورد به این شرح است: «علم ارتباطات و سیستم‌های کنترل خودکار در ماشین‌ها و موجودات زنده». همان‌طور که واژه فیزیکس [۲] به‌معنای دانش فیزیک است، واژه

[1] Cybernetics
[2] Physics

«سایبرنتیکس» نیز به‌معنای دانش سایبرنتیک است؛ این واژه به‌عنوان یک دانش در سال ۱۹۴۸ برای اولین بار توسط نوربرت وینر ریاضیدان و دانشمند آمریکایی مورد استفاده قرار گرفت؛ در لغت‌شناسی نیز واژه سایبرنتیکس به کوبرنه‌تس[۳] یونانی برمی‌گردد؛ که به‌معنای «سکان‌دار» است. این واژه با واژه گاورننس[۴] به‌معنای «عمل یا نحوه کنترل یک ایالت، سازمان و غیره» یک ریشه مشترک دارد. هم‌ریشه بودن واژگان مختلف به‌معنای ارتباط میان مفهوم آن واژگان است. در زبان پارسی واژه گاورننس به واژه «حکمرانی» ترجمه شده است. در لغت‌نامه آکسفورد واژه «کنترل» در تعریف مفهوم هر دو واژه «سایبرنتکیس» و «گاورننس» به کار برده شده است؛ در نتیجه واژه منسوب به علم حکمرانی و واژه منسوب به علم سایبرنتیک در لغت و مفهوم از یک ریشه هستند و دربردارنده یک مفهوم واحد هستند.

فرض ما در این مقاله این است که «حاکمیت» و «سایبر» یکی هستند؛ این فرض ما بر دو پایه استوار است، یک پایه آن از منظر علم لغت‌شناسی است که مورد اشاره واقع شد و دیگری موضوع فلسفه «حاکمیت» است. امروزه ساز و کار همه چیز با گردش بلادرنگ و لحظه‌ای اطلاعات ممکن است، از نامه‌نگاری‌های کوچک میان‌سازمانی گرفته تا سامانه‌های بزرگ بانک‌ها، مراکز داده، تاکسی‌ها و ... که دقیقه‌ای اخلال در کار آن‌ها می‌تواند منجر به خطرات جبران‌ناپذیر مالی، جانی و حتی به خطر افتادن امنیت ملی شود. همچنین در تمامی سازمان‌ها و سازوکارهای موجود در دولت‌ها، کم‌تر حوزه‌ای وجود دارد که تحت نظر و اشراف کامل بخش فناوری اطلاعات نباشد. به عنوان، مثال در سازمان‌ها حتی برای تغییر در کوچک‌ترین ساز و کار اجرایی و اداری ابتدا باید با بخش فناوری اطلاعات هماهنگی لازم به‌عمل بیاید؛ که آیا چنین تغییری از آن منظر قابل اجراست یا خیر، اگر که قابل اجرا باشد آنگاه می‌توان آن را در قالب کلی اجرا نمود و اعمال کرد.

فضای سایبر فضایی است که اطلاعات در آن به‌صورت هدفمند به گردش در می‌آید. فضای سایبر برگرفته از دانش سایبرنتیک است و قوانین دانش سایبرنتیک بر آن حاکم است، همان‌طور که در فضای فیزیکی، قوانین دانش فیزیک حاکم است.

۱.۱ پیشینه

در زمینه ارتباط حکمرانی و فضای سایبر کتاب‌ها و مقالات متعددی نوشته شده است؛ از جمله کتاب «تحول در عصر فضای مجازی» به کوشش فیروزآبادی [۲]، کتاب «حکمرانی: مقدمه‌ای بسیار کوتاه[۵]» [۱۲] نوشته مارک بور، کتاب «فضای سایبر و امنیت سایبر» [۱۱] نوشته کوستوپولوس، کتاب بنیادی «استفاده انسانی از انسان‌ها[۶]» [۸] نوشته نوربرت وینر، کتاب «سایبرنتیک: از گذشته تا آینده» [۹] نوشته نوویکو[۷]، مقاله «چالش‌های راهبردی حکمرانی با گسترش فضای سایبر» [۴] به کوشش احسان کیان‌خواه، کتاب «نظریه حکمرانی از منظر اندیشمندان» [۳]، مقاله «شناسایی نقش‌های سیاستی در نظام حکمرانی محتوای فضای مجازی کشور» [۵]، مقاله «تحلیل پیشینه حکمرانی فضای مجازی جمهوری اسلامی ایران» [۶] به کوشش

[3] Kubernētēs
[4] Governance
[5] Governance: a very short introduction
[6] The human use of human beings
[7] Novikov

فیروزآبادی، مقاله «آسیب‌شناسی فضای مجازی» [۷] به کوشش مرضیه رونقی، مقاله «حکمرانی حریم خصوصی» [۱۳] به کوشش دوندا[8] و آلمیدا[9]، «حکمرانی در قرن بیست و یکم» [۱۸] نوشته روسناو[10].

۲.۱ مفاهیم

واژه حکمرانی از واژگانی است که علاوه بر استفاده گسترده از آن، تلقی‌های گوناگون و متفاوتی از آن ارائه شده، تا جایی که حکمرانی را به یک لفظ مشترک برای معانی گوناگون بدل ساخته است. این وضعیت تا جایی پیش رفته است که بسیاری از اوقات مفهوم حکمرانی، معادل یکی از مفاهیم اخص آن، یعنی «حکمرانی خوب[11]» انگاشته شده و تمام مؤلفه‌های حکمرانی خوب به مفهوم حکمرانی نیز تسری داده شده است. در یک تعریف ساده و مقدماتی، حکمرانی عبارت است از «فرآیند حکومت کردن» که شامل همه فرآیندهای برنامه‌ریزی، سازماندهی، جهت‌دهی، هدایت و کنترل نیز می‌شود. حکمرانی در محاورات رایج معاصر نیز به این معناست که «چگونه بازیگران - موجودیت‌های چندملیتی، حکومت‌ها، شرکت‌های خصوصی، گروه‌های اجتماعی یا سیاسی، اشخاص حقیقی یا ترکیبی از این موارد - برای تحقق اهدافی که آن بازیگران در آن موافق یا مشترک بوده‌اند، جهت‌دهی شده‌اند.» [۱].

فعالیت حکومت‌ها به صورت روز افزون در تنظیمات فراملی و بین‌المللی تنیده شده است، امری که ناشی از بین‌المللی شدن تعاملات صنعتی و مالی، ظهور بلوک‌های منطقه‌ای و افزایش نگرانی‌ها درباره مسائل جهانی، مانند تروریسم و محیط زیست، است. «حکمرانی در اینجا به معنای استفاده از روش‌های رسمی و غیررسمی توسط دولت‌ها برای پاسخ به نظم در حال تغییر جهانی است.» [۱۲].

هدف دانش سایبرنتیک به بیان پدر این علم، یعنی نوربرت وینر، بدین شرح است که زبان و تکنیکی را توسعه دهد تا مشکل کنترل و ارتباطات را به‌طور کلی یک بار برای همیشه، نه‌تنها فقط در ماشین‌ها بلکه در انسان‌ها نیز حل شود [۸]. نوویکو نیز در کتاب خود دانش سایبرنتیک را شاخه‌ای از علم کنترل در کنار فلسفه مدیریت که شاخه دیگر آن است می‌داند؛ که به مطالعه کلی‌ترین قواعد نظری کنترل می‌پردازد: «مبانی علم کنترل شامل قوانین کلی و اصول کنترل کارآمد است که این موارد در حوزه سایبرنتیک قرار می‌گیرد.» [۹].

در این مقاله با بهره‌گیری از تعاریف ارائه شده تعریف ذیل پیشنهاد می‌شود و مقصود ما از حکمرانی در این مقاله، همین تعریف خواهد بود: «حکمرانی به سیستم و فرآیندهایی اطلاق می‌شود که سازمان‌ها، نهادها یا جوامع به‌وسیله آن تصمیم‌گیری می‌کنند، سیاست‌ها را اجرا می‌کنند و امور خود را مدیریت می‌کنند. حکمرانی، دربرگیرنده سازوکارها، ساختارها و اصولی است که اعمال و رفتار افراد، گروه‌ها یا نهادها را برای دستیابی به اهداف و مقاصد مدنظر هدایت و تنظیم می‌کند و در عین حال مسئولیت‌پذیری، شفافیت و پایبندی به قوانین و هنجارهای تعیین‌شده را تضمین می‌کند.»

[8] Doneda
[9] Almeida
[10] Rosenau
[11] Good governance

در این مقاله، فضای سایبر را نیز با این تعریف مورد استفاده قرار خواهیم داد: «فضای سایبر، فضای تغذیه هدفمند اطلاعات است: این فضا یک فضای حقیقی ناملموس است و چهار رکن اساسی دارد که شامل اطلاعات، کنترل، ارتباطات و محاسبات می‌باشد.

۲ ارکان فضای سایبر

در فضای سایبر سه رکن اساسی وجود دارند که منجر می‌شوند تا رکن پایه اطلاعات در آن به صورت هدفمند به گردش در آید: ۱- کنترل، ۲- ارتباطات، ۳- محاسبات.

در یک محیط برای هدفمندسازی گردش اطلاعات، دو عنصر حیاتی وجود دارد:

۱. کنترل‌کننده‌ای که با انجام محاسبات بر اطلاعات دریافتی از محیط و بازخورد (فیدبک) دریافتی از کنترل‌شونده، اطلاعات (فرمان) را به‌وسیله رکن ارتباطات به کنترل‌شونده منتقل می‌کند.

۲. کنترل‌شونده‌ای که با دریافت اطلاعات (فرمان) از کنترل‌کننده، محاسباتی بر روی داده‌های دریافت شده انجام داده و کنش متناظر را بر محیط انجام می‌دهد.

کنشی که نتیجه‌ی اطلاعات دریافتی توسط کنترل‌شونده است، خود اطلاعات جدیدی را در محیط قرار می‌دهد که کنترل‌کننده بر آن‌ها اشراف پیدا می‌کند و با انجام محاسبات بر روی آن، فرمان بعدی خود را به‌گونه‌ای تعیین می‌کند که کنترل‌شونده به هدف مورد نظر نزدیک‌تر شود. بدین‌گونه چرخه سایبرنتیک متولد می‌شود و اطلاعات به شکلی هدفمند در یک محیط به گردش در می‌آیند. به‌عنوان مثال، در یک اتومبیل، راننده در نقش کنترل‌کننده و پدال‌های گاز و ترمز عامل‌های انتقال پیام یا عامل‌های ارتباطی او هستند. به وسیله این عامل‌ها راننده دستور خود را به کنترل‌شونده که اتومبیل است ارسال می‌کند. اتومبیل نیز بر اساس سازوکارهای محاسباتی که در آن تعبیه شده بر محیط کنشی را اجرا می‌کند که می‌تواند افزایش و یا کاهش سرعت باشد؛ راننده نیز با تحلیل بر روی اطلاعاتی که از کنش اتومبیل بر محیط دریافت کرده، قدم بعدی خود را برنامه‌ریزی و اعمال می‌کند.

۳ قلمرو حکمرانی

منظور از قلمرو حکمرانی، دایره شمول عرصه‌های حکمرانی است. همان‌طور که در منابع مذکور نیز آمده است، قلمرو حکمرانی و دایره شمول آن، تمامی عرصه‌های زندگی بشر را در بر می‌گیرد. به‌عبارتی، حکمرانی، عهده‌دار ساماندهی عرصه‌های مختلف زندگی سیاسی، اقتصادی، فرهنگی، مدیریتی، اجتماعی و ... جوامع بشری و هر آن چیزی است که به‌نحوی با انسان مرتبط می‌شوند. به‌عنوان مثال محیط زیست، آب، برق، گاز و ...؛ به‌همین دلیل است که ملاحظه می‌کنیم مفهوم حکمرانی برای موضوعات گوناگون به‌کار رفته است؛ از جمله: حکمرانی فرهنگی، حکمرانی اقتصادی، حکمرانی حقوقی، حکمرانی آب، حکمرانی برق، حکمرانی سیاست خارجی و ...

در این مقاله بحث ما محدود به حکمرانی فضای سایبر است. امروزه فضای سایبر به‌خاطر گستردگی روزافزون، تمام جنبه‌های زندگی ما را در بر می‌گیرد. لذا رویکرد دقیق در نسبت‌سنجی بین قلمرو حکمرانی و فضای سایبر این است که امروزه با توجه به نقش و جایگاهی که فضای سایبر در حاکمیت کشورها پیدا کرده است و اینکه فضای سایبر از یک بحث صرفاً فنی و تکنولوژیک و یا صرفاً ابزاری برای تسهیل امور مختلف و یا ایجاد دولت الکترونیک و حتی نظریه حکمرانی خوب فراتر رفته و تمامی عرصه‌های حاکمیتی زندگی انسان را پوشش می‌دهد.

به‌طور کلی می‌توان گفت که پنج دیدگاه در رابطه با نسبت سایبر با حاکمیت در جهان مطرح است که در ادامه به آنها اشاره می‌کنیم.

۱- عدم نسبت میان حاکمیت و سایبر: در این دیدگاه این ادعا می‌شود که هیچ نسبتی میان سایبر و حاکمیت وجود ندارد. افرادی که این دیدگاه را دارند، به‌طور کلی، کسانی هستند که اصالت را به «تکنولوژی» می‌دهند. کسی که اصالت را به تکنولوژی می‌دهد، با کسی که از تکنولوژی استفاده می‌کند متفاوت است. چنین شخصی معتقد است که همه چیز در دنیا را باید از نگاه تکنولوژی ملاحظه کرد. این افراد طرح این سؤال که «نسبت میان سایبر و حاکمیت چیست؟» را به‌طور کلی غلط می‌دانند و استدلال می‌کنند که سایبر یک مقوله تکنولوژیک و فنی است، و حاکمیت یک مفهوم استراتژیک و راهبردی است و برای همین رابطه‌ای ندارند. امروزه طرفداران این دیدگاه نسبت به سالیان گذشته کمتر شده‌اند.

۲- حاکمیت به‌عنوان فراهم‌کننده زیرساخت «سایبر» و نه چیز دیگر: دیدگاه دوم، حاکمیت را به‌عنوان فراهم‌کننده زیرساخت و تمهیدکننده امکانات لازم برای سایبر قبول دارد. در واقع، در این دیدگاه شأن حاکمیت تأمین نیاز شهروندان در قبال دریافت حق اشتراک است –نظیر آنچه در زمینه‌ی برق، آب، گاز و موارد مشابه عمل می‌کند– و اساساً نباید به قانون‌گذاری، نظارت، وضع سیاست و ... ورود کند. این دیدگاه نسبت به دیدگاه اول واقعی‌تر است، زیرا برای دستیابی عموم به سایبر، نیازمندی‌های بسیاری وجود دارد، از جمله: تهیه نقشه‌های جغرافیایی از مکان‌های مورد نظر برای بهره‌برداری، کابل‌کشی، دکل‌کشی، زیرساخت‌های مخابراتی و ... و از آنجا که این نیازمندی‌ها استفاده‌ی عمومی دارند، جایگاهی در اندازه‌ی حاکمیت برای راه‌اندازی و پشتیبانی نیاز خواهند داشت. نتیجه‌ی طبیعی این دیدگاه این است که حاکمیت درباره‌ی نحوه‌ی مصرف و بهره‌برداری از سایبر توسط مردم نباید دخالتی داشته باشد، همان‌طور که در خصوص زیرساخت‌هایی چون آب، برق و گاز عمل می‌کند و نهایتاً حجم مصرف را با وضع تعرفه و تعیین هزینه مدیریت می‌کند.

۳- حاکمیت به‌عنوان سیاست‌گذار، قانون‌گذار و نظارت‌کننده بر «سایبر»: در عموم نقاط دنیا مسئله سیاست‌گذاری، قانون‌گذاری، نظارت و مواردی از این قبیل، برای مفهوم سایبر نه تنها به رسمیت شناخته شده بلکه بسیار مورد تأکید و توجه است. در این دیدگاه نقش حاکمیت به عنوان تأمین‌کننده زیرساخت نقض نمی‌شود؛ بلکه علاوه بر آن، به‌دلیل ویژگی‌های ماهیتی سایبر، برخلاف برق، آب، گاز و ...، حاکمیت باید قانون‌گذاری، سیاست‌گذاری و نظارت را در دستور کار خود قرار دهد. مقوله‌ای که از آن با

نام «حکمرانی فضای سایبر» یا به‌تعبیری (البته با تسامح) به‌عنوان «حکمرانی فضای مجازی» یاد می‌کنند، به‌نوعی از این دیدگاه تازه شروع می‌شود. این دیدگاه بیشتر در شورای عالی فضای مجازی کشورمان رایج است [۲]. این دیدگاه یک نگاه حداقلی و یک نگاه حداکثری دارد. افرادی که این دیدگاه را دارند، در گستره‌ی این طیف قرار می‌گیرند.

۴- حاکمیت به‌عنوان بزرگ‌ترین و پیشرفته‌ترین بهره‌بردار «سایبر»: در بسیاری از کشورهای پیشرفته دنیا، امروزه این دیدگاه در حال تقویت شدن است. این دیدگاه حاکمیت را نه تنها تأمین کننده زیرساخت، قانون‌گذار، سیاست‌گذار و ناظر می‌داند؛ بلکه آن را پیشرفته‌ترین و بزرگ‌ترین کاربر سایبر می‌داند. این مورد زمانی رقم می‌خورد که حاکمیت تمام خدماتی را که می‌خواهد به مردم ارائه کند و تمام وظائفی که بر عهده دارد را از طریق فضای سایبر محقق کند: از طریق پلتفرم‌ها، نظارت‌ها از طریق دوربین، از طریق هوش مصنوعی و دیگر مفاهیمی که امروزه در رسانه‌ها به کرات شنیده می‌شوند. تمامی این موارد مربوط به دیدگاه چهارم هستند. برخی افراد عبارت «دولت فوق هوشمند» را برای این دیدگاه به‌کار می‌برند. این‌ها همه زمانی اتفاق می‌افتد که حاکمیت، خود، بزرگ‌ترین بهره‌بردار و کاربر سایبر می‌شود. امتیاز این مورد آن است که اگر حاکمیت به چنین چیزی دست یابد و خود بزرگ‌ترین بهره‌بردار سایبر شود، آنگاه به‌دلیل نیازمندی‌های بالای سخت‌افزاری و نرم‌افزاری، اکوسیستم مربوط به پدیده آی‌تی[۱۲] و آی‌سی‌تی[۱۳] فوق‌العاده گسترده می‌شود، چرا که باید پاسخگوی نیازهای حاکمیت باشد. در نتیجه، سرریز تمام این پیشرفت‌ها وارد زندگی مردم نیز می‌شود و شهروندان نیز از این قابلیت‌ها بهره‌مند می‌شوند. در اسناد سازمان ملل این از این دیدگاه با عنوان «حکمرانی خوب» نام برده می‌شود.

۵- این‌همانی سایبر و حاکمیت به نظر می‌رسد چهار دیدگاه مذکور، برای شکل‌گیری یک حکمرانی و حاکمیت مستقل و قدرتمند در یک کشور، دیدگاه‌های کاملی نیستند. ضعف دیدگاه اول که بدیهی است، اما دیدگاه دوم، سوم و چهارم، همگی یک نقطه ضعف دارند و آن این است که دیدگاه آنها به سایبر یک نگاه ابزاری است و به‌عنوان یک پدیده ابزاری و وسیله به سایبر نگاه می‌شود، البته یک وسیله پیشرفته و شگفت‌انگیز. اما نگاه همه‌ی آنها درنهایت یک نگاه ابزاری است. اما در نگاه پنجم از نگاه ابزاری فاصله می‌گیریم و می‌گوییم که سایبر درواقع خود حاکمیت است. از این منظر، این‌همانی و نسبت تساوی بین این دو برقرار است. در نتیجه فضای بحث و اقدام از فضای تکنولوژیک و ابزاری به فضای استراتژیک و راهبردی تغییر می‌کند.

با این نگاه توجه به وجوه و لایه‌ها و سطوح حکمرانی سایبری دارای اهمیت است، که در ادامه مقاله به آن می‌پردازیم.

[12] Information technology
[13] Information and communications technology

۴ حکمرانی بر / با / در فضای سایبر

۱.۴ حکمرانی بر فضای سایبر

«فارغ از استفاده‌ای که دولت‌ها از فضای مجازی برای تقویت حاکمیت خود دارند، یکی از دغدغه‌های مهم آن سامان‌دهی و مدیریت فضای مجازی است. بر این اساس، دولت‌ها فضای مجازی را به‌عنوان یکی از اجزای زندگی مردم تحت حاکمیت در می‌آورند و آن را متناسب با قوانین موجود در کنار سایر اجزا مدیریت می‌نمایند. به عبارت دیگر، حکمرانی بر فضای مجازی[۱۴]، وضعیتی است که حاکمیت ملی بتواند فضای مجازی را به‌منزله بخشی از قلمرو خود، تحت قوه آمرانه خود قرار دهد.» [۲]. در اینجا، حاکم، فضای سایبر را به‌مثابه یک محصول می‌بیند. به‌عنوان پدیده‌ای که وارد قلمرو حاکمیتی می‌شود و حاکمیت مانند تمامی پدیده‌های دیگر، این پدیده را نیز باید تحت حاکمیت خود درآورد. به عنوان مثال، محصولی حیاتی همچون آب که نیازمند سازوکار مشخص و قانونی مطابق با اهداف حاکمیتی است، حکومت تلاش می‌کند تا این حوزه را تحت سلطه خود درآورد و بر آن سیطره پیدا کند. به‌عنوان مثالی دیگر، کارخانه‌ای بزرگ در حوزه ماشین‌آلات، این کارخانه را به‌اندازه‌ای بزرگ و قدرتمند تصور کنید که درصد زیادی از حجم بازار ماشین‌آلات کشوری را شامل شود؛ حکومت در اینجا چنین موجودیت عظیمی را به دلایل متعدد تحت سلطه خود در می‌آورد و بر آن قانون‌گذاری می‌کند تا بتواند از خطرات احتمالی جلوگیری کند و با استفاده از آن به سمت اهداف خود قدم بردارد.

۲.۴ حکمرانی با فضای سایبر

«در رویکرد حکمرانی با فضای سایبر[۱۵] از فضای مجازی به‌عنوان «ابزار خدمت‌رسانی» و اعمال حاکمیت در فضای حقیقی استفاده می‌کنند. آنچه به‌عنوان دولت الکترونیک طرح می‌شود در این سطح است. تلاش دولت‌ها در استفاده از این فضا برای اعمال حاکمیت کلاسیک و سنتی نیز در همین صورت خلاصه می‌شود. در این صورت، اصول حاکمیت تغییر نکرده و فقط از فناوری‌های اطلاعاتی و ارتباطی با نگاه ابزاری خدمات اتوماسیون ارائه می‌گردد.» [۲]. به‌نوعی در این منبع، روش حکمرانی همان حکمرانی خوب است. حکومت تنها به جهت سهولت بخشیدن به فرآیندها، خدمت‌رسانی و اتوماسیون، نقش فراهم‌کننده زیرساخت را خواهد داشت. در این رویکرد، اصول حاکمیت تغییر نکرده، فضای سایبر با ظهور خود نقش کلیدی در گستره حکمرانی نخواهد داشت، بلکه اهمیت این موضوع محدود شده و فقط دیدگاه «حاکمیت به عنوان فراهم‌کننده زیرساخت سایبر و استفاده ابزاری از آن» مورد نظر است.

رویکرد دو فضایی نیز بر این دیدگاه حاکم است. بدین‌گونه که فضای واقعی و فضای مجازی را به‌مثابه دو فضای جدا در نظر گرفته است. چرا رویکرد دوفضایی به‌جای رویکرد امتدادی به کار گرفته شده است؟ این پدیده زمانی اتفاق می‌افتد که ما واژه Cyberspace را با عنوان «فضای مجازی» ترجمه کنیم و به‌نوعی با به‌کار بردن این واژه در ترجمه، ماهیت واقعیت ناملموس فضای سایبر را از آن گرفته و ماهیت مجازی و غیرواقعی بودن را به آن بدهیم. این کار باعث می‌شود تا ما فضای مجازی را جدا از فضای واقعی بدانیم. از

[14] Governance on Cyberspace
[15] Governance by Cyberspace

این اشتباه شناختی، تعابیر غلطی نظیر «هر چیزی که در فضای واقعی وجود دارد، باید در فضای مجازی نیز وجود داشته باشد» سر بر می‌آورند.

ما در دیدگاه مورد نظرمان در این مقاله «حکمرانی با فضای سایبر» را نتیجه اعمال درست رکن «حکمرانی بر فضای سایبر» می‌دانیم، بدین‌گونه که اگر حکمرانی بر فضای سایبر به‌درستی صورت گیرد، می‌توان دست به عمل حکمرانی با فضای سایبر زد. در نتیجه باید سازوکارها، ساختار و اصولی را برای آن تعریف کرد تا بتوان با آن به اهداف مورد نظر حاکمیتی در فضای سایبر دست یافت.

۳.۴ حکمرانی در فضای سایبر

«در رویکرد حکمرانی در فضای سایبر[۱۶]، دولت‌ها تحول زندگی بشر در عصر فضای مجازی را به‌خوبی درک کرده و می‌پذیرند که فضای مجازی «فقط» مولد پاره‌ای از مسائل نیست؛ بلکه کلیت فضای زندگی مردم و افق تمدنی جدیدی را می‌سازد. به‌همین دلیل دولت‌ها، فراتر از دو حالت قبلی سعی می‌کنند ساختار خود را در راستای اعمال حاکمیت «در» آن عصر متحول کنند.» [۲]. در این دیدگاه فضای سایبر به‌عنوان یک زیست بوم تصور می‌شود. یک فضای زندگی که تمامی شئون زندگی در آن قرار دارد و حاکمیت نیز جزئی از آن است. لذا هنگامی که حاکمیت می‌خواهد اعمال حاکمیت کند، با در نظر گرفتن این موضوع اقدام می‌کند که خود نیز در آن زیست‌بوم حضور دارد. البته که این رویکرد پیچیدگی بیشتری از دو رویکرد قبلی دارد و به مراتب نیز اثربخش‌تر است، هرچند ملاحظات خاص خود را خواهد داشت.

۵ نتیجه‌گیری

با توجه به آنچه گفته شد و به‌ویژه تأکید بر این نکته که فضای سایبر دربردارنده همه قلمروهای حکمرانی است می‌توانیم اکنون بر این نتیجه تأکید کنیم که از میان نسبت‌های چهارگانه منطقی، یعنی نسبت تباین، نسبت عام و خاص من‌وجه، نسبت عام و خاص مطلق و تساوی، میان قلمرو حکمرانی و فضای سایبر، تساوی وجود دارد، دلایل این امر از آنچه آمد روشن شد. به‌طور خلاصه، استدلال این بود که چون فضای سایبر دربردارنده همه ساحت‌های امر حاکمیتی است و قلمرو حکمرانی هم در بردارنده تمام ساحت‌های حاکمیتی است، بنابراین بین این دو نسبت تساوی برقرار است. این امر از تأملاتی که در عرصه حکمرانی با فضای سایبر، حکمرانی در فضای سایبر و حکمرانی بر فضای سایبر آمد نیز به‌نحو دیگری روشن گشت.

مراجع

[۱] قلی‌پور، حسین (۱۴۰۰). حکمرانی علم: دانشمندان چگونه راهبری می‌شوند؟ انتشارات سروش.

[۲] فیروزآبادی، ابوالحسن (۱۳۹۹). تحول در عصر فضای مجازی. انتشارات پژوهشگاه فضای مجازی.

[۳] خان محمدی، هادی و خداپرست، عباس (۱۴۰۱). نظریه حکمرانی از منظر اندیشمندان. انتشارات سازمان جهاد دانشگاهی تهران.

[16] Governance in Cyberspace

[۴] کیان‌خواه، احسان (۱۳۹۸). چالش‌های راهبردی حکمرانی با گسترش فضای سایبر. انتشارات امنیت ملی.

[۵] خدمتگزار، حمیدرضا و نامداریان، لیلا (۱۴۰۲). شناسایی نقش‌های سیاستی در نظام حکمرانی محتوای فضای مجازی کشور. مجموعه مقالات نهمین کنفرانس بین‌المللی وب‌پژوهی.

[۶] فیروزآبادی، ابوالحسن، آزادی احمدآبادی، جواد (۱۳۹۹). تحلیل پیشینه حکمرانی فضای مجازی جمهوری اسلامی ایران. نشریه دانش سیاسی. شماره ۲.

[۷] رونقی، مرضیه (۱۳۹۶). آسیب‌شناسی فضای مجازی. کنفرانس پژوهش‌های نوین ایران و جهان در روان‌شناسی و علوم تربیتی حقوق و علوم اجتماعی.

[8] Wiener, N. (1954). The human use of human beings: Cybernetics and society.

[9] Novikov, D. N. (2016). Cybernetics: From past to future. Springer. https://link.springer.com/book/10.1007/978-3-319-27397-6

[10] Lerner, A. Ya. (1972). Fundamentals of Cybernetics. Plenum Publishing Corporation.

[11] Kostopoulos, G. K. (2017). Cyberspace and Cybersecurity. (2nd ed.). CRC Press.

[12] Bevir, M. (2012). Governance: a very short introduction. Oxford University Press.

[13] Doneda, D., & Almeida, V. A. F. (2015). Privacy governance in Cyberspace. IEEE, 19(3).

[14] Liaropoulos, A.N. (2017). Cyberspace Governance and State Sovereignty. In: Bitros, G., Kyriazis, N. (eds) Democracy and an Open-Economy World Order. Springer, Cham. https://doi.org/10.1007/978-3-319-52168-8_2

[15] Bajaj, K. (2014). Cyberspace: Post Snowden. Strategic Analysis, 38, 582–587.

[16] Betz, D., & Stevens, T. (2011). Cyberspace and the state. Toward a strategy for cyber-power (Adelphi Paper 424). Oxon: IISS, Routledge.

[17] Choucri, N. (2012). Cyberpolitics in international relations. Cambridge, MA: The MIT Press.

[18] Rosenau, J. (1995). Governance in the twenty-first century. Global Governance, 1, 13–43.

[19] Jayawardane, S.; Larik, J.E.; Jackson, E. (2015). Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance. http://www.thehagueinstituteforglobaljustice.org/wp-content/uploads/2015/12/PB17-Cyber-Governance.pdf

[20] Chertoff, M., & Simon, T. (2015). The impact of the dark web on Internet Governance and Cyber Security (Global Commission on Internet Governance: Paper Series No. 6). The Centre for International Governance. Retrieved Feburary 20, 2016, from https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf

[21] Cornish, P. (2015). Governing cyberspace through constructive ambiguity. Survival, 57, 153–176.

[22] Deibert, R. (2013). Bounding cyber power: Escalation and restrain in global cyberspace (Internet Governance Papers: Paper No. 6). The Centre for International Governance Innovation. Retrieved Feburary 20, 2016, from https://www.cigionline.org/sites/default/files/no6_2.pdf

مسئولیت حقوقی استفاده ابزاری نادرست از رسانه سایبر نسبت به مخاطبان و مسئولیت همزمان مخاطب

علی عرب نجف‌آبادی[۱]

[۱]دانشجوی کارشناسی ارشد فقه و مبانی حقوق اسلامی، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
ali.arab5965889@gmail.com

چکیده

استفاده ابزاری نادرست از رسانه‌ها در فضای سایبر در صورتی که منجر به ورود ضرر و زیان به مخاطبان شود از موجبات احراز مسئولیت حقوقی است که این مسئولیت ممکن است در نتیجه توهین و پخش ادعاهای واهی، هتک حرمت، انتشار ویروس‌های رایانه‌ای، تبلیغات دروغین، بی‌مبالاتی در تولید نرم‌افزارها و مواردی از این قبیل ایجاد شود. با وجود اینکه فرامرزی بودن، دشواری‌های کنترل و هویت پنهان بازیگران حاضر در این فضا می‌تواند موجب دشواری اثبات مسئولیت افراد گردد، اما در حالت احراز از جنبه حقوقی بیشتر نظریه تقصیر در باب مبنای مسئولیت حقوقی رسانه‌ها و نظریه خطر در باب مبنای مسئولیت همزمان مخاطب از توجه بیشتری برخوردار است. در این میان و در راستای استفاده ابزاری نادرست از رسانه سایبر نسبت به مخاطبان، می‌توان به احراز مسئولیت در مقابل مخاطبین و بعضا مسئولیت همزمان مخاطب اشاره نمود چرا که اگر استفاده از رسانه سایبر بر اساس سیاستی متناسب، معقول، منطقی و مبانی مستحکم صورت نگیرد نه فقط پیامدهای مطلوبی نخواهد داشت بلکه خود سبب ایجاد گرفتاری‌ها و معضلات اجتماعی و حقوقی زیادی خواهد گشت. بر همین اساس این مقاله از نوع نظری بوده و روش آن، توصیفی تحلیلی و کتابخانه‌ای می‌باشد و با مراجعه به اسناد، کتب و مقالات صورت گرفته است.

۱ مقدمه

رسانه‌های سایبری وسایلی هستند که پیام‌رسانی و انتقال اطلاعات موجود در جوامع را به مخاطبان خود انتقال می‌دهند. این رسانه‌ها که خود دارای شخصیت حقوقی می‌باشند، می‌توانند موجبات ضررهای مادی و معنوی را به مخاطبان وارد نمایند و متعاقب آن نیز برای مخاطبان امکان اثبات مسئولیت همزمان وجود دارد. رسانه‌ها مبرا از مسئولیت نیستند چرا که بعضا با استناد به آزادی‌های رسانه‌ای حریم خصوصی اشخاص نادیده گرفته می‌شود و به حرمت و حیثیت اشخاص یا اقوام یا اقلیت‌های دینی و مذهبی توهین می‌شود و یا با

استفاده نادرست از رسانه‌ها به افراد افترا زده می‌شود یا حتی داده‌هایی منتشر می‌شود که بر رویه رسیدگی در دادگاه‌ها تأثیرمی‌گذارد و حتی در استفاده نادرست مذکور بدون اجازه اشخاص اثر علمی آنان منتشر می‌گردد و حتی بعضا مشاهده شده است که با وجود احراز مسئولیت حقوقی در استفاده ابزاری نادرست از رسانه سایبر، قربانیان به علت خلاء قانونی یا نارسایی-های موجود موفق به مطالبه خسارت خود نمی‌شوند. نگاهی هر چند اجمالی به نظام حقوقی ایران روشن می‌نماید که با وجود بهتر شدن وضعیت با تصویب قانون جرایم رایانه‌ای در سال ۱۳۸۸ همچنان خلأهای زیادی در پاسخگویی به نیازهای کنونی جامعه در این باره وجود دارد و لازم است قوانین اختصاصی حاکم بر فعالیت رسانه‌های همگانی و استفاده از آن‌ها تبیین گردد. در رابطه با مسئولیت مذکور اعم از مسئولیت حقوقی استفاده ابزاری نادرست از رسانه سایبر نسبت به مخاطبان و مسئولیت همزمان مخاطب، مبانی مختلفی اعم از فقهی و حقوقی وجود دارد که بررسی آن‌ها می‌تواند زوایای اهمیت این موضوع را بیش از پیش نشان دهد.

۲ مبانی مسئولیت استفاده ابزاری نادرست از رسانه سایبر

در متون فقهی وحقوقی قواعد مختلفی در باب مبنای مسئولیت مطرح شده است که با توجه به عام بودن این قواعد، قابل تعمیم به حوزه رسانه نیز می‌باشند و علی‌القاعده این قواعد در حیطه‌های مختلف اعم از مسئولیت حقوقی و کیفری رسانه‌ها قابل استفاده می‌باشند و شامل مبانی فقهی وحقوقی است که در تقسیم‌بندی‌های ذیل قرار می‌گیرند.

۱.۲ مبانی فقهی

مبانی فقهی در احراز مسئولیت استفاده ابزاری نادرست از رسانه شامل موارد ذیل است:

الف: قاعده اتلاف و تسبیب

برخی از فقها قاعده اتلاف و تسبیب را به عنوان دو قاعده جداگانه بیان نموده‌اند و موجبات ضمان، آن-ها را تلقی نموده‌اند (علامه حلی، ۱۴۱۸: ۷۶۲). حقوقدانانی مانند مرحوم کاتوزیان نیز همین عقیده را داشتند (کاتوزیان ، ۱۳۸۶ :۱۵۶). اما برخی دیگر معتقدند اتلاف امکان دارد بالمباشره باشد یا بالسبب (شهیدثانی، ۱۴۱۶: ۱۶۲)؛ در نتیجه قاعده تسبیب، قاعده مستقلی محسوب نمی‌شود بلکه فرعی از قاعده کلی اتلاف خواهد بود. به عقیده این گروه از فقها؛ این مسئله که متلف سبب یا مباشر یا نحو آن باشد، اهمیتی ندارد چرا که این دو به مرتبه خاصی تعلق ندارند، بلکه یکی سبب و آن دیگری سبب سبب است (حسینی المراغی، ۱۴۱۷: ۴۳۵). به نظر می‌رسد نظر دوم در حیطه بحث این مقاله مناسب‌تر است. بر این اساس قاعده اتلاف اعم از بالمباشره یا بالتسبیب زمانی موجب مسئولیت است که رابطه سببیت عرفی بین زیان و عامل زیان

برقرار گردد. در اتلافی که به صورت مباشرت و مستقیم ناشی از استفاده ابزاری نادرست از رسانه باشد در اصل این رابطه محرز است و باید حکم به جبران خسارت داد. اما بعضاً در اتلاف بالتسبیب یعنی استفاده نادرست اگر به صورت غیرمستقیم موجبات ضرر را فراهم نموده باشد احراز تقصیر برای احراز سببیت عرفی باید وجود داشته باشد (مبین، ۱۳۸۷: ۱۰۲)، و در غیر این صورت تقصیر چه از طرف رسانه و چه از طرف مخاطب به صورت همزمان در مسئولیت مدنی دارای موضوعیت نمی‌باشد (حسینی سیستانی، ۱۴۱۴: ۳۹).

ب: قاعده لاضرر

در بحث قاعده لاضرر و ارتباط آن با موضوع این مقاله آنچه که اهمیت دارد این است که آیا قاعده لاضرر به تنهایی کافی است تا بتوان مسئولیت حقوقی استفاده ابزاری نادرست از رسانه سایبر را اثبات نمود و بتوان الزام به جبران خسارت داشت؟ برخی به این سوال پاسخ مثبت داده‌اند و عنوان داشته‌اند که این قاعده گویای حکم کلی قانون‌گذار مبنی بر جبران خسارت اعم از مادی و معنوی که به هر طریقی به دیگران وارد شده است، می‌باشد و به صورت قطع ضررهای ناشی از رسانه را نیزشامل می‌شود. در مقابل نیز برخی معتقدند که قاعده لاضرر جنبه ایجابی ندارد و نمی‌توان به استناد آن جبران ضرر را واجب تلقی نمود (شفیعی سروستانی و همکاران، ۱۳۷۶: ۲۱).

ج: قاعده غرور

اکثر فقها قاعده غرور را به عنوان یکی از مصادیق اقوی بودن سبب بر مباشر دانسته‌اند (شهیدثانی، ۱۴۱۶: ۱۶۵). در استفاده ابزاری نادرست از رسانه سایبر قاعده غرور یکی از بیشترین مصداق‌ها را دارد چرا که به‌طور مسلم این استفاده‌ها باعث می‌شود تا مخاطب به‌واسطه اطمینانی که به رسانه دارد، اقدام به انجام عملی نماید و در این حیطه متضرر و زیان دیده شود. در این حالت این امکان وجود دارد که رسانه مورد نظر را بر حسب قاعده غرور مسئول جبران خسارت وارده دانست و البته علم و قصد رسانه به نادرست بودن اخبار و اطلاعات پخش شده برای مسئول دانستن آن بر اساس قاعده غرور لازم و ضروری نیست، لذا استفاده‌هایی که در راستای تاسیس و سوء استفاده از اعتماد فرد باشد ویا مشتمل بر دروغ باشد، موجب ضمان فریب دهنده است.

۲.۲ مبانی حقوقی

مبانی حقوقی در احراز مسئولیت استفاده ابزاری نادرست از رسانه شامل موارد ذیل است:

الف: نظریه تقصیر مبنای مسئولیت حقوقی رسانه‌ها

براساس این نظریه، زیان‌دیده در حالتی می‌تواند عامل زیان را ملزم به جبران خسارت نماید که بتواند تقصیر او را ثابت نماید. به این معنا که چنانچه رفتار عامل زیان خطاکارانه باشد، محکوم به جبران خسارت وارده می‌شود و الا عمل وی مورد تأیید واقع شده و از جبران خسارت وارده معاف خواهد گردید (لوراسا، ۱۳۷۵: ۴۰).

بر مبنای این نظریه تنها دلیلی که می‌تواند مسئولیت کسی را نسبت به جبران خسارتی توجیه نماید، وجود رابطه علیت بین تقصیر او و ضرر است (کاتوزیان، ۱۴۰۰: ۱۸۳). با همین مبنا چنانچه رسانه‌ای در نتیجه عملکرد خود موجب ورود خسارتی به دیگران شود، تنها در حالتی باید خسارت وارده را جبران نماید که مقصر باشد؛ لذا بنابراین نظر، رسانه یا مدیرمسئول یک روزنامه مسئولیت ندارد. به‌نظر می‌رسد برای احراز مسئولیت حقوقی در استفاده ابزاری نادرست از رسانه سایبر برای احراز تقصیر خوانده در حالتی که قائل به نظریه تقصیر باشیم یا احراز نمودن تقصیر لازم باشد، باید با توجه به اوضاع و احوال قضیه را بررسی و با توجه به شرایط، حکم به تقصیر یا عدم تقصیر داد. دادرس باید برای احراز عنصر تقصیر به نوع رسانه دقت داشته باشد و بداند که نوع رسانه و استفاده از آن می‌تواند در وقوع تقصیر یا عدم آن مؤثر باشد. شرایط مخاطب‌های یک رسانه سایبری نیز می‌تواند در احراز تقصیر یا عدم آن مؤثر باشد، البته در مواردی که در استفاده ابزاری نادرست از رسانه فرض تقصیر شده است، زیان دیده تنها باید وارد شدن زیان و رابطه سببیت بین آن و فعل خوانده را ثابت نماید و نیازی به اثبات تقصیر خوانده ندارد و در مقابل بر عهده خوانده است که به هر وسیله‌ای که می‌تواند اثبات نماید که مقصر نبوده است. این مصداق‌ها را می‌توان شامل موارد ذیل دانست:

- در مورد رسانه‌های سایبری که کارکردشان از منظر تأثیر جغرافیایی در درجه بالایی واقع شده است، امکان وارد شدن زیان ناشی از استفاده ابزاری نادرست بسیار بیشتر است و از مسئول آن همیشه این انتظار وجود دارد که نظارت لازم را در خصوص برنامه‌ها داشته باشد چرا که زیان برگرفته از استفاده‌های نادرست قابل پیش‌بینی بوده است و عدم توجه به این مسئله یک تقصیر عرفی است.

- در مورد رسانه‌های سایبری که کارکرد آن‌ها از نظر تأثیر مردمی از اهمیت زیادی برخوردار است، شناسایی این رسانه‌ها در هر جامعه‌ای نیازمند مطالعات جامعه‌شناسی و فرهنگ‌شناسی است. در هرحال، تمام رسانه‌ها برافکار و اعمال مردم تأثیر یکسان نداشته، از شدت وضعف برخوردارند.

- در مورد رسانه‌های سایبری که درباره تندرستی و سلامت انسان‌ها به فعالیت می‌پردازند، چنانچه یک برنامه تلویزیونی یا رادیویی که در خصوص ماده‌های دارویی، آرایشی و بهداشتی مطالبی را به اطلاع عموم می‌رساند، تأثیرات زیان‌بار یک توصیه یا تجویز نادرست پزشکی و بهداشتی بر سلامتی افراد جامعه را که باید مورد توجه قرارداد در نظر نداشته باشد. این رسانه‌ها باید دقت و توجه بیشتری در برنامه‌های خودشان داشته باشند و گرنه مسئولیت‌های حقوقی آنان به وضوح قابل احراز است.

- در برنامه‌های رادیویی و تلویزیونی سایبری که بین زمان تولید یا تهیه آن‌ها تا زمان پخش آن‌ها، امکان کنترل و بازبینی وجود داشته است، اما متصدیان امر ازاین عمل کوتاهی نموده‌اند؛ این عمل برابر

با بی‌احتیاطی و مشمول ماده اول قانون مسئولیت مدنی می‌باشد. به‌نظر می‌رسد در صورتی که به زندگی و حریم خصوصی اشخاص بر اثر استفاده ابزاری نادرست از رسانه سایبر لطمه وارد شود، فرض بر این است که رسانه مقصر می‌باشد، مگر اینکه خلاف این فرض با اثبات وجود یک نفع بسیار مهم عمومی اثبات گردد.

ب: نظریه خطر و احراز مسئولیت حقوقی مخاطب

نظریه خطر را می‌توان در زمره یک نظریه موسع یا عینی برشمرد. بر مبنای این نظریه ملاک و معیار مسئولیت، رابطه سببیتی می‌باشد که بین فعالیت شخص و زیان وارده به شخص دیگر وجود دارد. بر مبنای این نظریه، منبع مسئولیت تنها تقصیری نیست که فرد مرتکب می‌گردد، بلکه حتی خطری که به وسیله فعالیت خود مخاطب ایجاد گردیده است، نیز می‌تواند منبع مسئولیت محسوب شود. اغلب افراد در ایجاد این نوع فعالیت‌ها نفعی هم دارند و به دلیل همین منافع خود را گسترش می‌دهند. این فعالیت–ها خطری را ایجاد می‌کند که به صورت بالقوه می‌تواند منجر به بروز خسارت شود. به عنوان مثال یک شرکت رسانه‌ای سایبری تبلیغاتی که از راه پخش آگهی بازرگانی به درآمدهای کلانی دست می‌یابد، باید در خطرات ناشی از فعالیت‌های رسانه‌ای خود نیز جوابگو باشد. برحسب نظریه خطر، عامل این فعالیت باید در برابر این خسارت پاسخگو باشد، حتی اگر مرتکب تقصیری نشده باشد، مسئولیت اشخاص در برابرخسارات ناشی از اشیاء تحت حفاظت آنان نتیجه همین تحول بود.

۳ ارکان تحقق مسئولیت حقوقی استفاده ابزاری نادرست از رسانه سایبر نسبت به مخاطبان و مسئولیت همزمان مخاطب

۱.۳ وجود ضرر

برای احراز مسئولیت حقوقی استفاده ابزاری نادرست از رسانه سایبر نسبت به مخاطبان و مسئولیت همزمان مخاطب باید ضرر وارد شده باشد. این ضرر امکان دارد موجب نقض در اموال یا از دست دادن منافع مسلم و یا لطمه به سلامت و حیثیت و عواطف شخص شود (یزدانیان، ۱۳۸۶: ۹۱) ضرر را باید با توجه به موقعیت و اوضاع و احوالی که خواهان دارد سنجید و نه به طور کلی؛ به عنوان مثال محروم شدن یک فروشنده جزء از چند مشتری همیشگی‌اش براثر تبلیغات گمراه کننده رسانه سایبری، برای وی زیان‌بار خواهد بود، در حالی که برای یک فروشنده بزرگ، محروم شدن از چند مشتری چندان زیان‌بار به حساب نمی‌آید.

درخصوص رسانه‌های گروهی سایبری هم مفهوم ضرر نباید چیزی متفاوت از آنچه که عنوان شد، باشد. اما از آن جایی که دامنه ایراد خسارت ناشی از اقدامات اصحاب رسانه در عموم موارد گسترده است، بنابراین

تعیین مفهوم ضرر نه تنها اهمیت بیشتری پیدا می‌نماید، بلکه موضوعی مشکل است زیرا که تشخیص مفهوم ضرر در حیطه فعالیت‌های رسانه‌ای، علی‌القاعده باید با کارکرد آن حوزه تبیین گردد. قوانین حوزه رسانه‌ها، تعریفی از مفهوم ضرر در این باره ارائه ننموده است، اما باید توجه نمود که فلسفه وجودی و قانونی هر یک از رسانه‌های جمعی از جمله رسانه‌های سایبری ماهیت و کارکرد آن و جامعه هدف آن رسانه، می‌تواند در تعیین نمودن مفهوم عرفی ضرر تأثیرگذار باشد. به عنوان نمونه خسارت ناشی از اقدام مجری سایت سایبری با خسارات ناشی از اقدامات یک خبرنگار در یک نشریه محلی، قاعدتا می‌تواند مفهوم ضرر در مقابل زیان دیده را تغییر دهد و عرف در این باره نقش مهم دارد.

استفاده ابزاری نادرست از رسانه سایبر نسبت به مخاطبان و مسئولیت همزمان مخاطب در حیطه ضرر مادی به دو صورت امکان دارد موجب احراز مسئولیت شود چرا که بعضا ممکن است این افعال موجب تلف شدن مالی شود که در حقوق از آن به عنوان اتلاف یاد می‌شود و بعضا ممکن است فعالیت‌های مذکور موجب ایجاد ضرر شود که آن را ضرر ناشی از تسبیب نامیده‌اند. قانون مدنی در ماده های ۳۲۸ و ۳۳۱ قانون مدنی به این موارد پرداخته است.[۱] در حیطه ضرر معنوی نیز شایان توجه است که دامنه شمول این نوع ضرر به ویژه در حیطه فعالیت‌های رسانه‌ای بسیار گسترده‌تر از ضررهای مادی است. به عنوان نمونه چنانچه سایت خبری سایبری اقدام به درج خبری خلاف واقعیت نماید و این خبر باعث ایراد خسارت به حیثیت و اعتبار شخص یا ارگانی شود، به نظر حکم به جبران خسارت امری مسلم باشد. در این باره باید گفت در کشورهای خارجی توجه به این نوع ضرر بسیار بیشتر از ایران است و جبران آن از موارد بسیار با اهمیت تلقی می‌شود اما متاسفانه در ایران در حیطه رسانه‌ها چه در حوزه عادی و چه سایبری درباره این نوع ضرر آن چنان که باید و شاید است مورد توجه صورت نگرفته است. البته عده‌ای امکان یا عدم جبران ضرر معنوی با پول را با اشکالاتی مواجه می‌دانند که به قرار ذیل است:

- زیان معنوی، تبلور خارجی ندارد و ملموس نمی‌باشد، بنابراین قابل اندازه‌گیری مادی نمی‌باشد وهر تصمیمی در این خصوص مبتنی بر حدس و گمان است.
- شرافت و احساسات انسانی به دلیل این که از جنس مادیات نمی‌باشد، پس قابل جبران با پول نیست و ما به ازای مادی ندارد (بهرامی احمدی، ۱۳۸۸: ۷۷).

در پاسخ به این اشکالات باید گفت در ضررهای مادی نیز همیشه تعیین نمودن میزان دقیق خسارت امکان‌پذیر نمی‌باشد و بر اساس عرف و نظریه کارشناسی میزان آن روشن می‌شود پس ضرر معنوی را هم می‌توان با استفاده از این مسئله روشن نمود. ضمنا همیشه جبران ضرر معنوی با پول نمی‌باشد و در مواردی حکم به جبران ضرر معنوی با پول امکان دارد که از منظر عقلی نیز درست باشد و قبیح تلقی نشود اما به طور

[۱] ماده ۳۲۸ قانون مدنی: هر کس مال غیر را تلف کند ضامن آن است و باید مثل یا قیمت آن را بدهد اعم از این که از روی عمد تلف کرده باشد یا بدون عمد و اعم از این که عین باشد یا منفعت و اگر آن را ناقص یا معیوب کند ضامن نقص قیمت آن مال است. ماده ۳۳۱: هر کس سبب تلف مالی بشود باید مثل یا قیمت آن را بدهد و اگر سبب نقص یا عیب آن شده باشد باید از عهده نقص قیمت آن برآید. (حقوق مذکور در این ماده انتقال به غیر است و انتقال گیرنده از نظر استفاده از این حقوق قائم مقام انتقال دهنده برای استفاده از بقیه مدت از این حق خواهد بود.)

عمده ضررهای معنوی از طریق غیرمالی جبران می‌شود. به عنوان مثال چنانچه فردی با استفاده نادرست از رسانه در محیط سایبری اقدام به دروغ‌پردازی علیه تولیدات شرکتی نمود و این موضوع موجبات لطمه‌های مختلفی برای آن شرکت گردید، ضمن محکومیت به جبران نمودن ضررهای مادی وارده، دادگاه می‌تواند او را ملزم به عذرخواهی و توضیح واقعیت در بخش‌های دیگر همان برنامه پخش شده در محیط سایبر نماید.

۲.۳ ارتکاب فعل زیان‌بار

مسئولیت حقوقی در حیطه فعالیت‌های سایبری نیز، همانند سایر موارد نیازمند ارتکاب فعل زیان بار می‌باشد. عمده افعال زیان‌بار در استفاده ابزاری نادرست از رسانه سایبر، به حیثیت و آبرو و شخصیت اشخاص باز می‌گردد و امکان دارد در برخی موارد نیز منجر به ضرر مادی به فرد گردد. به عنوان مثال در حیطه ارتکاب فعل زیان‌بار درمحدوده موضوع این مقاله می‌توان به تجاوز نمودن به حریم خصوصی مخاطب اشاره نمود که متاسفانه این عمل در ایران بارها اتفاق افتاده است و شاهد پخش مسائل بسیار خصوصی برخی افراد در محیط سایبری بوده‌ایم که مصداق بارز تجاوز به حریم خصوصی افراد تلقی می‌شود. به عنوان مثال استفاده از رسانه سایبری برای پخش عروسی یک فرد معروف نقض حریم خصوصی بوده و به طور قطع منتشر کننده آن مرتکب فعل زیان‌بار شده است و دارای مسئولیت حقوقی خواهد بود. بعضا نیز ممکن است در رسانه سایبر اقدام به هتک حرمت گردد که منجر به از بین رفتن آبروی فرد یا حیثیت و جایگاه خانوادگی وی شود که در این باره نیز مسئولیت قابل احراز است. این هتک حرمت دارای مصداق‌های متعددی است که از آن جمله می‌توان به افتراء، توهین و نشر اکاذیب اشاره نمود. به عنوان مثال افتراء در رسانه‌های سایبری می‌تواند موجب مسئولیت کیفری و مدنی رسانه خاطی باشد. البته در عمده موارد هر دو نوع مسئولیت شامل حال فرد می‌شود. مثلا چنانچه گوینده‌ای در رسانه سایبر یکی از مسئولان کشور را مفسد اخلاقی معرفی نماید نه تنها مسئولیت کیفری دارد بلکه دارای مسئولیت حقوقی نیز خواهد بود (آقائی‌نیا، ۱۳۸۴: ۳۶). توهین و نشر اکاذیب هم بر همین رویه است.

۳.۳ رابطه سببیت

سومین رکن مسئولیت مدنی وجود رابطه سببیت می‌باشد؛ یعنی برای محقق شدن مسئولیت حقوقی باید بین فعل زیان‌بار و وجود ضرر، رابطه سببیت وجود داشته باشد؛ یعنی ورود ضرر به یک شخص اعم از حقیقی یا حقوقی که توانایی انجام مسئولیت را دارد، قابل انتساب باشد تا آثار مسئولیت بر وی تحمیل گردد. در حوزه فعالیت‌های رسانه‌ای نیز باید برای مسئول شناختن رسانه سایبر یا فرد متخلف، باید فعل زیان‌بار و ضرر حادث شده رابطه سببیت احراز گردد. رسانه‌های سایبری همانند دیگر اشخاص حقوقی می‌توانند دارای شخصیت حقوقی باشند و این موضوع در غالب موارد در حالت احراز رابطه سببیت، مسئولیت را بر عهده رسانه و شخصیت حقوقی او قرار خواهد داد نه شخص حقیقی مگر این که رابطه سببیت روشن‌کننده مسئولیت شخص حقیقی مانند خبرنگار، مجری و... باشد. قانون تجارت درباره شخصیت حقوقی بخشیدن به

موسسه‌های دولتی مانند رسانه‌های دولتی عنوان می‌دارد که موسسات و تشکیلات دولتی و بلدی به محض ایجاد و بدون احتیاج به ثبت دارای شخصیت حقوقی می‌شوند. حال اگر رسانه‌ای سایبری دولتی به حساب بیاید، به محض ایجاد و بدون نیاز به ثبت در مرجع ثبت، دارای شخصیت حقوقی می‌شود، اما در حالتی که رسانه‌ای برای مقاصد غیرتجاری تشکیل شود. براساس ماده ۵۸۴ قانون تجارت، از تاریخ ثبت در دفتر خاصی که قوه قضائیه تعیین کرده است، دارای شخصیت حقوقی می‌شود. بنابراین براساس ماده‌های یاد شده، عمده رسانه‌ها اعم از عادی و رسانه‌ای از قبیل روزنامه، تلویزیون، نشریات جاری کشور دارای شخصیت حقوقی بوده و در حالت ایراد خسارت به اشخاص، می‌توان خسارت وارده را از آن‌ها در حالت وجود شرایط مسئولیت، مطالبه نمود.

۴ نتیجه‌گیری

رسانه‌های سایبری امروزه عضو غیر قابل انکاری از زندگی بشر هستند که با استناد به محتوای پیام خود بر وجوه مختلف اقتصادی، اجتماعی، فرهنگی و آموزشی جامعه اثر می‌گذارند. فعالیت رسانه‌های مذکور نیز بعضا امکان دارد سبب ایراد ضرر مادی یا معنوی به اشخاص حقیقی یا حقوقی شوند. از این رو مسئولیت حقوقی استفاده ابزاری نادرست از رسانه سایبر نسبت به مخاطبان ومسئولیت همزمان مخاطب در مقابل زیان‌هایی که ممکن است بر اثر فعالیت آن‌ها بر اشخاص مختلف وارد شود، امری ضروری است. یافته‌های این مقاله نشان می‌دهد که در زمینه مسئولیت مذکور، قاعده ضمان و جبران خسارت مبنای اصلی می‌باشد که البته پراکندگی و عدم وجود انسجام یا جامعیت لازم قوانین موضوعه در باب رسانه‌های سایبری مانع از این می‌شود که این رسانه‌ها، الزامات لازم را شناخته و آن را رعایت نمایند یا دادرس قادر باشد منابع مسئولیت آن‌ها را پیدا نموده و التزام به جبران خسارت برپایه آن‌ها را بنا نماید. همچنین روشن شد که انواع ضرر ناشی از این نوع مسئولیت حقوقی اعم از مادی و معنوی است و با توجه به مطالب در مجموع این نتیجه روشن است که رسانه‌های سایبری به دلیل کارکردهای متفاوت و عمومی بودن، چنانچه شخصی را اعم از حقوقی یا حقیقی یا دولتی یا خصوصی متحمل ضرر و زیان اعم از مالی و معنوی نماید باید درصدد جبران زیان وارده برآیند. ضمنا پیشنهاد می‌شود با توجه به این که هدف از وضع قواعد مسئولیت حقوقی، جبران خسارت وارده به افراد می‌باشد، بنابراین ضروری است تا اشخاص مسئول در برابر زیان دیده به علت کثرت افراد فعال در حوزه رسانه مشخص گردد. به عنوان نمونه مقنن در مورد انعکاس خبر کذب در یک رسانه سایبری، چه کسی یا کسانی را در برابر زیان دیده و به چه صورت مسئول جبران خسارت می‌داند؟ مدیرمسئول، سردبیر، مجری، کارگردان، تهیه کننده و... اشخاصی هستند که در قالب شخص حقیقی می‌توانند مسئول قرار گیرند، علاوه بر این که خود رسانه سایبری نیز در عمده موارد دارای شخصیت حقوقی است و بنابر قانون ممکن است مسئول خسارت وارده باشد. آیا زیان زنندگان بنابرماده ۱۴ قانون مسئولیت مدنی در برابر زیان دیده مسئولیت تضامنی خواهند داشت یا خیر؟ لازم است این موارد به صراحت روشن و تفکیک گردد.

مراجع

[۱] آقائی‌نیا، حسین (۱۳۸۴). جرائم علیه اشخاص، چاپ اول، تهران، انتشارات میزان.

[۲] بهرامی احمدی، حمید (۱۳۸۸). مسئولیت مدنی، چاپ اول، تهران، انتشارات میزان.

[۳] شفیعی سروستانی، ابراهیم و همکاران، قانون دیات و مقتضیات زمان، چاپ اول، انتشارات مرکز تحقیقات استراتژیک ریاست جمهوری.

[۴] کاتوزیان، ناصر (۱۴۰۰). حقوق مدنی، ایقاع، نظریه عمومی، ایقاع عمومی، چاپ هشتم، تهران، انتشارات گنج دانش.

[۵] کاتوزیان، ناصر (۱۴۰۰). قواعد عمومی قراردادها، چاپ سی و نهم، تهران، انتشارات میزان.

[۶] کاتوزیان، ناصر (۱۳۸۶). الزام‌های خارج از قرارداد (ضمان قهری)، مسئولیت مدنی، چاپ ششم، تهران، انتشارات میزان.

[۷] لوراسا ، میشل (۱۳۷۵). مسئولیت مدنی، چاپ اول، مترجمان: حسین صفایی و محمد اشتری، تهران، انتشارات حقوقدان.

[۸] مبین، حجت (۱۳۸۷). نظریه قابلیت استناد به‌عنوان مبنای مسئولیت مدنی در فقه امامیه و حقوق ایران با مطالعه تطبیقی در حقوق فرانسه، تهران، دانشگاه امام صادق.

[۹] مصطفوی، مصطفی (۱۳۸۴). احسان، منبع مسئولیت، سال دوم، مجله فقه و حقوق.

[۱۰] یزدانیان، علیرضا (۱۳۸۶). حقوق مدنی، قواعد عمومی مسئولیت مدنی، چاپ اول، جلد اول، تهران، انتشارات میزان.

[۱۱] الجبعی العاملی، زین الدین بن علی (شهیدثانی) (۱۴۱۶). مسالک الافهام فی تنقیح شرائع الاسلام، الطبعه الاولی، قم، مؤسسه المعارف الاسلامیه.

[۱۲] حسینی سیستانی، علی (۱۴۱۴). قاعده لاضرر و لاضرار، الطبعة الاولی، قم، مکتب آیت الله العظمی السید سیستانی.

[۱۳] حسینی المراغی، میرعبدالفتاح (۱۴۱۷). العناوین، الطبعة الاولی، جلد دوم، قم، مؤسسه النشر الاسلامی.

[۱۴] علامه حلی، حسن بن یوسف بن علی مطهر (۱۴۱۸). قواعد الاحکام، قم، المکتبة المرتضویة لاحیاء الآثار الجعفریة.

[۱۵] مکارم شیرازی، ناصر (۱۴۱۷). القواعد الفقیهة، الطبعة الثالثة، قم، مدرسة الامام امیرالمومنین (ع).

پایش کتابشناختی علم و فناوری در حوزه امنیت سایبری

علیرضا رضوانیان[۱]، سید مهدی وحیدی پور[۲]

[۱]استادیار، گروه مهندسی کامپیوتر، دانشگاه علم و فرهنگ، تهران
rezvanian@usc.ac.ir
[۲]استادیار، دانشکده مهندسی برق و کامپیوتر، دانشگاه کاشان، کاشان
vahidipour@kashanu.ac.ir

چکیده

تردیدی نیست که فراوانی استفاده از منابع دیجیتالی و پدیدار شدن فناوری‌های نوظهور در زندگی روزانه افراد رو به افزایش است و همچنین گستردگی محتوا و اطلاعات متنوع، امکان نفوذ و سوء استفاده از افراد و سازمان‌ها را روز به روز افزایش می‌دهد. مطالعات و پژوهش‌های گوناگونی نیز برای حفاظت از منابع دیجیتالی و ارائه راه‌کارهای امنیت سایبری از جنبه‌های مختلف پژوهشی تا صنعتی توسط پژوهشگران و صنعتگران در سال‌های اخیر ارائه شده است. بنابراین، با توجه به اهمیت موضوع امنیت در فضای سایبری، در این مقاله پایش کتابشناختی علم با بررسی مقالات منتشر شده و پایش فناوری با بررسی ثبت اختراعات، مورد بررسی قرار گرفته است. برای بررسی مقالات از منابع نمایه‌شده موجود در پایگاه علمی اسکپوس استفاده شده است و برای بررسی ثبت اختراعات از داده‌های موجود در لنز استفاده شده است. در نهایت گزارش‌های مختلف به تفکیک آمار به‌دست آمده از زوایای مختلف و بر اساس شاخص‌های مختلف ارائه شده است.

کلمات کلیدی: امنیت سایبری، تحلیل کتابشناختی، پایش علم، پایش فناوری.

۱ مقدمه

امروزه با توجه به گسترش کاربردهای دیجیتالی در زندگی بشری، خیلی از نیازهای روزانه انسان‌ها توسط سیستم‌های دیجیتالی با استفاده از کامپیوترهای شخصی، تبلت، موبایل و حسگرهای هوشمند به صورت از راه دور و بدون نیاز به حضور فیزیکی انجام می‌پذیرد. این امر از یک طرف سهولت و مزایای فراوان را برای افراد فراهم آورده و از طرف دیگر افزایش اهمیت امنیت سایبری در سیستم‌های دیجیتالی مختلف مورد استفاده در زمینه‌های اجتماعی، فرهنگی، کاری، تجاری، سازمانی، اداری و کاربردهای مختلف روزانه بشری را نشان می‌دهد [۱]. در این مقاله پس از معرفی مفاهیم اولیه از امنیت سایبری و ارائه آمار متنوعی از اهمیت امنیت در فضای سایبری، در نهایت پایش کتابشناختی علم و فناوری در حوزه امنیت سایبری ارائه شده است.

۲ امنیت سایبری

امنیت سایبری شامل مجموعه‌ای از فناوری‌ها و فرآیندهای طراحی شده به منظور از حفاظت از کامپیوتر، سیستم، شبکه، برنامه‌های کامپیوتری، موبایل و داده‌ها در برابر حملات دیجیتالی است. به طور معمول هدف این نوع از حملات، دسترسی غیرمجاز، تغییر، تخریب و یا از بین بردن اطلاعات مهم و حیاتی، استخراج پول از کاربران، یا ایجاد خلل و توقف در فرآیندهای یک کسب و کار است. امروزه طراحی، پیاده‌سازی و اجرای اقدامات موثر امنیت سایبری در عمل چالش برانگیز است، زیرا تعداد فراوانی از دستگاه‌های دیجیتالی نسبت به جمعیت افراد جامعه وجود دارد و مهاجمان با نیت‌های مختلف هر روز با نوآوری و ابتکارات بیشتری دست به حملات و خرابکاری خود می‌زنند [۲]. یکی از رویکردهای موفقیت آمیز در امنیت سایبری ایجاد چندین لایه حفاظت در کامپیوتر، شبکه، برنامه یا داده‌های موبایل است تا حداقل امنیت لازم فراهم شود. در یک سازمان، کاربران، فرایندها و فناوری‌ها بایستی همگی به صورت یکپارچه به یکدیگر مرتبط باشند تا دفاع موثری در برابر حملات اینترنتی و سایبری ایجاد کنند [۳].

برخی توصیه‌ها برای کاربران، سازمان‌ها و فناوری در ادامه ذکر شده است:

- کاربران بایستی ضرورت اصول امنیتی داده‌های اساسی مانند انتخاب رمز عبور قوی، مراقبت از پیوست‌ها در ایمیل و پشتیبان گیری از داده‌ها را درک کنند. در این مورد آموزش دوره‌ای کاربران می‌تواند مفید باشد.
- سازمان‌ها بایستی چارچوبی برای چگونگی مقابله با حملات سایبری داشته باشند. یک چارچوب مناسب می‌تواند سازمان‌ها را هدایت کند. بدین صورت که چگونه سازمان می‌تواند حملات را شناسایی کند، سیستم‌ها را محافظت کند، تهدیدات را شناسایی و پاسخ دهد، و نسبت به حملات رخ داده محفوظ باشند.
- فناوری برای استفاده توسط سازمان‌ها و افراد نیازمند مجهز شدن به ابزارهای امنیتی مستحکم است تا از حملات سایبری محافظت کند. در حوزه فناوری، سه بخش اصلی باید محافظت شوند: دستگاه‌های پایه‌ای مانند رایانه، دستگاه‌های هوشمند، روتر، شبکه و فناوری رایج مورد استفاده برای محافظت از این موارد شامل فایروال‌های نسل بعدی، فیلترسازی سرویس‌های نام دامنه، حفاظت از نرم‌افزارهای مخرب، نرم‌افزار آنتی‌ویروس و راه‌حل‌های امنیتی ایمیل است.

۱.۲ امنیت سایبری از دیدگاه آمار

براساس آمار بدست آمده از حوادث مرتبط با امنیت سایبری در سال ۲۰۲۲ در سطح جهان، حدود ۱۶۰۰۰ حادثه در صنایع مختلف از ضعف‌های مربوط به امنیت سایبری دچار خسارت شده‌اند.[۱] به عنوان مثال تخمین زده شده است که آژانس اعتباری Equifax در سال ۲۰۱۹ حدود ۵۷۵ میلیون دلار خسارات ناشی از امنیت سایبری را داشته است.[۲] گزارش تفکیکی صنایع خسارت دیده مرتبط با امنیت سایبری در سال ۲۰۲۲ در جدول ۱ فهرست شده است. بنابراین امروزه وجود سیستم تشخیص نفوذ امنیت سایبری به منظور اجتناب از

[1] https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size
[2] https://www.statista.com/topics/1731/smb-and-cyber-crime/

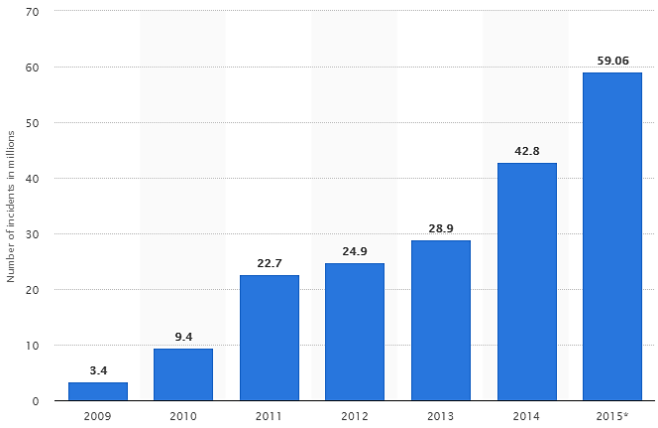
تهدیدات و حملات مختلف برای سازمان‌ها نفوذگران ضروری و حیاتی است [۴].

جدول ۱: گزارش تفکیکی صنایع خسارت دیده مرتبط با امنیت سایبری در سال ۲۰۲۲

مقیاس صنعت / نام صنعت	بزرگ	کوچک	نامشخص	مجموع
اقامتی	۲	۴	۲۴۸	۲۵۴
اداری	۱۴	۸	۱۶	۳۸
کشاورزی	۵	۱	۶۰	۶۶
ساخت و ساز	۱	۷	۷۹	۸۷
آموزش	۱۵	۶۳	۴۱۸	۴۹۶
سرگرمی	۳	۱۳	۴۱۶	۴۳۲
مالی	۳۰	۷۰	۱۷۲۹	۱۸۲۹
سلامت	۱۵	۲۸	۴۷۹	۵۲۲
اطلاعات	۱۱۰	۴۵	۱۹۵۰	۲۱۰۵
مدیریت	۰	۱	۸	۹
ساخت	۲۴	۳۷	۱۷۵۳	۱۸۱۴
معدن	۰	۲	۲۳	۲۵
سایر خدمات	۲	۷	۱۳۴	۱۴۳
خدمات حرفه ای	۵۴	۱۷۶	۱۱۶۶	۱۳۹۶
مدیریت دولتی	۱۱۰	۸۷	۳۰۷۳	۳۲۷۰
املاک	۵	۱۵	۶۳	۸۳
خرده فروشی	۴۴	۶۲	۲۹۸	۴۰۴
عمده فروشی	۲۵	۱۳	۳۱۱	۳۴۹
حمل و نقل	۶	۱۲	۹۹	۱۱۷
خدمات رفاهی	۲۲	۴۲	۳۲	۹۶
ناشناخته	۲	۱	۵۱۹۹	۲۷۷۷
مجموع	۴۸۹	۶۹۴	۱۵۱۲۹	۱۶۳۱۲

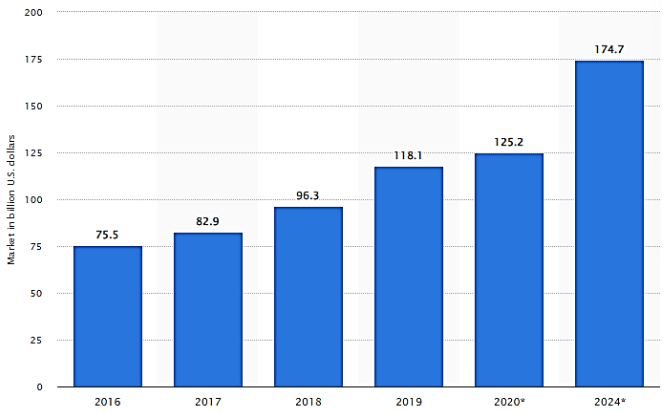
با توجه به افزایش فزاینده تعداد کاربردهای برخط و الکترونیکی مورد استفاده توسط کاربران، وجود سرویس‌های فراوان برخط، وجود داده‌های زیاد و ترافیک بالا، نوع تهدیدات و حملات به حالت پیشرفته‌تر، فزاینده‌تر و هدف‌دارتری درآمده است که اغلب مراکز داده‌ای، خدماتی، دولتی، صنعتی، صنایع دفاعی و نظامی به طور هدفمند و مستمر توسط نفوذگران مورد حمله قرار می‌گیرند [۵]. آمار افزایشی تعداد حوادث مرتبط

با امنیت سایبری در سطح جهان در بازه زمانی ۲۰۰۹ تا ۲۰۱۵ در شکل ۱ ارائه شده است.



شکل ۱: آمار افزایشی تعداد حوادث مرتبط با امنیت سایبری در سطح جهان در بازه زمانی ۲۰۰۹ تا ۲۰۱۵

بدین ترتیب روش‌های سنتی با استفاده از تکنیک‌های آماری، مبتنی بر فراوانی و مبتنی بر الگو صرفاً برای شناسایی حملات قدیمی و تکراری مناسب هستند ولی به منظور شناسایی و جلوگیری از تهدیدات سایبری نوین، پیشرفته و پیچیده امروزی عملاً ناکارآمد محسوب می‌شوند [۶]. بنابراین استفاده از روش‌های هوشمند و نوین براساس داده‌کاوی و شناسایی الگوهای مهم در حملات حائز اهمیت است. پیش‌بینی شده است که تا سال ۲۰۲۴ بیش از ۱۷۴ میلیارد دلار از سهم بودجه به تکنولوژی‌های امنیت اطلاعات اختصاص یابد.[۳] روند افزایشی این تخصیص بودجه از سال ۲۰۱۶ و پیش‌بینی برای سال‌های بعد از آن تا ۲۰۲۴ در شکل ۲ گزارش شده است.



شکل ۲: آمار تخصیص بودجه در فناوری امنیت اطلاعات برای سال‌های ۲۰۱۶ تا ۲۰۲۴

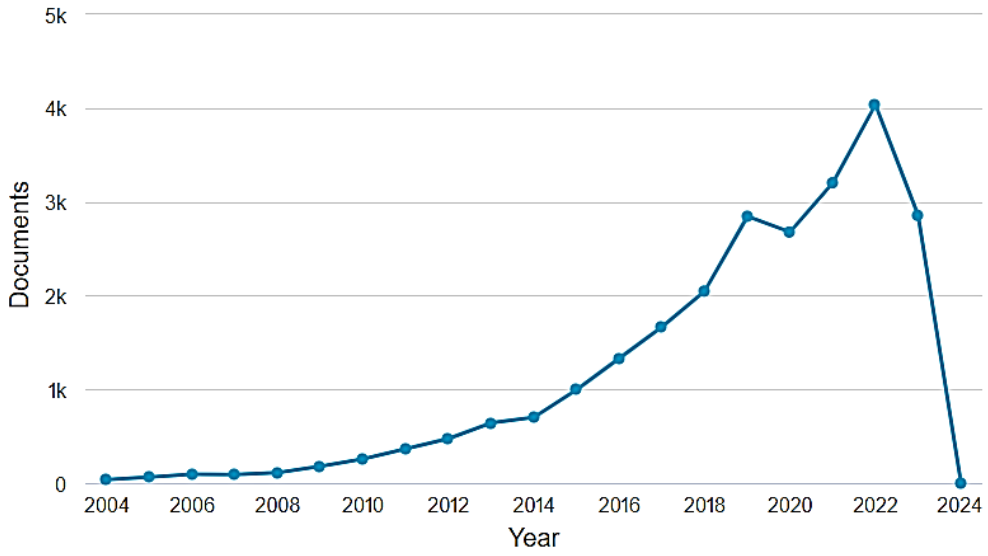
[3] https://www.statista.com/statistics/640141/worldwide-information-security-market-size/

۳ روش پژوهش

فرآیند پژوهش به صورت کتابشناختی [۷] انجام شده است؛ این فرایند شامل استخراج منابع مطالعاتی مرتبط با کارهای انجام شده در رابطه با امنیت سایبری است که در آن تحلیل کتابشناختی از دو منظر انتشار مقالات به عنوان پایش علمی و ثبت اختراعات به عنوان پایش فناوری مورد بررسی قرار گرفته است. انتشار مقالات اهمیت موضوع در حوزه علمی و شکل‌گیری حوزه‌های پژوهشی حال و آینده را مشخص می‌کند. ثبت اختراعات، اهمیت تجاری شدن موضوع در حوزه‌های کاربردی و صنعتی را مشخص می‌کند، بدین مفهوم که نیاز به حل یک مشکل در قالب یک پژوهش به یک فناوری کاربردی قابل خرید و فروش مبدل شده است.

۱.۳ پایش مقالات علمی

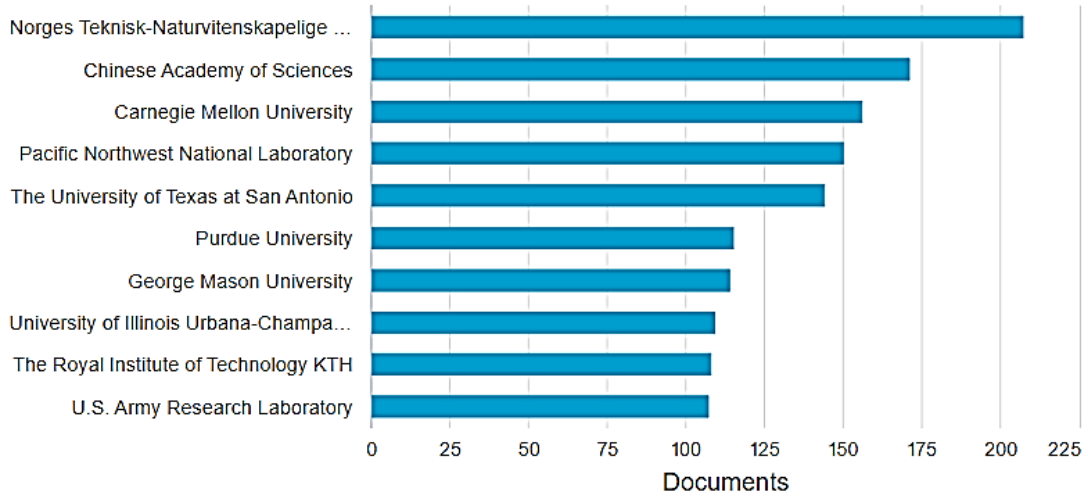
در بخش مقالات منتشر شده با موضوع امنیت سایبری، براساس نتایج پایگاه اسکپوس[۴] ، تعداد ۲۴۶۸۳ مقاله توسط پژوهشگران مختلف در مجلات و کنفرانس‌های مختلف از سال ۲۰۰۴ تا ۲۰۲۴ به چاپ رسیده است. در شکل ۳، نمودار فراوانی تعداد مقالات منتشر شده با موضوع امنیت سایبری به تفکیک سال نمایش داده شده است، که روند فراوانی تعداد مقالات به صورت افزایشی است و این روند از حدود سال ۲۰۱۸ از شتاب بیشتری برخوردار است. علت پایین بودن این آمار برای سال ۲۰۲۳ به این دلیل می‌تواند باشد که اطلاعات مربوط به این سال هنوز کامل نشده است و در انتهای سال، فراوانی مربوط به این سال تکمیل خواهد شد.



شکل ۳: نمودار فراوانی مقالات منتشر شده با موضوع امنیت سایبری به تفکیک سال از ۲۰۰۴ تا ۲۰۲۴

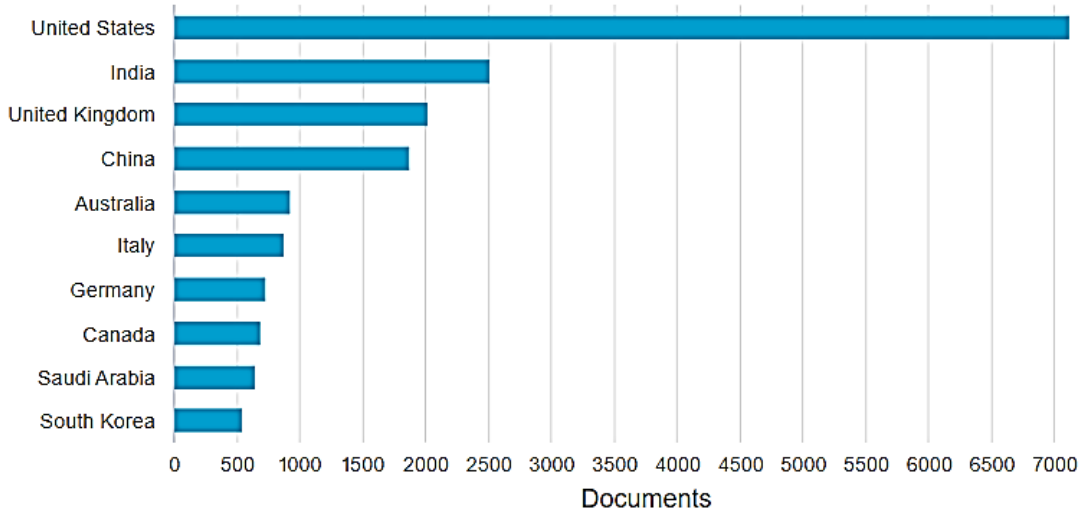
مهم‌ترین مراکز علمی، تحقیقاتی و دانشگاهی پیشتاز که در این حوزه مشغول به فعالیت هستند، در شکل ۴ نشان داده شده است. در رتبه‌های بالا، دانشگاه‌هایی از کشورهای نروژ، چین، آمریکا و سوئد قرار گرفته‌اند.

[۴] نتایج مستخرج از پایگاه دانش https://www.scopus.com در ماه سپتامبر سال ۲۰۲۳



شکل ۴: مهمترین مراکز علمی، تحقیقاتی و دانشگاهی پیشتاز در حوزه امنیت سایبری

آمار مربوط به ۱۰ کشور برتر که در این حوزه فعالیت‌های فراوانی را در حوزه تحقیقاتی دارند، در شکل ۵ گزارش شده است.

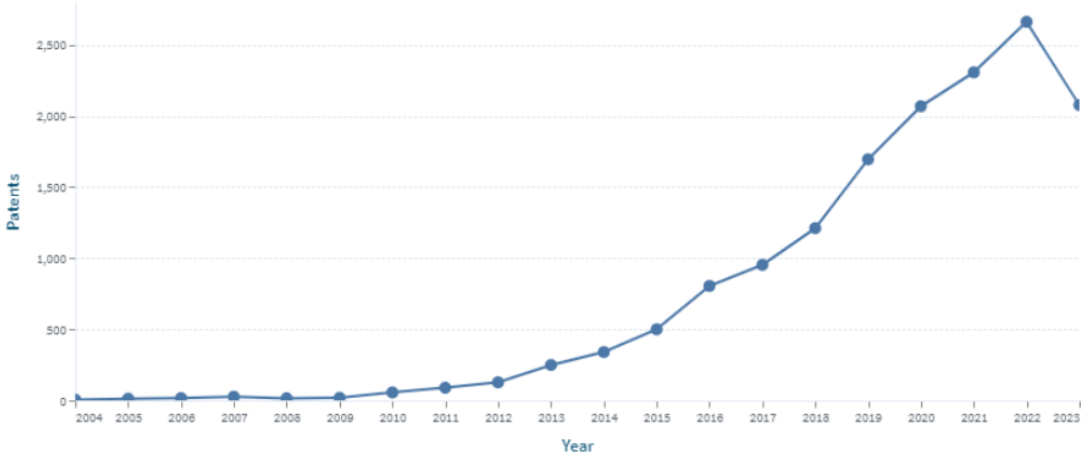


شکل ۵: کشورهای برتر در حوزه تحقیقات پیرامون موضوع امنیت سایبری

۲.۳ پایش فناوری

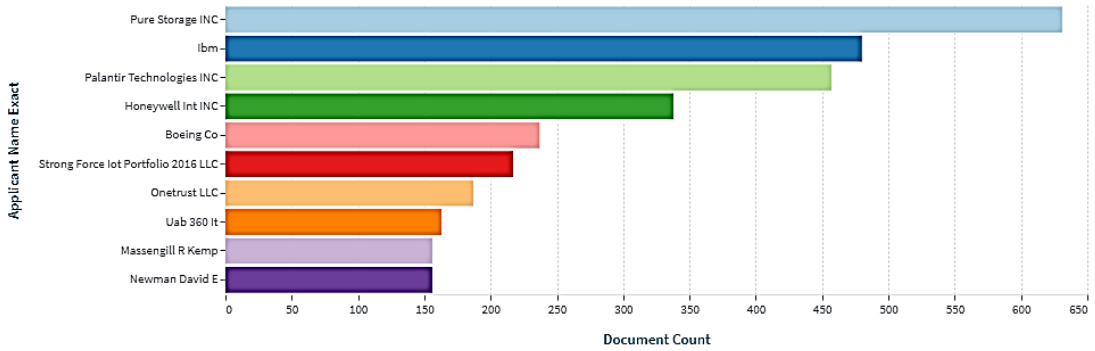
برای پایش فناوری به موارد مربوط به ثبت اختراع توجه می‌شود. بنابراین، در بخش اختراعات ثبت شده با موضوع امنیت سایبری، براساس نتایج پایگاه ثبت اختراعات، تعداد ۱۵۲۳۱ ثبت اختراع توسط مخترعین مختلف در دفاتر ثبت اختراع در کل جهان از سال ۲۰۰۴ تا ۲۰۲۳ به ثبت رسیده است. در شکل ۶، نمودار

فراوانی تعداد اختراعات به ثبت رسیده با موضوع امنیت سایبری به تفکیک سال نمایش داده شده است که روند فراوانی تعداد اختراعات ثبت شده به صورت افزایشی است و این روند از حدود سال ۲۰۱۸ از شتاب بیشتری برخوردار است. علت پایین بودن این آمار برای سال ۲۰۲۳ به این دلیل مربوط می‌شود که اطلاعات مربوط به این سال هنوز کامل نشده است و در انتهای سال، فراوانی مربوط به این سال تکمیل خواهد شد.



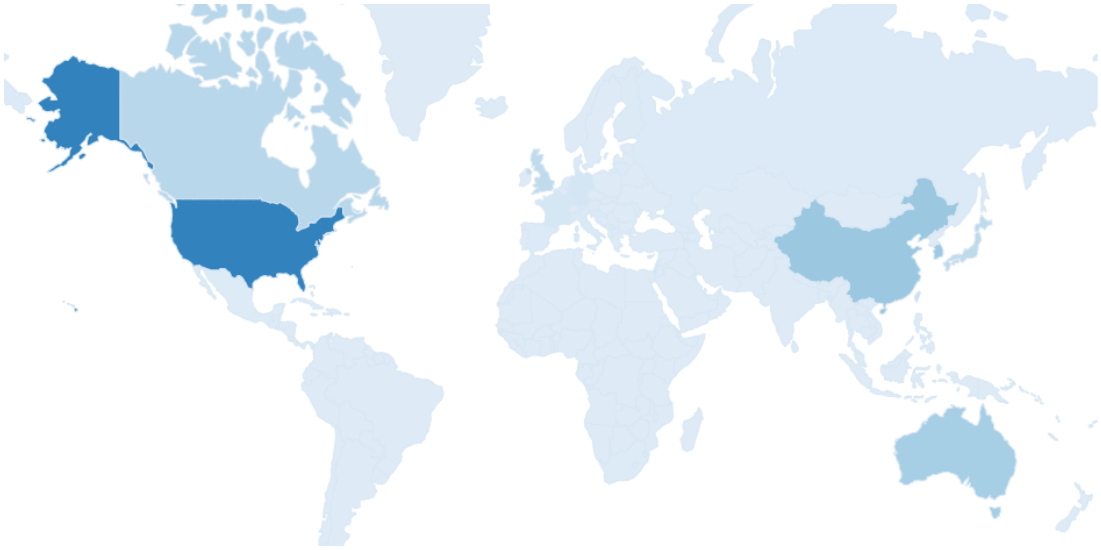
شکل ۶: فراوانی تعداد اختراعات ثبت شده پیرامون موضوع امنیت سایبری به تفکیک سال از ۲۰۰۴ تا ۲۰۲۳

مهمترین سازمان‌ها، موسسات، مراکز علمی و تحقیقاتی پیشتاز در حوزه تجاری سازی موضوع امنیت سایبری که مشغول به فعالیت هستند، در شکل ۷ نشان داده شده است که به طور عمده مربوط به موسسات و سازمان‌هایی از آمریکا هستند.



شکل ۷: مهمترین سازمان‌ها، موسسات، مراکز علمی و تحقیقاتی پیشتاز در حوزه تجاری سازی موضوع امنیت سایبری

از دیدگاه تجاری سازی موضوع امنیت سایبری، نقشه جهانی کشورهای برتر از نظر ثبت اختراع، پیرامون موضوع امنیت سایبری، در شکل ۸ نمایش داده شده است.



شکل ۸: نقشه جهانی کشورهای برتر در حوزه تجاری‌سازی از نظر ثبت اختراع پیرامون موضوع امنیت سایبری

۴ نتیجه گیری

با توجه به افزایش وابستگی و گسترش کاربردهای الکترونیکی در زندگی بشری، خیلی از نیازهای روزانه انسان‌ها توسط سیستم‌های الکترونیکی با استفاده از موبایل به صورت از راه دور و بدون نیاز به حضور فیزیکی انجام می‌پذیرد. این امر از یک طرف سهولت و مزایای فراوانی را برای بشر فراهم آورده است اما از طرف دیگر منجر به افزایش احتمال خسارات ناشی از تهدیدات، حمله و نفوذ در فضای سایبری شده است. در این مقاله، علاوه بر بیان اهمیت موضوع امنیت سایبری، پایش کتابشناختی علم با بررسی مقالات منتشر شده و پایش فناوری با بررسی ثبت اختراعات مورد بررسی قرار گرفت.

مراجع

[1] L. Yuchong, and Q. Liu. “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments”, Energy Reports, vol. 7, pp. 8176-8186, 2021.

[2] Z. Zhang, H. Ning, F. Shi, F. Farha, X. Y. Xu. J. Xu. F. Zhang, K, R. Choo, “Artificial intelligence in cyber security: research advances, challenges, and opportunities”, Artificial Intelligence Review, vol. 55, pp. 1029-1053, 2022.

[3] M. E. Whitman, H. J. Mattord. Principles of information security. Cengage learning, 2021.

[4] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, “Security and Privacy in Cyber-Physical Systems: A Survey of Surveys”, IEEE Design , Test of Computers, vol. 34, no. 4, pp. 7–17, 2017.

[5] Zuech, T. M. Khoshgoftaar, and R. Wald, “Intrusion detection and Big Heterogeneous Data: a Survey”, J. Big Data, vol. 2, no. 1, p. 3, 2015.

[6] Y. Harel, I. Ben Gal, and Y. Elovici, “Cyber Security and the Role of Intelligent Systems in Addressing its Challenges”, ACM Trans. Intell. Syst. Technol., vol. 8, no. 4, pp. 1–12, 2017.

[7] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, W. M. Lim, “How to conduct a bibliometric analysis: An overview and guidelines”. Journal of business research, vol. 133, pp. 285-296, 2021.

سایبرنتیک دروازه نوگشوده علم و تکنولوژی

زهرا بیگلری[۱]، زهرا عزتی نیا[۲]

[۱]دانشجوی کارشناسی ارشد، مؤسسه شناخت
biglari110@gmail.com
[۲]دانشجوی دکتری مدیریت رسانه، دانشگاه آزاد اسلامی واحد علوم تحقیقات، تهران
pasia529@yahoo.com

چکیده

ارتباط ناگسستنی علم و تکنولوژی و سیر تاریخی کاربردی‌شدن علم در زندگی بشری زمینه‌ساز پیدایش مفهوم تکنوساینس گردید. به گونه‌ای که می‌توان شیء تکنیکی را برون‌داد همکاری دانشمندان و مهندسین به‌شمار آورد. فناوری فراگیر که در عصر کنونی با گسترش فناوری اطلاعات و هوش مصنوعی چهره‌ای بی‌بدیل به نمایش گذاشته است مسبب چالش‌ها و فرصت‌های تازه‌ای است؛ به‌گونه‌ای که ساحت فکر و اندیشه‌ی انسانی را نیز تحت سیطره‌ی القائات و ادراکات جدیدی از مفاهیم قرار داده است. فرایند تلاش‌های گروهی سیستم علمی، اکنون به جایگاهی رسیده که گونه‌ای جدید از سیستم بازخورد و کنترل به نام «سایبرنتیک» را معرفی نموده است. سایبرنتیکِ برآمده از انبوه اطلاعات و دستگاه‌های محاسباتی، نرم‌افزاری فراهم آورده که هدف نهایی آن پیدایش یک ماشین به تقلید از انسان نیست، بلکه به‌عکس، انسان سخت‌افزاری است که نرم‌افزار او در این سیستم علمی پردازش می‌شود؛ به‌گونه‌ای که پیچیدگی دنیای علم می‌تواند بازخورد و بازنمایی همه اهداف خود را در رفتار انسانی نظاره کند. مقاله پیش رو می‌کوشد با روش توصیفی-تحلیلی رابطه فناوری و گام‌های نخستین در شبکه علمی را برای دستیابی به دانش سایبرنتیک تبیین کند. برای این منظور نخست سیر تحول فناوری از ابزاری در دست انسان تا خلق ماشینی دارای قدرت تفکر و تکلم را بررسی می‌کند. سپس نشان می‌دهد که این ایده دکارتی در نسخه‌های جدید خود چگونه به تسلط ماشین بر کالبد انسان از راه کنترل قوه تفکر و تکلم می‌پردازد.

کلمات کلیدی: فناوری، شیء تکنیکی، انسان، سایبرنتیک.

۱ مقدمه

علم و تکنولوژی از گذشته تاکنون پیوند ناگسستنی و تأثیر اجتناب‌ناپذیر در حیات انسان داشته‌است. تکنولوژی مقدم بر علم و در تمامی فرهنگ‌های بشری نقش داشته است. کاربردی‌کردن علم با ابزار تکنولوژی، ابعاد گوناگونی برای زندگی انسان ایجاد کرده که نوع مواجهه و ارتباط انسان و تکنولوژی در طول تاریخ

گواه این موضوع است. اختراع ابزارهای گوناگون، از اهداف علم کاربردی برای ایجاد تغییرات سودمند در جهان است. تاریخچه گسترش تکنولوژی، ارتباط متقابل ابزار با فرهنگ جوامع و درهم‌تنیدگی ادراک انسان با ابزارهای ساخته‌شده توسط فناوری که در این مقاله تحت عنوان شیء تکنیکی یاد می‌شود، موجب به‌وجودآمدن مسائل گوناگون در ساحت فکر و اندیشه شده است. فناوری‌های علمی در سنّت پزشکی یا عملکرد دانش در اختراع ماشین چاپ، موتور بخار، الکتریسیته، و فناوری اطلاعات هر یک طرحی اثرگذار در تاریخ تکنولوژی به نمایش می‌گذارند. مفاهیم مرتبط به فناوری با تغییر نگرش علمی در سنت ارسطویی و نیوتنی با توجه به تغییر متافیزیک و پیش‌زمینه علمی، موجب تفاوت تئوریک در نگرش به فناوری گردیده و واکاوی و بررسی این مفاهیم در شناخت کارکرد و برهم‌کنش فرهنگ و فناوری قابل توجه است.

گسترش فناوری، یکی از ویژگی‌های عصر حاضر است که در عصر اطلاعات و ارتباطات با گسترش فناوری اطلاعات و هوش مصنوعی، مسبب فراهم آمدن فرصت‌ها و چالش‌های متفاوت شده است. تکامل فناوری‌های مختلف که روزمره شدن استفاده از ابزارهای متکی به تکنولوژی‌های ملزوماتی را به همراه خواهد داشت.

انسان، کاشف علم و خالق اولین ابزار تکنیکی است. با گذشت زمان و در طول تاریخ همواره پیشرفت تکنولوژی متکی به کشفیات علمی و نگاه بشر به علم و فناوری بوده است. اولین جرقه‌های رشد فناوری مرهون تدبر در قوانین و الگوهای ساخت ماشین‌های اولیه است. رشد علمی تمدن بشری به معنای تصدیق گزاره‌های موجه بنابر تعریف ارسطویی، هرگز بدون ارشمیدس و فیثاغورث بارور نمی‌شد.

شیء تکنیکی محصول همکاری دانشمندان و مهندسین است و مفهوم علم و تکنولوژی را آن‌چنان به هم نزدیک کرده که از علم و تکنولوژی با اصطلاح تکنوساینس یاد می‌شود. سیر تاریخی تکنولوژی علاوه بر نقشی که در کاربردی کردن علم در زندگی داشته، تأثیر هم‌زمان در ادراکات و القائات معانی در ذهن بشر داشته است. از کاربردی شدن اولین فناوری تا عصر حاضر، شامل ماشین‌های ساده، دستگاه چاپ، موتور بخار، الکتریسیته، یا فناوری‌های ارتباطات و اطلاعات و هوش مصنوعی، هر یک علی‌رغم تأثیر فوق‌العاده در رفاه و افزایش بازده در حوزه‌های مرتبط داشته‌اند. جامعه انسانی نیز در استفاده از تکنولوژی، روش‌های مختلفی را آزموده و با گذشت زمان، سیطره شیء تکنیکی در جوامع انسانی قابل مشاهده است و مواجهه ذهنی اندیشمندان و جامعه انسانی نسبت به شیء تکنیکی، در آثار اندیشمندان مورد توجه قرار گرفته است.

این مقاله به بررسی سیر تحول تکنولوژی در سه بخش می‌پردازد؛ در بخش اول به تعریف تکنولوژی و تولید فناوری و تلاش اول انسان از تولید ابزار تا دستیابی به تکنیک‌های گوناگون و رشد تکنولوژی تا تولید ماشین به دست مهندسین و دانشمندان می‌پردازد. در بخش دوم به بررسی رابطه فکر و تکنولوژی در اندیشه بشری اشاره می‌شود و هدف از این بخش برجسته کردن ایده‌های فلسفی و طرح‌های دانشمندان و نقش این مداخلات فکری در هدایت شیء تکنیکی ساخت دست مهندسین به سمت اهداف انتزاعی دانشمندان می‌پردازد. درنهایت در بخش سوم با پرداختن به تعریفی کوتاه از سایبرنتیک، به زمینه‌های پیدایش این دانش به‌عنوان ثمره نگرش شبکه‌ی علمی پست مدرن به ابزار و تکنیک و ایده‌ای جمعی برای کاربرد شیء تکنیکی در شبکه‌ی معنایی منجر به تولد سایبرنتیک متبلور می‌شود.

۲ پیشینه تحقیق

یکی از مقالاتی که موجب شکل‌گیری ایده‌ی اولیّه این نوشتار شد، «تحلیل فلسفی فناوری و نقش آن در شکل‌گیری فضای مجازی» [۸] است. یافته‌های این پژوهش نشان می‌دهد آن چیزی که یک شیء را به سطح تکنولوژیک می‌رساند، ساختاربندی و عقلانیّت موجود در آن است که هم با ضرورت‌های زیستی مواجه می‌شود و هم نیازهای جدید برای انسان تولید می‌کند و در یک فرایند دیالکتیکی، برای یافتن نسبت خود با تولید اندیشه پیشروی می‌کند. همچنین بررسی رابطه فکر با فناوری نشان می‌دهد نگرش گشتالتی به فناوری با نسبت میان انسان و فناوری رابطه دارد؛ این نسبت را دانش خاص فناوری با اتکای مفهومی خود به دانش پست مدرنی تبیین می‌کند. دانشی که انعطاف‌پذیر، نسبی و شکننده است و مناسبتی با روش‌های عقلانی مدرنیسمی ندارد؛ همین دانش در فضای مجازی که فراگیرترین شکل رویدادهای فنّاورانه است و بیش از هر چیز بیانگر ماهیّت تکنولوژی است، به‌صورت وانمودگی، دولایگی و توسعه شبکه‌ای حضور دارد.

همچنین مقاله «ارائه تعریف فضای سایبری و فضای مجازی بر پایه مبانی علم فضای سایبرنتیک» [۵] که با بررسی فضای سایبر ضمن تشریح مفاهیم پایه‌ای فضای سایبری مانند سیستم پیچیده، سایبرنتیک، فضای سایبری و فضای مجازی به ارائه تعاریف برگزیده از مفاهیم بالا پرداخته است.

از سوی دیگر، کتابی از نوربرت وینر به نام «Cybernetics: or Control and Communication in the Animal and the Machine» به تشریح زمینه‌های شکل‌گیری دانش سایبرنتیک در سیر تحولی فناوری پس از انباشت و تراکم دانش و فناوری و بازخورد نظرات دانشمندان پرداخته است که زمینه‌ساز دیگر نگارش این مقاله شد.

این مقاله می‌کوشد با استفاده از نتایج تحقیقات گذشته درباره فناوری و جمع‌آوری شواهد، پیدایش شبکه‌ای از ارتباطات علمی و فنی در بستر علم پست مدرن را دست‌مایه پژوهش قرار دهد و سعی دارد با برجسته‌سازی ایده‌های فلسفی در بازتولید تکنیک و فناوری، مروری بر پیدایش دانش سایبرنتیک در این فضا داشته باشد.

۳ فناوری و مهندسی

تکنولوژی به معنای به‌کاربردن دانش برای مقاصد عملی، ساختن چیزها و به‌دست‌آوردن نتایج سودمند برای انسان می‌باشد [۱]. کاربردی کردن علم، ریشه در تلاش‌های علمی بشر و همکاری فناوران و دانشمندان در طی سنت‌های مختلف علمی از ارسطو تا نیوتن و طلیعه عصر کوانتوم است. گذر از عصر ارسطویی علم با تمام تفاوت‌های آن نسبت به سنت علمی نیوتنی، در طول دوره‌ای بیش از دو هزار سال، همواره با افت‌وخیز فکری همراه بوده است.

علی‌رغم کاربرد گسترده و روزمره ابزارآلات مکانیک و ادراک اصول کمی نهفته در عملکرد ابزار حتی پیش از عصر ارسطو و آگاهی ارسطو و شاگردانش به این اصول، که به نگارش و تدوین ایده‌های ارسطو از مفاهیم محوری همچون صورت، بالقوگی، علت‌ها، امور کلی و مفاهیم دیگر منجر شده است [۲]. طبقه‌بندی اجتماعی یونان باستان، مانع ادغام علم و فن به معنای امروزی بوده است، چرا که فرومایگانی مانند صنعتگران

در معرض دشنام و ناسزا قرار داشته و ارسطو «کارگر افرازمند» را از جرگه شهروند خارج می‌شمارد [۳].

روند گسترش تکنولوژی در اروپا هم‌زمان با دوران مدرنیسم آغاز شد. علم مدرن در میان عامه مردم رواج یافت و همگانی شدن علم، دستاورد دوران مدرنیته به شمار رفت [۳]. تغییر اندیشه در اروپا از ناچیز شمردن فعالیت مکانیکی به سمت ارج نهادن به تلاش کارگران آغاز شد و نویسندگان در جامعه‌ای که مهندسی را توهین تلقی می‌کرد به عصر تمجید دست‌ها و دست‌ساخته‌های انسان وارد شدند. آثار جوردانو برونو، دفاع از هنرهای مکانیکی در آثار و مقالات مهندسان و ماشین‌سازان سده شانزدهم و تفکرات بیکن و دکارت نشانه اولین پیوندها بین علم و ابزار و ظهور عصر جدیدی از همگانی شدن علوم و تکریم صنعتگران است.

دورانی آغاز می‌شود که دانش‌های جدید و رو به گسترش با طراحی ماشین‌ها، ساخت و تولید ابزارهای جنگی، احداث استحکامات، کانال‌ها، سدها، آبگیرها، و استحصال فلزات در کارگاه‌های معدنی ایجاد می‌شوند. مهندسان، صنعتگران و هنرمندان صنایع‌دستی روزبه‌روز از وجهه و اعتبار بیشتری برخوردار می‌شوند و با اقشار ممتازی مانند طبیبان و استادان دانشگاه هم‌ردیف می‌شوند و حتی آراء و اعمال آنان را به محک تجربه و آزمون سپردند [۳].

۱.۳ انسان و ماشین

در دیدگاه رنه دکارت، دستگاه مکانیکی یا ماشین تفاوتی با انسان یا حیوان ندارد. حیوان همان ماشین است و تمایز میان ماشین‌های دارای حیات در دو کارکرد ویژه ماشینی به نام انسان نهفته است. این دو تمایز عبارت‌اند از تفکر و تکلم. پس راه تبدیل ماشین مکانیکی به انسان، اعطای قدرت تفکر و تکلم به شیء تکنیکی است.

اندیشه دکارتی، ماشینی را متصور می‌سازد که اندام و عضو دارد و برای انجام وظایف به ابزار ارگانیک خاص نیازمند است، اما ماشینی با همه اندام‌ها که با فکر و عقل انسانی عمل کند امری محال به نظر می‌رسید. دکارت دانایی و خردمندی یا سازگاری با محیط را استعدادی می‌داند که در هیچ ماشینی نهاده نشده است. از سوی دیگر قدرت تکلم و زبان محاوره انسان نیز همین‌طور است، اگر چه در اندیشه دکارت می‌توان ماشینی ساخت که به تکرار برخی کلمات بپردازد و یا در برابر کلماتی که ادا می‌شوند، از خود واکنش نشان دهد، اما برای چنین ماشینی امکان ندارد که «به تنظیم و انشای کلمات بپردازد و همانند انسان به جملات گفته شده به طور ذهنی پاسخ دهد.» [۳] و اگر انسان نوعی ماشین تلقی شود، طبیعتاً می‌تواند هدفی برای تسلط و ابزاری تکنولوژیک به شمار رود. چنان‌که تمدن غربی همواره در صدد تسلط بر ابزار برمی‌آید.

بر اساس اینکه تکنولوژی نوعی آلت دانسته شود یا نه، موضع ایدئولوژیکی متفاوتی به وجود می‌آید. به گفته هایدگر، اگر تکنولوژی ابزار باشد ما تلاش می‌کنیم آن را از لحاظ فکری دست‌آموز خود کنیم و بر آن مسلط شویم؛ اما هایدگر معتقد است که تعریف ابزاری، ماهیت حقیقی تکنولوژی را برای ما آشکار نمی‌کند. تکنولوژی یک فرآورده است و هر فرآورده‌ای ریشه در انکشاف دارد؛ لذا تکنولوژی نوعی انکشاف است. انکشاف یا استتارزدایی ما را به ساحت حقیقت رهنمون می‌کند. بودریار نیز بدون پرداختن به بحث حقیقت، ساخت اشیاء را نوعی خودشکوفایی و تظاهر انسانی می‌داند و می‌گوید: «انسان با آفرینش و ساخت اشیاء، از طریق تحمیل یک صورت یعنی فرهنگ که به طبیعت جوهری دیگر می‌بخشد، خود را برملا می‌سازد.» اما مسئله‌ای

که وجود دارد و دیدگاه هایدگر را نسبت به تکنولوژی دیدگاهی منفی می‌کند این است که از نظر او در ماهیت تکنولوژی جدید نوعی تعرض به طبیعت نهفته است. او از واژه «گشتل» برای تبیین این مطلب استفاده می‌کند و این واژه را در معنای نامرسوم آن به‌عنوان «امر گردآورنده‌ی تعرض‌آمیزی که انسان را مخاطب قرار می‌دهد و به معارضه می‌خواند» به کار می‌برد. طبیعی است که میان استفاده از فناوری برای تسلط و تصرف بر طبیعت و ارتباط با آن به مثابه گسترش وجود انسان یا به تعبیر برایان آرتور «امتداد طبیعت» ما تفاوت هست؛ لذا باطن انسان آن نوعی از فناوری را که به نابودی و مرگ می‌انجامد، نمی‌پذیرد. اما آنچه انسان را به ابهام و تکاپو می‌کشاند این است که نوعی احساس تردید نسبت به فناوری و تبعات آن در حیات انسان وجود دارد که در حال رشد است و از دغدغه انسان نسبت به طبیعت برمی‌خیزد؛ زیرا انسان با محتوای فناوری آشنایی فراوان و با اصول آن آشنایی اندکی دارد [۸].

۴ رابطه فکر و فناوری

در خصوص ارتباط فکر و فناوری دو الگو وجود دارد که ساخت ابزار و هر اختراعی در قالب آن شکل می‌گیرد:

۱. **بر اساس هدف.**

در این الگو ساخت ابزار تابع فکر است و عزیمت از هدف و نیاز به‌سوی پدیده است.

۲. **بر اساس اثر.**

در این الگو فکر تابع ساخت ابزار است و عزیمت از پدیده به‌سوی هدف و نیاز است.

برایان آرتور این دو الگو را به این صورت تقریر می‌کند که گاه اختراع از سر زنجیره آغاز می‌شود؛ از یک نیاز یا یک هدف خاص و به دنبال قاعده‌ای می‌گردد که بتواند آن نیاز را برآورده کند، و گاه اختراع از سر دیگر آغاز می‌شود؛ یعنی از پدیده یا اثر، و معمولاً از یک کشف جدید، آنگاه کاربردی برای آن در نظر می‌آید. از نظر کانت، فیلسوف عقل‌گرای قرن هجدهم، جهان خارج باید مطابق الگوهای ذهنی ما تنظیم گردد. اما اندیشه پست مدرنی که نسبت فکر و فناوری را در بستر تلقی غیر کُل‌گرایانه از هستی می‌انگارد، در تقابل با دیدگاه کانتی، اندیشه را تابع ابزار می‌داند. ماکس وبر، یکی از بزرگ‌ترین جامعه‌شناسان غربی، معتقد است که تخصص فنی علت عقلانی شدن انسان است، نه برعکس؛ «فن یکی از عوامل تعیین‌کننده عقلانی شدن فزاینده جامعه‌ها در همه زمینه‌های اقتصادی، دینی، یا هنری بوده است.»

در نسبت میان فکر و فناوری، رابطه میان تولیدکننده و مصرف‌کننده‌ی فکر و فناوری اهمیت به‌سزایی دارد. تولیدکننده و مصرف‌کننده‌ی فناوری هر دو صاحب فکرند اما فکر در یکی مقدم و در دیگری مؤخر از ابزار است. تولیدکننده‌ی فناوری عموماً در الگوی نخست عمل می‌کند و مصرف‌کننده تقریباً همواره در الگوی دوم. یعنی مصرف ابزار موجب ساخت فکر در او می‌شود. این وضعیت در عموم کشورهای جهان سوم شایع است. در واقع، چون فناوری و ابزار توسعه تولیدکننده بر مصرف‌کننده غلبه دارد، دانش او که مرکب از علم و فرهنگ است هم غلبه پیدا می‌کند.

تولیدکننده و مصرف‌کننده هر دو مصرف‌کننده‌ی ابزارند؛ اما به دلیل اینکه در تولیدکننده الگوی اول غالب است و در مصرف‌کننده الگوی دوم، نفس عمل مصرف، قادر است هویت مصرف‌کننده را متحول، متکامل، یا متزلزل کند. زیرا اگر گفته برایان آرتور درست باشد که «نداشتن فناوری به معنای نا انسان بودن است، فناوری بخش هنگفتی از انسان بودن ماست»، خروجی مصرف‌کننده و تولیدکننده بعد از مصرف ابزار متفاوت خواهد بود؛ چون دارایی آن‌ها متفاوت است [۸].

۵ سایبرنتیک و دوران معاصر

مارکس مقتضیات یک تکنولوژی را در ارتباط و قرابت با عادات روحی و روانی یک جامعه می‌داند و اندیشمندان زیادی مانند او معتقدند با بررسی خصلت‌ها و شرایط صنعتی و تکنولوژیکی یک عصر و حتی از تفاوت‌های تکنولوژی‌های مختلف می‌توان به تفاوت‌های فرهنگی یک جامعه با جوامع دیگر پی برد.

در حال حاضر شیء تکنیکی سیطره خود را در عرصه‌های اقتصادی و زندگی روزمره گسترش داده تا در روزگار ما سخن از ظهور و گسترش ارتباطات الکترونیکی و عبور از مراحل فرهنگ شفاهی، دست‌نویس و چاپی به میان آید [۴]. شاید یکی از ویژگی‌های عصر ارتباطات الکترونیک، پردازش تراکنش‌های الکترونیک و ردیابی پیام‌های ارتباطی و اثرات آن در تحولات روزمره سیاسی، اجتماعی و اقتصادی و قابلیت رهگیری این تحولات باشد.

ثبت تراکنش‌های بانکی و اقتصادی در روزگار کنونی اهمیتی بیش از گذشته می‌یابد، حتی اگر تلاش بر پنهان‌سازی ارتباطات سرلوحه کار سیاستمداران و یا ذی‌نفعان در ارتباطات و قدرت‌های سیاسی قرار داشته باشد. به‌عنوان مثال، کشف دریافت رشوه بایدن از چین در اظهارات رقبای حزبی براساس اطلاعات تراکنش‌های بانکی که صاحب حساب بانکی را فردی ساکن خانه بایدن معرفی کرده است، یکی از نمونه‌های اهمیت اطلاعات و تأثیر تکنولوژی در جهان سیاست محسوب می‌شود [۱۰]. یا در تازه‌ترین رویارویی اطلاعاتی ایران و اسرائیل [۱۱]، درز اطلاعات ۷۰ هزار پرونده قضایی اسرائیل نشان‌دهنده‌ی تبعیض بین شهروندان عرب و غیرعرب در نظام قضایی اسرائیل است که دسترسی به این اطلاعات براساس بازخوردگیری و تحلیل داده‌ها از اسناد امکان‌پذیر است.

اگر بپذیریم که در گذشته چنین پرونده‌هایی قابل کشف بود، سرعت کشف و نشر و پردازش اطلاعات در آن‌ها به مراتب طاقت‌فرسا و زمان‌بر بود و چه‌بسا اثرگذاری اندکی در محیط پیرامون خود داشت و این‌چنین است که حرکت روزگار را به سمتی هدایت می‌کند که بال‌زدن پروانه‌ای در اقیانوس آرام طوفانی در اقیانوس هند را پدید آورد و گویا فضای سایبر همچون بازخورد توپ روی صفحه میز پینگ‌پنگ باشد. صفحه‌ای که میز آن در سرتاسر دنیای وب گسترده شده و اینترنت اشیاء و موج اطلاعات کنش و واکنش را به ابعاد فرهنگی، سیاسی، اجتماعی و اقتصادی می‌گستراند.

این رویکرد با مطالعاتی گره خورده است که تا پیش از سال ۱۹۴۷م نامی بر آن نهاده نشده بود. اگرچه سیستم فلسفه علم غرب گویا طرحواره این دانش جدید را از مدت‌ها قبل تنظیم کرده بود و دانشمندان زیادی در ثبت نام سایبرنتیک برای این دانش تلاش کرده بودند. اگرچه اولین مقاله مهم و مرتبط با دانش

سایبرنتیک توسط کلرک ماکسول در سال ۱۹۶۸ منتشر شد و در این مقاله در خصوص مکانیسم‌های بازخورد و سیستم حاکمیتی صحبت شده بود. این حوزه مطالعاتی جدید که طوفانی از ایده‌های گوناگون را به همراه داشت و پای دانشمندان ریاضی را به مطالعات زیست‌شناسی باز کرد، امیدی را در سر دانشمندان و فیلسوفان غربی می‌پروراند که عبارت بود از ساخت ماشین محاسباتی با استفاده از منطق ریاضی و ماده زمینی با هدف اختراع ابرماشین هوشمندی که شاید ایده خدایی انسان را جامه‌ی عمل بپوشاند. چنانکه در منابع اولیه معرفی سایبرنتیک می‌خوانیم: «ما تصمیم گرفته‌ایم که کل حوزه تئوری کنترل و ارتباط را، چه در ماشین و چه در حیوان، با نام Cybernetics که از یونانی $\kappa\upsilon\beta\varepsilon\rho\nu\eta\tau\iota\kappa\eta$ یا steersman تشکیل می‌دهیم، بنامیم.» [۹] واژه سایبر مشتق از کلمه‌ای یونانی است که به سیستم هدایت کشتی اشاره می‌کند و یادآور این واقعیت است که موتورهای فرمان یک کشتی از اولین و بهترین شکل‌های توسعه‌یافته مکانیسم‌های بازخورد هستند [۹].

تولد سایبرنتیک مرهون تلاش دانشمندانی است که به ویژه در حوزه بازخوردهای شناختی، مطالعه قشر مغز، مکانیک، مکانیسم‌های کنترل و بازخورد، منطق ریاضی و فلسفه علم و در مراحل بعد نظریه‌های ارتباطات و ... تلاش می‌کردند.

اگرچه قدمت واژه سایبرنتیک بیشتر از تابستان ۱۹۴۷ نیست، اما استفاده از آن برای اشاره به دوره‌های قبلی توسعه این رشته راحت است. از سال ۱۹۴۲ یا حدود آن، توسعه این موضوع در چندین جبهه پیش رفت. ابتدا، ایده‌های مقاله مشترک بیگلو، روزن‌بلوث و وینر توسط دکتر روزن‌بلوث در جلسه‌ای که در سال ۱۹۴۲ در نیویورک و تحت نظارت بنیاد جوزیا میسی برگزار شد، منتشر شد و به مشکلات بازداری مرکزی در سیستم اعصاب اختصاص یافت. از جمله حاضران در آن جلسه، دکتر وارن مک‌کالوچ، از دانشکده پزشکی دانشگاه ایلینویز بود که قبلاً با دکتر روزن‌بلوث و دکتر رابرت وینر در تماس بود و علاقه‌مند به مطالعه سازماندهی قشر مغز بود.

در این مرحله عنصری وارد می‌شود که به طور مکرر در آن رخ می‌دهد و اگر در تاریخچه سایبرنتیک – تأثیر منطق ریاضی، بخواهیم یک قدیس حامی را برای سایبرنتیک از تاریخ علم انتخاب کنیم، باید لایب‌نیتس را انتخاب کنیم. فلسفه لایبنیتس بر دو مفهوم نزدیک به هم متمرکز است: مفهوم نمادگرایی جهانی و حساب استدلال. نمادهای ریاضی و منطق نمادین امروزی از این‌ها نشأت می‌گیرند. اکنون، همان‌طور که تحلیل محاسباتی خود را به مکانیزه‌شدن از طریق چرتکه و ماشین‌های محاسباتی رومیزی به ماشین‌های محاسباتی فوق‌سریع امروزی می‌رساند، نسبت حساب لایب‌نیتس نسبت به ماشین شبیه اجزای محاسباتی ماشین نسبت به استدلال منتج از دستگاه (ماشین) است. در واقع، خود لایب‌نیتس، مانند سلف خود پاسکال، به ساخت ماشین‌های محاسباتی علاقه‌مند بود و همان انگیزه فکری که منجر به توسعه منطق ریاضی شد درعین‌حال به مکانیزه‌شدن ایده‌آل یا واقعی فرایندهای فکری منجر شده است.

۱.۵ تکنولوژی ارتباطات

رسانه به‌عنوان یکی از ابزارهای تکنیکی در عصر ارتباطات نقش ویژه‌ای در تبادلات و تعاملات فناورانه به عهده دارد. اگر رسانه را حامل پیام به‌عنوان اصلی‌ترین عنصر عصر اطلاعات بدانیم، کانون توجه نظریه‌های

ارتباطات، آثار پیام‌های ارتباطی و بررسی تأثیر محتوای ارتباطی یا پیام بر نگرش و رفتار مخاطبان است.

مخاطب در این سیستم، بخشی از نگاه تجربی به انسان است که با نظریه‌های اجتماعی – رفتاری در قالب نظریه‌های کارکرد پیام‌های ارتباطی و نظریه تأثیر پیام‌های ارتباطی و یا سنت دیگری که موسوم به نظریه‌های فرهنگی است و متکی بر جامعه‌شناسی زبان‌شناسی یا مطالعات ادبی و انسان‌شناسی به مطالعه آثار ارتباطات بر جوامع انسانی می‌پردازد [۷].

در چنین ساختاری است که انسان و پیام‌های رد و بدل شده چیزی به جز واکنش عصبی و الکترونیکی تلقی نمی‌شود و عبور و مرور ماشینی پیام با کمک فرستنده و گیرنده‌ها به‌عنوان تراکنش‌های الکترونیکی دستگاه‌های ارتباطی شامل شبکه‌ای از کامپیوترهای خانگی، گوشی‌های موبایل، ابزارهای الکترونیکی، کامپیوترهای کوچک متصل به ابزارهای خانگی و شبکه‌های اجتماعی و اینترنت اشیاء ثبت می‌شود.

در نگاه دورکیم، رسانه جامعه را به مثابه سیستم واحد شامل ارگانیسم زنده به تصویر می‌کشد که ضمن تأکید بر نظم و انسجام اجتماعی بر اهمیت ارتباط بین اجزا در فرایند حفظ و تحول جامعه و نقش این ارتباط در تولید و بازتولید اجتماع و توافق در مورد مسائل و حفظ تعادل در جامعه تأثیرگذار هستند [۷].

۲.۵ تسلط بر ابزار انسانی

براساس یافته‌های تجربی، بسیاری از رازهای زیستی بر دانشمندان گشوده شده است. تجمیع اطلاعات زیست‌شناختی، مکانیک، الکترونیک، روان‌شناسی، ارتباطات، جامعه‌شناختی، روان‌شناسی و... توسط ابزاری که روزگاری در خدمت انسان قرار داشت، موجب بازشدن افق‌های نو برای دانشمندان حوزه‌های مطالعاتی مختلف شده است و سؤالی که حجم انبوه اطلاعات به ذهن اندیشمندان متبادر می‌شود این است که آیا همان‌گونه که دکارت از ماشین متکلم سخن می‌گفت، می‌توان انسان متکلم را به ماشینی تبدیل کرد که فرایندهای اندیشه و سخنگویی آن با ابرماشینی قابل کنترل تحت نظارت قرار گیرد؟ و در مرحله بعدی، آیا امکان سرایت این وضعیت به جامعه و اجتماعی بزرگ‌تر از افراد انسانی وجود دارد؟

شاید پاسخ این سؤال با حجم فزاینده اطلاعاتی از پروژه‌هایی مانند پروژه ژنوم، نظریه پیام، نظریه‌های ارتباطات و نظریه کنترل و الگوریتم‌های زیستی و سایر نظریات تجربی قابل دسترسی باشد.

به عبارتی، شاید یک ریاضی‌دان نیازی به مهارت انجام آزمایش فیزیولوژیک نداشته باشد؛ اما باید توان ادراک، ارائه انتقاد و پیشنهاد در فیزیولوژی را داشته باشد و رؤیای وجود یک مؤسسه از دانشمندان با قابلیت درک، تحلیل و انتقاد از انبوه دانش در رشته‌های مختلف و تحت کنترل افسران نظامی [۹]، اندیشه‌ای بود که پیش از جنگ جهانی دوم در اذهان اندیشمندان غربی پرورده می‌شد. به نظر می‌رسد قدرت محاسبات رایانه‌ای به کمک عملی شدن این ایده آمده باشد.

اکنون اکثریت عظیم محاسبات وسایل محاسباتی غیرانسانی روی شبکه‌های عصبی وسیع موازی انجام می‌گیرد که بیشترین بخش آن بر مبنای مهندسی معکوس مغز انسان استوار است. بسیاری از بخش‌های تخصصی مغز انسان رمزگشایی شده و الگوریتم‌های وسیع موازی آن‌ها شناخته شده است. تعداد مناطق تخصصی که به صدها می‌رسد، بیشتر از آن چیزی است که بیست سال قبل پیش‌بینی می‌شد.

اکنون مجموعه‌ای از اعضای پیوندی عصبی وجود دارد که جهت بهبود قابلیت‌های درک و تعبیر سمعی

و بصری، حافظه و قوه استدلال در دسترس همگان قرار دارد [۶].

۶ جمع‌بندی

حجم انبوه اطلاعات و قابلیت الگوریتم‌های زیستی و قدرت تحلیل هوش مصنوعی، امروزه قابلیت استفاده از کالبد انسانی به‌جای ماشین مدنظر دکارت را فراهم نموده است، با این تفاوت که دکارت به ساختن ماشین مشابه انسان و برنامه‌ریزی تفکر و تکلم برای آن می‌اندیشید و اکنون می‌توان به نفوذ و هک اندیشه و تکلم و بهره‌برداری از این قابلیت انسانی و اجتماعی با کمک تکنولوژی جدید امیدوار بود.

سیر تلاش‌های گروهی سیستم علمی اکنون به جایگاهی راه یافته که نوعی جدید از سیستم بازخورد و کنترل تحت عنوان سیستم سایبر متولد شده است. این سیستم که پس از سال ۱۹۴۷ کتابی از نوربرت وینر به نام سایبرنتیک معرفی شده است، برآمده از انبوه اطلاعات و دستگاه‌های محاسباتی است که اکنون نرم‌افزاری را فراهم آورده که قابلیت تولید انسانی جدید را به اذهان دانشمندان متبادر کرده است.

این قابلیت که یادآور تلاش‌های فرانکشتاین برای خلق انسانی از کالبد مرده و بی‌جان با استفاده از نیروی مادی است، در دل سعادتی که بیکن در نهاد تجربه می‌کاوید خودنمایی می‌کند. گویا رشته‌های اصلی اعصاب جهان به‌صورت اندامی واحد درآمده و جهان علم تمام دانش رو به افزونی خود را در مورد هر یک از این رشته‌ها در دل پایگاه‌های داده و ماشین‌های هوشمند برای بازتولید قدرت تکلم و منطق انسانی ذخیره کرده است . اما این بار هدف نهایی تولید ماشینی به تقلید از انسان نیست، بلکه اکنون انسان سخت‌افزاری است که نرم‌افزار آن در این سیستم علمی پردازش می‌شود.

در این سیستم که با دانش سایبرنتیک یا در واقع ابرپروژه سایبرنتیک هدایت می‌شود، تمام پیچیدگی دنیای علم می‌تواند بازخورد و بازنمایی اهداف خود را در رفتار انسان نظاره‌گر باشد؛ چرا که بخش منطق و شناخت آن با منطق ریاضی و بررسی بازخوردهای طبیعی رفتار انسان و بخش کارکردی و اجتماعی آن با علوم ارتباطات و علوم اجتماعی و به ویژه رسانه به‌عنوان ابزاری تکنولوژیک اتفاق می‌افتد.

مراجع

[۱] استیونستن، لزلی. هزار چهرهٔ علم؛ ترجمه: میثم محمدامینی؛ انتشارات نشر نو، تهران، ۱۳۹۸.

[۲] دویت، ریچارد. جهان‌بینی‌ها؛ ترجمه: احسان ثنایی اردکانی؛ انتشارات ققنوس، تهران، ۱۳۹۷.

[۳] روسی، پائولو. تاریخ پیدایش علوم جدید در اروپا؛ ترجمه: بهاءالدین بازرگانی گیلانی؛ انتشارات سروش، تهران، ۱۳۹۳.

[۴] پستمن، نیل. تکنوپولی، تسلیم فرهنگ به تکنولوژی؛ ترجمه: صادق طباطبایی؛ انتشارات اطلاعات، تهران، ۱۳۹۰.

[۵] خوشحال‌پور، احسان. ارائه تعریف فضای سایبری و فضای مجازی بر پایه مبانی علم سایبرنتیک؛ مجموعه مقالات نخستین کنفرانس ملی فضای سایبر، دانشگاه تهران، ۱۴۰۱.

[۶] کورزویل، ری. عصر ماشین‌های معنوی؛ ترجمه: سیمین موحد؛ نشر پیکان، تهران، ۱۳۹۶.

[۷] مهدی‌زاده، سید محمد. نظریه‌های رسانه؛ انتشارت همشهری، تهران، ۱۳۹۹.

[۸] سرمدی، محمدرضا. تحلیل فلسفی فناوری و نقش آن در شکل‌گیری فضای مجازی؛ نشریه علمی فناوری آموزش، شماره ۴، پاییز ۱۳۹۸.

[9] Wiener, Norbert. Cybernetics: or Control and Communication in Animal and the Machine; the M.I.T. PRESS, Cambridge, Massachusetts, 1985; p.27.

[10] http://fna.ir/3f9su8

[11] http://mehrnews.com/x336yk

مدل‌سازی رفتاری مصرف منابع در بخش رمزنگاری فایل‌ها در باج‌افزارها

مهران گرمه‌ء[۱]، رجبعلی سجادیان فر[۲]، محمد شاه‌پسندی[۲]

[۱]استادیار گروه مهندسی کامپیوتر دانشگاه بجنورد
m.garme@ub.ac.ir
[۲]دانشجوی کارشناسی ارشد مؤسسه آموزش عالی اشراق
{sajadianfar,m.shahpasandi}@ub.ac.ir

چکیده

امروزه باج‌افزارها بدترین چالش مدیران و مسئولین فناوری اطلاعات سازمان‌ها هستند. سازندگان محصولات ضدویروس و تحلیل‌گران بدافزار دشواری‌های زیادی برای شناسایی و کالبدشکافی یک بدافزار پیچیده متحمل می‌شوند. یکی از نکات کلیدی موجود در این فرآیند، سرعت تشخیص و پاسخگویی به یک حمله باج‌افزاری می باشد که این امر گاهی سرنوشت‌ساز بوده و علاوه بر مقدار داده از دست رفته و سرعت انتشار باج‌افزار، بر امکان رمزگشایی اطلاعات نیز تأثیرگذار خواهد بود. با توجه اینکه امکان دور زدن تکنیک‌های سنتی شناسایی همواره وجود دارد، استفاده از روش‌های نوین تشخیص باج‌افزار کمک شایانی به مدافعین این حوزه خواهد کرد. این پژوهش با رویکرد بررسی میزان مصرف منابع سیستم (پردازنده، حافظه و دیسک) نمونه‌هایی از پنج خانواده از باج‌افزارها با تاریخ انتشار حداکثر سه سال گذشته انجام گرفته است که در نهایت با تحلیل نتایج به‌دست آمده، رفتار باج‌افزارها نسبت به نحوه مصرف منابع، مدل‌سازی و گزارش شده است. نتایج به‌دست آمده از این تحقیق نشان می‌دهد که ساختار کد و الگوی رمزنگاری در بین باج‌افزارهای هم‌خانواده تشابهات زیادی دارد. بنابراین با استفاده از مدل به‌دست آمده خواهیم توانست سایر باج‌افزارهای یک خانواده را شناسایی کرده و دقت و سرعت تشخیص را بمراتب بالاتر ببریم.

کلمات کلیدی: Ransomware، Detection، Responding، Obfuscation.

۱ مقدمه

باج‌افزار[۱]، اصطلاحی کلی برای توصیف نوعی بدافزار است که هدف آن باج‌گیری دیجیتالی از قربانیان با ایجاد محدودیت سیستمی می‌باشد؛ این تهدید به محل جغرافیایی یا نوع سیستم محدود نیست و می‌تواند علیه هر

[1]Ransomware

دستگاهی اتفاق بیفتد. هر یک از انواع سیستم‌عامل‌ها، از اندروید گرفته تا سیستم‌های iOS و ویندوز، همه در معرض خطر این نوع سوء استفاده قرار دارند.

باج‌افزارهای امروزی با درس گرفتن از گذشته، برای اطمینان یافتن از اینکه قربانی با احتمال بیشتری به خواسته آن‌ها تن دهد، از روش‌های پیشرفته رمزنگاری و با اتکا بر کلیدهای یکتا به ازای هر حمله، بهره می‌برند. با این شگرد، مهاجمین می‌توانند اطمینان داشته باشند که نه تنها گروه امداد راهی برای یافتن کلید رمزگشایی نخواهند یافت، بلکه کلید رمزگشایی یک حمله، در سایر حملات کاربردی نخواهد داشت.

توجه به این نکته نیز ضروری است که در اغلب موارد، اقدامات تخریبی با استفاده از قابلیت‌ها و منابع سیستمی موجود در دستگاه قربانی انجام می‌شود و تنها محدود به کارایی و امکانات پردازشی همان دستگاه خواهد بود. در این میان، بسیاری از رفتارهای مخرب باج‌گیرها از الگوهای خاصی پیروی می‌کنند که قابل تشخیص هستند؛ بنابراین می‌توان از این الگوها برای شناسایی و مقابله با انواع خاصی از باج‌افزارها استفاده کرد؛ لذا شناسایی خانواده باج‌افزارها دارای اهمیت فراوان است، چرا که علاوه بر شناسایی خانواده باج‌افزارها، می‌توان از روش‌های طراحی شده برای مقابله و بازیابی از حملات نیز استفاده کرد.

اما چیزی که برای متخصصین امنیت اطلاعات ترسناک‌تر است، این است که به نظر نمی‌رسد الگویی قابل تشخیص برای حملات باج‌افزارها وجود داشته باشد. اکثر روش‌های سنتی شناسایی مبتنی بر امضا[۲] نیز توسط گروه‌های هکری مهاجم دور زده می‌شوند؛ بنابراین پیاده‌سازی روش‌های نوین شناسایی باج‌افزارها به شدت احساس می‌شود. در این پژوهش مدلی ارائه شده که سایر پژوهشگران، با استفاده از معیارهای به دست آمده در خصوص مصرف منابع و همچنین با بهره‌گیری از روش‌های ابتکاری در هوش مصنوعی یا روش‌های اکتشافی، ابزارهای موثرتری برای تشخیص باج‌افزار توسعه دهند.

۲ مروری بر پژوهش‌های انجام شده

در مطالعه و مرور پژوهش‌های صورت گرفته در حوزه شناسایی باج‌افزارها بر اساس الگوی مصرف منابع سیستمی، مقالات اندکی تاکنون به چاپ رسیده است. بیشتر پژوهش‌های مرتبط در روی نظارت بر رفتار فرآیندها و تحلیل لاگ انجام شده است. همچنین بیشتر تحقیقات صورت گرفته که مرتبط با موضوع این پژوهش می‌باشند، در خصوص مطالعه رفتار باج‌افزار بر روی هارد دیسک بوده و بررسی همزمان هارد دیسک، حافظه RAM و پردازنده تاکنون انجام نشده است. به طور کلی پژوهش‌های مرتبط با شناسایی خانواده‌های مختلف باج‌افزاری را می‌توان به صورت زیر دسته‌بندی کرد: تشخیص مبتنی بر امضا، تشخیص بر اساس تحلیل ایستا و تشخیص بر اساس تحلیل پویا.

با توجه به بررسی‌های انجام شده، در این پژوهش‌ها نرخ تشخیص ارائه شده برای شناسایی تعداد بالای باج‌افزارها دارای کاستی‌هایی چون پایین بودن نرخ دقت تشخیص، نرخ بالای مثبت کاذب و حتی بالا بودن نرخ عدد تشخیص داده شده هستند. از دیگر کاستی‌های پژوهش‌های مذکور، غفلت از تأثیر نرخ سرعت در تشخیص باج‌افزارها است؛ عدم رفع کاستی‌های مذکور در زمان پیاده‌سازی اینگونه روش‌های شناسایی،

[2] Signature

موجب متحمل شدن هزینه‌هاي زمانی و مادي زيادي، و نيز موجب كندي سيستم شناسايی و عدم دستيابی بـه خروجی صحيح و واقعی خواهد شد.

ديموو همكاران در سال ۲۰۱۹ با اندازه‌گيری و استخراج شاخص‌های متريک HDD در يک حمله باج‌افزاری برای نوع از خانواده باج‌افزار، بر اين باور قرار گرفتند كه بهترين و كارآمدترين زمان برای شناسايی باج‌افزار در شبكه در زمان اجرای پی لود آغاز حمله می‌باشد. با اندازه‌گيری عملكرد هارد ديسک در زمان اجرای باج‌افزار اين امكان را می‌دهد كه در خلال رمزنگاری رفتار سيستم سنجيده شود؛ بنابراين می‌توان سرعت دامنه رمزنگاری را مشخص و ساير سيستم‌ها را ايزوله كرد. از معايب اين روش عدم بررسی ديگر منابع مرتبط با حمله باج‌افزاری می‌باشد.

دارابيان و همكاران در سال ۲۰۲۰ برای دسته‌بندی و شناسايی نمونه باج‌افزارها، از روش كاوش الگوهای متوالی استفاده نمودند. آن‌ها ويژگی‌هايی را به دست آورده، تا قابل استفاده برای الگوريتم‌های دسته‌بندی كننده يادگيری ماشين باشد. دقت ۹۹% در تشخيص نمونه‌های باج‌افزار و همين طور دقت ۹۶% در شناسايی و دسته‌بندی خانواده آن‌ها روی الگوريتم‌های متداول يادگيری ماشين، نشان از كيفيت بالای ويژگی‌های پيشنهادی دارد. اين روش دقت بالايی در شناسايی نمونه های بی‌خطر ندارد؛ از اين رو در حوزه امنيت و دفاع با درصد بالا قابل اطمينان نمی‌باشد.

جليليان و همكاران در سال ۲۰۱۶ روشی را پيشنهاد دادند كه مبتنی بر تشخيص امضا در محيط ايستا برای استخراج امضای فايل‌ها از روی آپكدهای برنامه بود كه بر اين اساس، باج‌افزارها به دو دسته سالم و مخرب تقسيم‌بندی گرديدند. اين روش دارای دقت مناسبی بوده ولی مستلزم پردازش زياد بوده و بسيار زمان‌بر می‌باشد، از اين رو در تمامی شرايط قابل استفاده نمی‌باشد.

در اين مقاله كه با رويكرد آزمايشگاهی انجام شده است، ابتدا جامعه آماری متشكل از ۵۰ نمونه باج‌افزار از ۱۰ خانواده مختلف گردآوری گرديده و پس از آماده‌سازی يک بستر امن و ايزوله، تک تک باج‌افزارها در اين محيط اجرا و آزمايش گرديده‌اند. ابزارهای اندازه‌گيری از پيش تهيه شده پارامترهای سرعت رمزنگاری، ميزان مصرف پردازنده، حافظه رم و ديسک را اندازه‌گيری می‌كنند. با توجه به فرضيه اصلی تحقيق، باج‌افزارهای هم خانواده تشابهات زيادی در پارامترهای ذكر شده خواهند داشت. اين موضوع در اين تحقيق به اثبات رسيده و در انتهای پژوهش مدلی برای اين ۱۰ خانواده باج‌افزاری ترسيم گرديده است. مدل ترسيم شده قابل بهره‌برداری برای متخصصين تحليل بدافزار و پژوهشگران و دانشجويان حوزه امنيت سايبری خواهد بود.

۳ محيط آزمايشگاهی

هرچند مطالعه رفتار باج‌افزارها را می‌توان با يک ميزبان ويندوز نيز انجام داد، اما معماری ايده‌آل بر اساس سيستم‌عامل مک يا لينوكس است؛ در صورتی كه باج‌افزار بتواند از داخل ماشين مجازی به ميزبان انتقال پيدا كند، به احتمال كمتر ميزبان را آلوده می‌كند؛ اين رخداد معمولاً از طريق آسيب‌پذيری در نرم‌افزار ماشين مجازی يا خطای تحليل‌گر رخ می‌دهد. با توجه به اينكه باج‌افزارهای ويندوزی در محيط لينوكس اجرا

نمی‌شوند، ترجیح ما استفاده از یک میزبان لینوکسی است؛ پس بنا به دلایلی که اشاره شد، سیستم‌عامل میزبان در این پژوهش نسخه دسکتاپ لینوکس اوبونتو ۲۲٫۰۴ در نظر گرفته شده است.

جامعه‌ی آماری مورد استفاده در این پژوهش مربوط به باج‌افزارهای ویندوزی می‌باشد؛ لذا برای پیاده‌سازی محیط آزمایشگاه از سیستم‌عامل خانواده ویندوز استفاده شده است. در انتخاب نوع سیستم‌عامل مهمان دو گزینه ویندوز ۷ و ویندوز ۱۰، با توجه به محبوبیتی که دارند پیش رو قرار داشت. با توجه به اینکه دیتاست مورد استفاده در این پژوهش مربوط به ۳ سال گذشته می‌باشد، در انتخاب نوع سیستم‌عامل مهمان نیز سعی شده تا از آخرین نسخه‌های سیستم‌عامل ویندوز ۱۰ استفاده گردد که مشکلی به لحاظ سازگاری به وجود نیاید.

در این پژوهش، سیستم‌عامل ویندوز ۱۰ با مشخصات زیر برای ساخت آزمایشگاه در نظر گرفته شد:

OS Name: Microsoft Windows 10 Enterprise LTSC (X64)
OS Version: 10.0.17763 N/A Build 17763
CPU: Intel Corei7-7700 3.60GHz (4 Core)
RAM: 8.00 GB
Disk: ADATA SU800 256GB NVME

برخی از باج‌افزارها برای اجرا نیاز به اتصال به اینترنت دارند تا با سرور فرمان و کنترل خود ارتباط بگیرند. با توجه به این که ماشین مجازی تحلیل، یک محیط ایزوله است و دسترسی به اینترنت ندارد، از طرفی به خاطر به حداقل رساندن امکان گسترش باج‌افزار به سیستم‌عامل میزبان، امکان فعال کردن اینترنت بر روی آن وجود ندارد. راهکاری که برای این موضوع در نظر گرفته شد، استفاده از یک شبیه‌ساز پروتکل‌های اینترنت می‌باشد. نرم‌افزار INetSim و BurpSuite برای این منظور در محیط لینوکسی REMnux پیکربندی شدند و با هدایت ترافیک شبکه ماشین تحلیل به سمت INetSim این مشکل مرتفع گردید. REMnux در واقع یک سیستم‌عامل لینوکسی بر پایه اوبونتو می‌باشد که مختص آنالیز بدافزار و مهندسی معکوس ساخته شده است.

به‌دلیل یکسان‌سازی شرایط محیط آزمایشگاه تست باج‌افزار، تمامی موارد مرتبط با سیستم عامل مهمان از قبیل Windows Defender، Windows Update غیرفعال گردیدند. برای تست و برداشت اطلاعات مورد نیاز نیز از نرم‌افزارهای HashOptionRightClick.reg، Process Explorer، FreeCommanderXE، Dummy File Generator استفاده گردید؛ درنهایت، تعدادی فایل طعمه بر اساس جدول ۱ با ویژگی‌های زیر با استفاده از ابزار اسکریپتی ایجاد گردید، تا در فرآیند آزمایش مورد استفاده قرار گیرند. برای اینکه فایل‌های طعمه جزء لیست سفید[3] باج‌افزارها نباشند و صد در صد رمزگذاری شوند، پسوند (doc.) برای آن‌ها در نظر گرفته شده است. همچنین برای سهولت در رمزنگاری و افزایش سرعت، مسیر فایل‌های طعمه در مسیر ریشه[4] سیستم‌عامل در نظر گرفته شده است.

[3] Whitelist
[4] Root

جدول ۱: مشخصات فایل‌های طعمه

حجم فایل طعمه	1 KB	100 KB	1 MB	100 MB	1 GB
تعداد	۱۰۰۰	۱۰۰۰	۱۰۰۰	۱۰۰۰	۱۰۰۰

۴ آماده‌سازی دیتاست پژوهش

برای آماده‌سازی دیتاست، ابتدا ۵ نمونه از باج‌افزارهای خانواده‌های HiddenTear، Dharma، Phobos، STOP/Djvu، Ryuk، Maze، Revil، Makop، LockBit و Conti از سامانه مرجع VirusTotal[۵] انتخاب و دانلود گردید. خانواده‌های باج‌افزاری به گونه‌ای انتخاب شده‌اند که بر اساس آمارهای جهانی، قربانیان زیادی را به خود اختصاص داده و در مناطق جغرافیایی متعددی منتشر شده باشند. همچنین سعی بر آن بوده که از بین باج‌افزارهای مطرح که قربانیانی را نیز در داخل کشور داشته‌اند، نمونه‌های تصادفی انتخاب گردند. تاریخ انتشار نمونه‌های انتخاب شده حداکثر مربوط به سه سال گذشته می‌باشد؛ دلیل این امر این است که بسیاری از باج‌افزارهای قدیمی به دلیل از کار افتادن سرورهای فرمان و کنترل و باگ‌های نرم‌افزاری یا سازگاری با سیستم‌عامل‌های جدید، هرگز اجرا نمی‌شوند. لذا برای حل این مشکل، بازه زمانی انتشار باج‌افزارها، حداکثر سه سال گذشته در نظر گرفته شده است. ملاک شناسایی نمونه‌های باج‌افزاری بر اساس الگوریتم هش[۶] SHA256 می‌باشد.

اجرای باج‌افزارها در محیط آزمایشگاهی شامل سه مرحله شروع، رمزنگاری و پایان می‌باشد. مدت زمان فرآیند رمزنگاری بسته به نوع باج‌افزار متفاوت است؛ این بازه معمولاً بین ۱ تا ۲۰ دقیقه ممکن است به طول بینجامد و این رفتار، محاسبه دقیق سرعت رمزگذاری فایل‌ها را دچار مشکل می‌کند. برای حل این مسأله، نتایج آزمایش به صورت میانگین بازه‌ای از زمان که شامل Peakهای متعدد می‌باشد، در نظر گرفته شده است.

در حین اجرای باج‌افزارها، میزان منابع مصرف شده توسط ابزار Process Explorer ثبت گردید. پس اتمام فرآیند رمزنگاری نیز، کلیه فایل‌هایی که پسوندشان تغییر کرده بود را به صورت صعودی مرتب کرده و تاریخ آخرین تغییر انجام شده بر روی فایل‌ها را توسط ابزار FreeCommanderXE ثبت نمودیم.

۵ تحلیل دست‌آوردهای فنی و ترسیم مسیر آینده پژوهش

تحلیل نتایج: بر اساس مشاهدات صورت گرفته از اجرای باج‌افزارها در محیط آزمایشگاهی و شاخص‌های به دست آمده، نتایج مطابق جدول ۲ حاصل گردیده است.

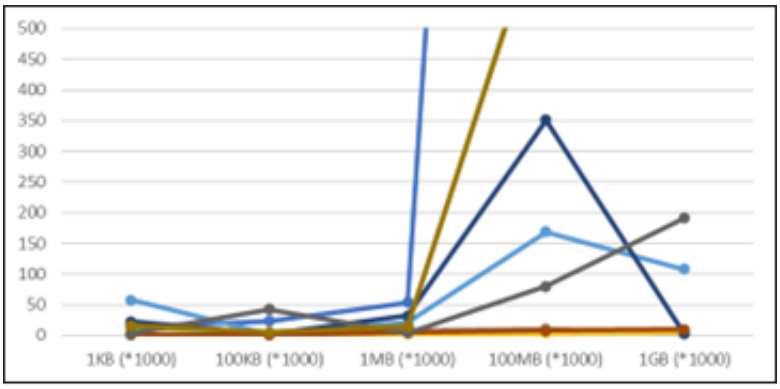
نتیجه اول: بر اساس شکل ۱ سرعت رمزنگاری فایل‌های با حجم مشخص توسط باج‌افزارهای هم‌خانواده، تقریباً یکسان است. به‌عنوان مثال، باج‌افزار خانواده Ryuk تعداد ۱۰۰۰ عدد فایل با حجم ۱۰۰ کیلوبایت

[۵] https://www.virustotal.com/

[۶] هش تابعی است که ورودی از حروف و اعداد را به یک خروجی رمزگذاری شده با طولی ثابت تبدیل می‌کند. توابع hash در سرتاسر اینترنت به منظور ذخیره ایمن کلمه عبور، یافتن سوابق تکراری، ذخیره سریع و بازیابی اطلاعات و موارد این‌چنین به‌کاربرده می‌شوند.

جدول ۲: میانگین سرعت رمزنگاری فایل‌ها

Ransomware Family	1KB (*1000)	100KB (*1000)	1MB (*1000)	100MB (*1000)	1GB (*1000)
Tear Hidden	15.8	23.2	54	3418	5940
Dharma	2.8	1.2	8	10.8	4.8
Phobos	1	1.4	9.2	11	3.4
STOP/Djvu	1	2.4	2.6	4.2	6
Ryuk	58.2	2.4	21	168.8	108
Maze	14	4.8	15	708	6370
Revil	22.6	2.2	32.2	351	3.6
Makop	1	1.4	5.4	8.2	10.2
LockBit	3.2	42.6	4	80	190.8
Conti	16.2	5.4	14.8	704	1757



شکل ۱: میانگین سرعت رمزنگاری فایل‌های طعمه توسط باج‌افزارها

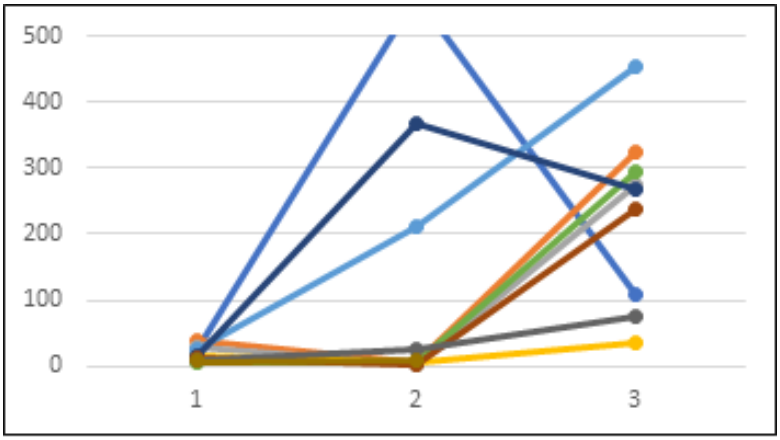
را در بازه زمانی ۱ تا ۴ ثانیه رمزگذاری می‌کند. این رفتار در بین تمام نمونه‌های باج‌افزاری در این خانواده مشابه است. دلیل این موضوع این است که ساختار کد و الگوی رمزنگاری در بین باج‌افزارهای یک خانواده تشابهات زیادی دارد.

نتیجه دوم: بر اساس جدول ۳، میزان مصرف منابع سیستم هنگام رمزنگاری فایل‌های با حجم مشخص توسط باج‌افزارهای هم خانواده، تقریباً یکسان است؛ به عنوان مثال در مورد باج‌افزار Makop میزان اشغال حافظه RAM حین اجرای باج‌افزار بین بازه ۲٫۲ تا ۲٫۸ مگابایت قرار دارد. با توجه به شکل ۲، این رفتار در بین تمام نمونه‌های باج‌افزاری در این خانواده مشابه است.

نتیجه سوم: در این آزمایش، هنگامی که حجم فایل‌ها رفته رفته افزایش می‌یابد، خانواده‌های مختلف باج‌افزاری دو رفتار متفاوت از خود نشان دادند:

جدول ۳: میانگین منابع اشغال شده رمزنگاری فایل‌ها

Ransomware Family	(%) CPU	(MB) RAM	(MB/s) Disk
Tear Hidden	24.26	561.44	109.1
Dharma	40.46	6.88	326
Phobos	28.44	3.94	274.8
STOP/Djvu	15.06	6.84	34.48
Ryuk	24.6	210.1	452.9
Maze	7.06	6.98	293.98
Revil	16.66	368.12	267.94
Makop	12.64	2.44	237.98
LockBit	8.8	26.9	75.84
Conti	7.56	8.94	351.06



شکل ۲: منابع اشغال شده توسط Process مربوط به باج‌افزار در حین رمزنگاری

- حجم فایل با سرعت رمزنگاری و مصرف منابع رابطه مستقیم دارد؛ یعنی با افزایش حجم فایل‌ها، سرعت رمزنگاری و مصرف منابع سیستم نیز افزایش می‌یابد. باج‌افزارهای Hidden، Tear Maze و Conti این رفتار را از خود نشان دادند. بررسی ساختار فایل‌های رمزگذاری شده نشان داد که این باج‌افزارها در مواجهه با فایل‌های با حجم متفاوت، تمام ساختار فایل را رمزگذاری می‌کنند و حجم فایل هیچ تاثیری در الگوی رمزنگاری ندارد؛ به همین دلیل فایل‌های با حجم پایین، سریع‌تر و فایل‌های با حجم بالا، کندتر رمزگذاری می‌شوند. شکل شماره ۱ نیز گویای این مطلب است.

- حجم فایل با سرعت رمزنگاری و مصرف منابع رابطه عکس دارد؛ یعنی با افزایش حجم فایل‌ها، سرعت رمزنگاری و میزان مصرف منابع سیستم کاهش می‌یابد یا تغییر چندانی نمی‌کند؛ باج‌افزارهای Dharma، Phobos، STOP/Djvu، Ryuk، Revil، Makop و LockBit این رفتار را از خود نشان دادند. بررسی ساختار فایل‌های رمزگذاری شده نشان داد که این باج‌افزارها در مواجهه با فایل‌های با حجم پایین (حدوداً ۱۰۰ مگابایت)، تمام ساختار فایل را رمزگذاری می‌کنند؛ اما هنگامی که باج‌افزار با فایل‌های بیشتر از این حجم مواجه می‌شود، الگوی رمزنگاری تغییر کرده و تنها بخشی از ساختار فایل (شامل Header فایل و بخش‌هایی از بدنه یا انتهای فایل) رمزگذاری می‌گردد؛ به همین علت، سرعت رمزنگاری بسیار بالاتر از گروه قبلی است. دلیل این موضوع این است که باج‌افزارهای ساخت یافته، با کاهش مدت زمان رمزنگاری، دیتای بیشتری را در فاصله زمانی کوتاه رمزگذاری می‌کنند و بدین ترتیب، خسارت بیشتری به بار می‌آورند. این به حداقل رساندن سربار عملکرد باج‌افزار، نه تنها به کاهش احتمال شناسایی شدن توسط نرم‌افزارهای امنیتی نظارت بر فرایندها کمک می‌کند، بلکه به طور موثری نیز از منابع پردازشی سیستم آلوده استفاده می‌کند تا تعداد و حجم بیش‌تری از فایل‌ها را رمزگذاری نماید؛ از سوی دیگر هرچه زمان رمزنگاری کوتاه‌تر باشد، قدرت مهار حمله یا محدودسازی دامنه خسارت توسط مدیر سیستم نیز کاهش می‌یابد. بنابراین باج‌افزارهای این گروه جزو خطرناکترین باج‌افزارهای دنیا محسوب می‌گردند.

- با استفاده از نتایج حاصل از پژوهش، با بررسی رفتار مشترک بین خانواده‌های باج‌افزاری و الگوبرداری از میزان مصرف منابع مختلف سیستم، با ایجاد نمودن یک دسته‌بندی و به کارگیری تکنیک‌های هوش مصنوعی می‌توان نتایج مناسب‌تری حاصل نمود.

مراجع

[۱] آلن لیسکا، تیموتی گالو (۲۰۱۹). «باج‌افزار: روش‌های دفاع در برابر باج‌گیری دیجیتال»، (ترجمه دکتر مهران گرمه‌ء، میلاد حضرتی، سارا رحیمی دوین، ۱۳۹۶)، انتشارات نشر گسترش علوم پایه.

[۲] حمید دارابیان، ستار هاشمی، سجاد همایون، کرم‌الله باقری‌فرد (۱۴۰۰). «شناسایی باج‌افزارها و خانواده آن‌ها با بهره‌گیری از روش کاوش الگوهای متوالی در تحلیل پویا».

[۳] آزاده جلیلیان، ابراهیم انصاری (۱۳۹۶). «شناسایی بدافزار براساس تشخیص امضای ایستا کد دستور و فایل باینری».

[4] Manaar Alam, Sayan Sinha, Sarani Bhattacharya, Swastika Dutta, Debdeep Mukhopadhyay, Anupam Chattopadhyay (2018). Ransomware Prevention via Performance Counters.

[5] Dimo Dimov, Yuliyan Tsonev (2020). Observing, Measuring and Collecting HDD Performance Metrics on a Physical Machine During Ransomware Attack, DOI:10.11610/isij.4723.

[6] Hesham A. Hefny, Nagy Ramadan, Hesham Alshaikh (2020)., Ransomware Prevention and Mitigation Techniques, International Journal of Computer Applications 117(40):31-39.

[7] Nathanael Paul, Sudhanva Gurumurthi, David Evans (2005). Towards Disk-Level Malware Detection.

[8] Jelena Milosevic, Miroslaw Malek, Alberto Ferrante (2016). A Friend or a Foe? Detecting Malware using Memory and CPU Features, International Conference on Security and Cryptography, 10.5220/0005964200730084.

[9] Juan A. Herrera-Silva, Lorena Barona, Leonardo Valdivieso, Myriam Hernandez Alvarez (2019). A Survey on Situational Awareness of Ransomware Attacks—Detection and Prevention Parameters, Remote Sensing 11(10):1168.

[10] Patrick Düssel, Thorsten Holz, Pavel Laskov, Konrad Rieck (2009). Learning and Classification of Malware Behavior, 10.17877/DE290R-2041.

[11] Abdullahi Arabo, Remi Dijoux, Timothee Poulain, Gregoire Chevalier (2020). Detecting Ransomware Using Process Behavior Analysis, Procedia Computer Science 168:289-296, 10.1016/j.procs.2020.02.249.

[12] Daniel Gonzalez, Thaier Hayajneh (2017). Detection and Prevention of Crypto-Ransomware, Conference: 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), 10.1109/UEMCON.2017.8249052.

[13] Patrick Luckett, J. Todd Mcdonald (2018). Identifying stealth malware using CPU power consumption and learning algorithms, Journal of Computer Security 26(10):1-25, 10.3233/JCS-171060.

[14] Robert Bridges, Jarilyn Hernandez Jimenez (2018). Towards malware detection via CPU power consumption: Data collection design and analytics, Project: Power consumption analysis for malware detection.

[15] Hernandez Jimenez, J., & Goseva-Popstojanova, K. (2019). Malware Detection Using Power Consumption and Network Traffic Data. 2019 2nd International Conference on Data Intelligence and Security (ICDIS).

[16] Kuruvila AP, Kundu S, Basu K. (2020). Analyzing the efficiency of machine learning classifiers in hardware-based malware detectors.

[17] Ramesh G, Menen A. (2020). Automated dynamic approach for detecting ransomware using finite-state machine. Decision Support Systems 138:113400.

[18] Tanana, D., & Tanana, G. (2020). Advanced Behavior-Based Technique for Cryptojacking Malware Detection. 2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS), 7.

ارائه روشی برای تشخیص اجتماع در شبکه‌های پیچیده با الگوریتم بهینه‌سازی خرگوش‌های مصنوعی

آرش هدایتی [۱]، محسن محمودی [۱]

[۱] پژوهشگر پژوهشگاه علوم انتظامی و مطالعات اجتماعی فراجا، تبریز
mohsen.nahmoudi98@email.com ،waro.info@gmail.com

چکیده

شبکه پیچیده نگاهی جدید به پدیده‌های می‌باشد که با توجه به ارتباط اجزای آن و همچنین ارتباط با دیگر پدیده‌ها، دارای پیچیدگی بالایی بوده و رفتار جمعی متفاوتی از خود نشان می‌دهند. تشخیص اجتماع یک چالش مهم در این شبکه‌ها می‌باشد. در این مقاله برای تشخیص اجتماع در شبکه‌های پیچیده از رویکرد فرا اکتشافی و الگوریتم بهینه‌سازی خرگوش مصنوعی استفاده شد. روش پیشنهادی در محیط نرم‌افزاری متلب پیاده‌سازی شده و کارایی آن در چهار مجموعه داده حقیقی (باشگاه کاراته زاخاری، شبکه فوتبال کالج آمریکایی، شبکه دلفین‌های، شبکه پول بوکز) با شاخص‌های پیمانگی و NMI مورد تجزیه‌وتحلیل قرار گرفت. تجزیه‌وتحلیل نتایج نشان داد که در مجموعه داده‌های حقیقی بالاترین مقدار پیمانگی به‌صورت میانگین برای مجموعه داده Polbooks و پایین‌ترین مقدار آن برای مجموعه داده Karate می‌باشد. این در حالی است که در مجموعه داده حقیقی بالاترین میزان NMI برای مجموعه داده Dolphins و کمترین مقدار برای مجموعه داده Karate به‌دست‌آمده است.

کلمات کلیدی: شبکه پیچیده، شبکه اجتماعی، تشخیص اجتماع، الگوریتم بهینه‌سازی خرگوش مصنوعی.

۱ مقدمه

شبکه‌های پیچیده را می‌توان در قالب گراف نمایش داد که در این گراف، گره‌ها معادل با موجودیت‌های شبکه پیچیده بوده و یال‌های گراف نشان‌دهنده ارتباط بین این موجودیت‌ها می‌باشد. در این گراف‌ها توزیع یال‌ها به‌صورت ناهمگن می‌باشد. به این ویژگی شبکه‌های پیچیده ساختار اجتماعی می‌گویند [۱]. اجتماع‌ها اطلاعات ارزشمندی در مورد نوع ارتباط بین موجودیت‌ها، نحوه انتقال اطلاعات بین آن‌ها و نحوه‌ی توزیع موجودیت‌ها در شبکه‌های پیچیده ارائه می‌کنند [۲]. یکی از زمینه‌های تحقیقاتی که در تحلیل شبکه‌های پیچیده بسیار موردتوجه قرارگرفته است، شناسایی اجتماع‌ها می‌باشد. شناسایی اجتماع، روشی برای پیدا کردن ساختار اجتماعی آن شبکه می‌باشد [۳]. شناسایی اجتماع یکی از چالش‌های مهم در شبکه‌های پیچیده

است [۴].

رویکردهای مختلفی برای تشخیص اجتماع ابداع‌شده است. اما با توجه به اینکه شناسایی اجتماع همواره در قالب یک مسئله NP-Hard مطرح‌شده است؛ بهترین رویکرد در این زمینه استفاده از الگوریتم‌های فرا اکتشافی می‌باشد. الگوریتم‌های متعددی در این زمینه مطرح‌شده است. هرکدام از این الگوریتم‌ها در کنار محاسنی که دارند؛ دارای معایبی نیز هستند. یکی از معایب اصلی آن‌ها گرفتار شدن در بهینه‌های محلی است که بی‌شک در کارکرد الگوریتم تأثیر منفی خواهد گذاشت. در این مقاله تلاش خواهد شد از الگوریتم بهینه‌سازی خرگوش مصنوعی برای تشخیص اجتماع در شبکه‌های اجتماعی استفاده شود. این الگوریتم کمتر در بهینه‌های محلی گرفتار می‌شود. در الگوریتم خرگوش مصنوعی، فرآیندهای جستجو با یک ضریب انرژی (A) کنترل می‌شود. روند کاهشی A به الگوریتم کمک می‌کند تا به‌آرامی از جستجوی سراسری به جستجوی محلی تغییر مکان دهد. خرگوش مصنوعی با استفاده از A ابتدا عملیات اکتشاف و سپس عملیات بهره‌برداری را انجام می‌دهد. ضریب انرژی A باعث می‌شود که الگوریتم حتی در مراحل پایانی تکرارها نیز کاوش داشته باشد. از دیگر مزیت‌های الگوریتم خرگوش مصنوعی می‌توان به تعداد کم پارامترها برای تنظیم اشاره کرد. با توجه به مطلب عنوان‌شده مهم‌ترین نوآوری مقاله را می‌توان در موارد زیر خلاصه کرد:

- استفاده از الگوریتم بهینه‌سازی خرگوش مصنوعی برای تشخیص اجتماع
- بهبود دقت تشخص اجتماع در شبکه‌های پیچیده

این مقاله مشتمل بر شش بخش می‌باشد که در بخش دوم آن کارهای پیشین بررسی شده و سپس در بخش سوم روش پیشنهادی شرح داده می‌شود. در بخش چهارم محیط شبیه‌سازی و مجموعه داده معرفی می‌گردد. بخش پنجم نیز به تجزیه‌وتحلیل نتایج می‌پردازد. نهایتاً در بخش ششم، پیرامون نتایج بحث و نتیجه‌گیری شده است.

۲ پیشینه تحقیق

در [۵] پژوهشگران استفاده از الگوریتم‌های مبتنی بر جمعیت را برای تشخیص اجتماع در شبکه‌های اجتماعی موردبررسی قرار داده‌اند. آن‌ها در این راستا چند الگوریتم بهینه‌سازی را انتخاب کرده و فرآیند بیشینه‌سازی را انجام داده‌اند. در [۶] نیز از الگوریتم بهینه‌سازی شعله پروانه گسسته برای یافتن راه‌حل تشخیص اجتماع در شبکه‌های اجتماعی استفاده‌شده است. همچنین در این مقاله پژوهشگران باارزش گذاری گره‌ها و شناسایی گره‌های مؤثر با رویکرد فرا ابتکاری نسبت به بیشینه‌سازی انتشار اقدام کرده‌اند. در [۷] از الگوریتم بهینه‌سازی کلونی مورچه برای تشخیص اجتماع در شبکه اجتماعی استفاده‌شده است. در این مقاله فرآیند تشخیص اجتماع با بهره‌گیری از گره‌های مؤثر انجام می‌گیرد.

در [۸] استفاده از الگوریتم بهینه‌سازی جهش قورباغه بهبودیافته برای شناسایی بهینه اجتماع و همچنین بیشینه‌سازی انتشار در شبکه‌های اجتماعی پیشنهادشده است. در این پژوهش برای حل مسئله ابتدا کاربران در شبکه اجتماعی خوشه‌بندی‌شده و سپس در هر خوشه کاربران بانفوذ شناسایی می‌شوند؛ در ادامه فرایند

انتشار در شبکه با بهره‌گیری از این گره‌های بانفوذ انجام می‌گیرد. در [۹] پژوهشگران با استفاده از الگوریتم بهینه‌سازی علف‌های هرز راه‌حلی را برای شناسایی اجتماع و بیشینه‌سازی انتشار در شبکه‌های اجتماعی پیشنهاد داده‌اند. در این مقاله نیز تمرکز پژوهشگران بر شناسایی گره‌های مؤثر شبکه و انتشار پیام به‌وسیله آن‌ها می‌باشد. در [۱۰] از ترکیب رویکرد مبتنی بر مرکزیت و الگوریتم بهینه‌سازی گرگ خاکستری برای شناسایی اجتماعی در شبکه‌های اجتماعی استفاده‌شده است؛ در این رویکرد الگوریتم بهینه‌سازی گرگ خاکستری با بهبود فرآیند نظریه مرکزیت راه‌حلی را برای تشخیص اجتماع در شبکه‌های اجتماعی ارائه می‌دهد.

در [۱۱] پژوهشگران استفاده از الگوریتم بهینه‌سازی خفاش گسسته را برای شناسایی اجتماع در شبکه‌های اجتماعی، پیشنهاد کرده‌اند. در [۱۲] رویکرد بهینه‌سازی چندهدفه برای بیشینه‌سازی انتشار در شبکه اجتماعی پیشنهادشده است.

بررسی کارهای پیشین گویای آن است که پژوهشگران برای تشخیص اجتماع اغلب از الگوریتم‌های فرااکتشافی استفاده می‌کنند. ولی در استفاده از چنین مدل‌هایی علیرغم نتایج مطلوب باید دو چالش اساسی گرفتار شدن در بهینه‌های محلی و همگرایی زودرس را در نظر گرفت.

۳ روش پیشنهادی

درروش پیشنهادی، جمعیت اولیه خرگوش‌های مصنوعی به‌صورت تصادفی و کاملاً پویا تولیدشده و پس از محاسبه خرگوش‌های مصنوعی (ترکیبی از توابع پیمانگی و پراکندگی)، اعضای جمعیت اولیه بر اساس برازندگی‌های محاسبه‌شده و خرگوش برتر (خرگوشی که بالاترین مقدار برازش را دارد) به‌عنوان راه‌حل انتخاب می‌گردد. لازم به ذکر است در این رویکرد هر خرگوش به‌صورت یک بردار مدل‌سازی شده و هر بردار بیانگر یک راه‌حل برای تشخیص اجتماع در شبکه‌های پیچیده می‌باشد. در ادامه خرگوش‌های مصنوعی با کمک عملگرهای جستجوی انحرافی، پنهان شدن مصنوعی و به‌روزرسانی راه‌حل‌های جدیدی برای تشخیص جوامع در شبکه‌های پیچیده تولید می‌کنند. در هر نسل از الگوریتم راه‌حل‌های جدید جایگزین راه‌حل‌های مرحله قبل شده و مجدد برازندگی آن‌ها محاسبه می‌شود. اگر در بین راه‌حل‌های جدید، راه‌حلی یافت شود که برازندگی آن از برازندگی خرگوش برتر بهتر باشد؛ آن راه‌حل با راه‌حل برتر قبلی جایگزین شده و عملگرهای الگوریتم اجرا می‌شود. این فرآیند تا برقراری شرط خاتمه ادامه یافته و در نسل آخر خرگوش مصنوعی برتر به‌عنوان یک راه‌حل برای تشخیص جوامع در شبکه‌های پیچیده انتخاب می‌شود. شکل ۱ بلوک دیاگرام روش پیشنهادی را نشان می‌دهد.

۱.۳ جمعیت اولیه خرگوش‌های مصنوعی

درروش پیشنهادی هر راه‌حل (عضو جمعیت اولیه) یک جواب برای مسئله تشخیص اجتماع خواهد بود. لذا عضو iام در جمعیت اولیه خرگوش‌های مصنوعی برداری از x_i است که طبق رابطه (۱) مدل‌سازی می‌گردد.

$$x_i = [x_i^1, x_i^2, , x_i^{nv}] \quad (۱)$$

شکل ۱: بلوک دیاگرام روش پیشنهادی

که x_i^j نشان‌دهندهٔ جامعه jاُمین عضو با i اُمین خرگوش مصنوعی و nv نشان‌دهنده تعداد گره‌ها در هر مجموعه داده (شبکه پیچیده) است. شکل ۲ بردار یک عضو از جمعیت اولیه خرگوش‌های مصنوعی را برای شبکه پیچیده مدل‌سازی کرده است.

$W_{1,1}$	$W_{1,2}$	...						...	$W_{1,n}$

شکل ۲: نمایش یک عضو جمعیت اولیه در طرح پیشنهادی برای شبکه تک لایه

۲.۳ محاسبه برازندگی خرگوش‌های مصنوعی

در تشخیص جوامع با الگوریتم‌های فرا اکتشافی می‌توان شاخص‌های مختلفی را برای ارزیابی اعضای جمعیت اولیه استفاده کرد. در این مقاله از شاخص پیمانگی استفاده شده است. رابطه (۲) این شاخص را معرفی

می‌کند.

$$Q = \sum_{k=۱}^{S} \left[\frac{l_k}{L} - \left(\frac{d_k}{۲L} \right)^{۲} \right] \quad (۲)$$

این شاخص، ملاکی برای سنجش امکان تقسیم‌بندی شبکه به اجتماعات است. بر اساس این شاخص هر چه تعداد پیوندها بین گره‌های اجتماع بیشتر باشد و تعداد پیوندهای بین اجتماعات کمتر باشد؛ آن شبکه پیمانگی بالاتری دارد. در این رابطه پارامتر S نشان‌دهنده تعداد کل اجتماعات است. همچنین پارامتر L تعداد کل یال‌های شبکه را نشان می‌دهد. پارامتر l_k و d_k نیز به ترتیب معرف تعداد یال‌های داخل اجتماع، مجموع درجات تمام گره‌های داخل اجتماع k هستند.

۳.۳ جستجوی غذا

فرض بر این است که در الگوریتم پیشنهادی، در مناطق تحت پوشش هر خرگوش، مقداری علف و حفره وجود دارد و خرگوش‌ها همیشه به‌طور تصادفی از موقعیت یکدیگر برای جستجوی غذا بازدید می‌کنند. رفتار جستجوی غذا برای خرگوش نشان می‌دهد؛ هر خرگوش تمایل دارد موقعیت خود را نسبت به خرگوش دیگر که به‌طور تصادفی در منطقه‌ی که تحت پوشش آن قرار دارد، به‌روز نماید. مدل ریاضی جستجوی غذا توسط خرگوش‌ها به‌صورت زیر فرموله می‌شود:

$$\vec{v}_i(t+۱) = \vec{x}_j(t) + R \cdot (\vec{x}_i(t) - \vec{x}_j(t)) + \text{round}(۰/۵ \cdot (۰/۰۵ + r_۱)) \quad (۳)$$

$$R = L \cdot c \quad (۴)$$

$$L = (e - e^{(\frac{t-۱}{T})^{۲}}) \cdot \sin(۲\pi r_۲) \quad (۵)$$

$$c(k) = \begin{cases} ۱ & \text{if } k = g(l) \\ ۰ & \text{else} \end{cases} \quad k = ۱, \ldots, d \text{ and } l = ۱, \ldots, \lceil r_۳ \cdot d \rceil \quad (۶)$$

$$g = \text{randperm}(d) \quad (۷)$$

$$n_۱ \sim N(۰, ۱) \quad (۸)$$

در رابطه (۳) مقدار $\text{round}(۰/۵ \cdot (۰/۰۵ + r_۱))$ به‌عنوان دلتا شناخته می‌شود که به جمعیت اولیه اضافه می‌گردد. هدف از این کار قرار نگرفتن الگوریتم در بهینگی محلی می‌باشد و الگوریتم بتواند به سمت بهینگی سراسری حرکت نماید. L بیانگر میزان دویدن خرگوش می‌باشد که در طول تکرار الگوریتم تغییر می‌نماید. L در طول تکرار از بیشترین مقدار به سمت کمترین مقدار حرکت می‌کند. همچنین C یک بردار نگاشت است که می‌تواند به الگوریتم پیشنهادی کمک کرده تابه صورت تصادفی تعدادی از عناصر جمعیت را برای انجام عملیات جهش انتخاب نماید. نهایتاً R نشان‌دهنده متغیر حرکتی الگوریتم می‌باشد که در شبیه‌سازی تعبیه گردیده است. برای روابط (۳) الی (۸) توضیحات زیر را باید در نظر گرفت.

- $\vec{v}_i(t+1)$ نشان‌دهنده موقعیت خرگوش در لحظه‌ی $t+1$
- $\vec{v}_i(t)$ بیانگر موقعیت خرگوش در لحظه‌ی t
- n بیانگر ابعاد جمعیت اولیه (تعداد خرگوش‌ها)
- d بیانگر ابعاد مسئله‌ی بهینه‌سازی
- T بیانگر حداکثر تکرار الگوریتم بهینه‌ساز خرگوش
- $\lceil . \rceil$ بیانگر تابعی جهت محاسبه‌ی حد بالا (سقف)
- تابع round() گرد کننده عدد به نزدیک‌ترین عدد صحیح
- تابع randperm() بیانگر تولید عدد صحیح در بازه‌ی $[1..d]$
- r_1، r_2 و r_3 سه عدد تصادفی در بازه $(0, 1)$
- L نشان‌دهنده سرعت حرکت در هنگام جستجو
- n_1 تابع توزیع نرمال

معادله (۳) نشان می‌دهد که خرگوش‌ها با توجه به موقعیت خرگوش‌های دیگر، عملیات جستجو را برای یافتن غذا انجام می‌دهند.

۴.۳ پنهان شدن تصادفی

در هر تکرار، خرگوش‌ها d حفره در اطراف خود (هر بعد از فضای جستجو) ایجاد می‌کند؛ تا از دست شکارچیان در امان باشند.در این میان هر خرگوش فقط یکی از لانه‌ها را برای مخفی شدن انتخاب می‌کند (به‌طور تصادفی). روابط زیر فرآیند پنهان شدن تصادفی را نشان می‌دهد.

$$\vec{b}_{i,j}(t) = \vec{x}_i(t) + H \cdot g \cdot \vec{x}_i(t) \quad (۹)$$

$$H = \frac{T - t + 1}{T} \cdot r_4 \quad (۱۰)$$

$$n_2 \sim N(0, 1) \quad (۱۱)$$

$$g(k) = \begin{cases} 1 & \text{if } k = j \\ 0 & \text{else} \end{cases} \quad k = 1, \ldots, d \quad (۱۲)$$

در معادله (۹)، H پارامتر پنهان شدن است که به‌صورت خطی از ۱ به $1/T$ با یک تغییر تصادفی در طول تکرارها کاهش می‌یابد. این پارامتر، در ابتدا، حفره‌ها را در فاصله‌ی دورتری از موقعیت خرگوش ایجاد

می‌کند. با افزایش تکرارها، این فاصله نیز کاهش می‌یابد. برای مدل‌سازی ریاضی استراتژی پنهان شدن تصادفی، معادلات زیر پیشنهادشده‌اند.

$$\vec{v}_i(t+1) = \vec{x}_i(t) + R \cdot (r_4 \cdot \vec{b}_{i,r}(t) - \vec{x}_i(t)) \quad (13)$$

$$g_r(k) = \begin{cases} 1 & \text{if } k = \lceil r_5 \cdot d \rceil \\ 0 & \text{else} \end{cases} \quad k = 1, \ldots, d \quad (14)$$

$$\vec{b}_{i,r}(t) = \vec{x}_i(t) + H \cdot g_r \cdot \vec{x}_i(t) \quad (15)$$

که در آن $\vec{b}_i$ نشان‌دهنده یک لانه تصادفی انتخاب‌شده از میان لانه‌های d و r_4 و r_5 دو عدد تصادفی در بازه $(0, 1)$ هستند.

۵.۳ به‌روزرسانی موقعیت خرگوش

بر اساس معادله (۱۳)، خرگوش سعی خواهد کرد موقعیت خود را نسبت به لانه‌ای که به‌طور تصادفی از میان لانه‌های موجود (d) انتخاب کرده است، به‌روزرسانی نماید. به‌روزرسانی موقعیت خرگوش iام بر اساس دو استراتژی جستجوی علوفه و پنهان شدن تصادفی به‌صورت زیر خواهد بود:

$$\vec{x}_i(t+1) = \begin{cases} \vec{x}_i(t) & f(\vec{x}_i(t)) \leq f(\vec{v}_i(t+1)) \\ \vec{v}_i(t+1) & f(\vec{x}_i(t)) > f(\vec{v}_i(t+1)) \end{cases} \quad (16)$$

این معادله نشان می‌دهد که اگر تناسب موقعیت خرگوش iام بهتر از موقعیت فعلی باشد، خرگوش موقعیت فعلی را رها کرده و در موقعیت کاندید ایجادشده توسط معادله (۱۳) قرار می‌گیرد.

۶.۳ کاهش انرژی

در الگوریتم بهینه‌ساز خرگوش مصنوعی، خرگوش‌ها همیشه تمایل دارند که اغلب در مرحله اولیه تکرارها، جستجوی اکتشافی انجام دهند درحالی‌که اغلب در مرحله بعدی تکرارها مخفی سازی تصادفی انجام می‌دهند. این مکانیسم جستجو، ناشی از انرژی یک خرگوش است که باگذشت زمان به‌تدریج تضعیف می‌شود. بنابراین، احتمال علوفه یابی در فرآیند تکراری حدود ۰٫۵ است. که این فاکتور نشان‌دهنده‌ی تعادل بین مرحله‌ی اکتشاف و بهره‌برداری می‌باشد.

۷.۳ بررسی شرط خاتمه

رویکردهای مختلفی برای خاتمه الگوریتم‌ها مطرح می‌باشد. در این پژوهش از تعداد دفعات اجرا (۱۰۰ دور) برای خاتمه روش پیشنهادی استفاده‌شده است. پس از برقراری شرط خاتمه برترین خرگوش به لحاظ برازندگی، بیانگر بهترین راه‌حل برای تشخیص اجتماع در شبکه‌های پیچیده خواهد بود.

جدول ۱: مجموعه داده‌های تک لایه و واقعی در طرح پیشنهادی

Networks	n	m	C	K	d
Karate	34	78	0.58	4.58	0.139
Dolphins	62	159	0.3	5.12	0.084
Football	115	613	0.4	10.66	0.093
Polbooks	105	441	0.48	8.4	0.068

۴ پیاده‌سازی و مجموعه داده

برای شبیه‌سازی روش پیشنهادی مقاله از نرم‌افزار متلب ۲۰۱۶ استفاده‌شده است. همچنین مجموعه داده پیشنهادی برای این مقاله، مجموعه داده‌های حقیقی شامل داده‌های مربوط به باشگاه کاراته زاخاری، شبکه فوتبال کالج آمریکایی، شبکه دلفین‌ها، شبکه پول بوکز هستند. تمامی این شبکه‌ها دارای ساختار اجتماعی واقعی هستند.

در جدول ۱ پارامتر n نشان‌دهنده تعداد کل گره‌های هر شبکه و پارامتر m نیز بیانگر تعداد کل لبه‌های متصل در هر شبکه است. همچنین پارامتر C معرف میانگین ضریب خوشه‌بندی در هر شبکه و پارامتر K میانگین درجه برای هر خوشه می‌باشد. نهایتاً پارامتر d نیز بیانگر میانگین درجه هر خوشه می‌باشد. روابط (۱۷)، (۱۸) و (۱۹) چولگی محاسبه پارامترهای C، K و d در جدول ۳ را نشان می‌دهند.

$$C = \frac{\sum_i^n C_i}{n} \tag{۱۷}$$

$$K = \frac{\sum_i^n K_i}{n} \tag{۱۸}$$

$$d = \frac{۲m}{n(n-۱)} \tag{۱۹}$$

۵ تجزیه‌وتحلیل

در این بخش، عملکرد روش پیشنهادی مقاله در تشخیص اجتماعات شبکه‌های پیچیده با دو شاخص اطلاعات متقابل نرمال شده و پیمانگی مورد تجزیه‌وتحلیل قرارگرفته است. روابط (۲۰) و (۲۱) این شاخص‌ها را معرفی می‌کنند.

$$\mathrm{NMI}(A,B) = \frac{-۲\sum_{i=۱}^{c_A}\sum_{j=۱}^{c_B} c_{ij}\log\left(\frac{c_{ij}N}{c_{i\cdot}\cdot c_{\cdot j}}\right)}{\sum_{i=۱}^{c_A} c_{i\cdot}\log\left(\frac{c_{i\cdot}}{N}\right)+\sum_{j=۱}^{c_B} c_{\cdot j}\log\left(\frac{c_{\cdot j}}{N}\right)} \tag{۲۰}$$

$$Q = \sum_{k=۱}^{S}\left[\frac{l_k}{L}-\left(\frac{d_k}{۲L}\right)^{۲}\right] \tag{۲۱}$$

جدول ۲: ارزیابی مدل پیشنهادی با شاخص پیمانگی

	Karate	Dolphins	Football	Pollbooks
std	0.07	0.08	0.04	0.05
min	**0.33**	0.38	0.51	0.50
max	0.42	0.52	**0.63**	0.55
mean	0.34	0.44	0.57	0.52

جدول ۳: مقایسه عملکرد طرح پیشنهادی با طرح‌های مشابه در شاخص پیمانگی

	Ref	Karate	Dolphins	Football	Polbooks
MOEA/D-TS	[13]	0.42	0.53	0.60	0.53
MOACO	[14]	0.41	0.52	0.60	0.52
ARO	Our	0.42	0.52	0.63	0.55

یکی از مطرح‌ترین و معتبرترین معیارها در شبکه‌های پیچیده NMI می‌باشد؛ این معیار اطلاعات متقابل نرمال شده نیز نامیده می‌شود؛ یک شاخص ارزیابی خارجی برای شبکه‌های پیچیده بوده و زمانی استفاده می‌شود که ساختار اجتماعِ درست در دست باشد. مقدار NMI در بازه‌ی $[۰, ۱]$ قرار دارد و مقدار بزرگ‌تر برای آن نشان‌دهنده آن است که اجتماعات یافت شده با اجتماعات درست مطابقت بیشتری دارد. در رابطه (۲۰) پارامتر c_{ij} نشان‌دهنده تعداد گره‌های مشترک در اجتماع درست i و اجتماع یافت شده j می‌باشد. با فرض اینکه A و B دو افراز مختلف از شبکه‌ای با N گره باشند و c_A و c_B به ترتیب نشان‌دهنده تعداد افرازهای اجتماعات A و B خواهند بود. همچنین پارامترهای $c_{i.}$ و $c_{.j}$ به ترتیب نشان‌دهنده حاصل جمع عناصر سطر iام و ستون jام هستند. شاخص دیگری که در این مقاله برای ارزیابی مدل پیشنهادی استفاده‌شده است؛ شاخص پیمانگی خواهد بود. توضیحات این شاخص در رابطه (۲) آمده است.

۱.۵ شاخص پیمانگی

در این آزمایش، روش پیشنهادی به تعداد ۳۰ مرتبه بر روی مجموعه داده‌های معرفی‌شده در جدول ۲ اجرا و نتایج ثبت شد. بررسی نتایج نشان می‌دهد که بالاترین مقدار پیمانگی در این آزمایش به‌صورت میانگین برای مجموعه داده Polbooks و پایین‌ترین مقدار آن برای مجموعه داده Karate به‌دست‌آمده است. همان‌طور که در جدول ۲ مشخص‌شده است؛ بالاترین نرخ پیمانگی با روش پیشنهادی مقاله در طول آزمایش‌های مختلف برای مجموعه داده Football با ۰٫۶۳ درصد شده است. این در حالی است که پایین‌ترین نرخ آن نیز برای مجموعه داده Karate با ۰٫۳۳ به‌دست‌آمده است.

مقایسه نتایج در بهترین حالت با الگوریتم‌های مشابه نشان می‌دهد که پیمانگی مدل پیشنهادی در همه داده حقیقی نسبت به طرح‌های مشابه بهبودیافته است. جدول ۳ نتایج این بررسی را نشان می‌دهد.

جدول ۴: بررسی کارایی مدل پیشنهادی با شاخص NMI

	Karate	Dolphins	Football	Polbooks
std	0.05	0.04	0.04	0.06
min	**0.83**	0.88	0.82	0.85
max	**1.00**	**1.00**	0.97	**1.00**
mean	0.90	0.94	0.89	0.91

جدول ۵: مقایسه نتایج مدل پیشنهادی با طرح‌های مشابه در شاخص NMI

	Ref	Karate	Dolphins	Football	Polbooks
MOEA/D-TS	[13]	1.00	1.00	0.97	1.00
MOACO	[14]	1.00	1.00	0.92	0.60
ARO	Our	1.00	1.00	0.97	1.00

۲.۵ شاخص اطلاعات متقابل نرمال شده

در این بررسی روش پیشنهادی به ازای هر یک از مجموعه داده‌های جدول ۳ به تعداد ۳۰ مرتبه اجرا و نتایج ثبت گردید. بررسی نتایج برای نشان می‌دهد که بالاترین نرخ NMI به‌صورت میانگین برای مجموعه داده‌های Polbooks و Dolphins حاصل‌شده است. همچنین پایین‌ترین نرخ آن نیز برای مجموعه داده‌های Football و Polbooks به‌دست‌آمده است. جدول ۴ نتایج این بررسی را نمایش می‌دهد.

بر اساس نتایج به‌دست‌آمده در جدول ۴، بالاترین نرخ NMI به‌دست‌آمده با روش پیشنهادی مقاله در طول آزمایش‌های مختلف برای مجموعه داده‌های Polbooks، Dolphins و Karate حاصل‌شده که مقدار آن برابر با ۱ است. این در حالی است که پایین‌ترین مقدار آن نیز برای مجموعه داده‌های Football و Polbooks با ۰٫۸۳ به‌دست‌آمده است.

مقایسه نتایج طرح پیشنهادی مقاله که یک رویکرد مبتنی بر الگوریتم بهینه‌سازی خرگوش‌های مصنوعی می‌باشد؛ در بهترین حالت بیانگر آن است که نرخ NMI با آن در مجموعه داده‌های حقیقی نسبت به الگوریتم‌ها و مدل‌های مشابه بهبودیافته است. جدول ۵ نتایج روش پیشنهادی و روش‌های مشابه در مجموعه داده‌های حقیقی را با شاخص NMI مقایسه کرده است. بررسی نتایج درج‌شده در جدول ۵ نشان می‌دهد که روش‌های MOACO و MOEA/D-TS نتایج نزدیکی به روش پیشنهادی داشته‌اند. به‌نحوی‌که در مجموعه داده‌های Karate و Dolphins این طرح‌ها همانند روش پیشنهادی از NMI برابر ۱ برخوردند. این در حالی است که الگوریتم MOEA/D-TS در مجموعه داده Polbooks نیز NMI برابر ۱ به دست آورده است. اما در مجموعه داده Football روش پیشنهادی مقاله که یک روش مبتنی بر الگوریتم بهینه‌سازی شاهین طلایی است؛ نسبت به آن نتایج بهتری ارائه می‌دهد.

۶ بحث و نتیجه‌گیری

شبکه پیچیده معرف پارادایم پیچیدگی است که عناصر سازنده آن تشکیل شبکه‌ای را می‌دهند که اجزاء شبکه دارای برهم‌کنش هستند و از اندیشه کل‌نگر بهره می‌گیرند. این شبکه‌ها با چالش‌های مختلفی مواجه هستند که یکی از مطرح‌ترین چالش‌ها شناسایی اجتماع است. روش‌های مختلفی برای تشخیص اجتماع در شبکه‌های پیچیده پیشنهادشده است. اما با توجه به اینکه شناسایی اجتماع همواره در قالب یک مسئله NP-Hard مطرح بوده است؛ بهترین الگو و روش در این زمینه استفاده از الگوریتم‌های فرا اکتشافی می‌باشد. در این مقاله برای برطرف کردن چالش شناسایی اجتماع در شبکه پیچیده از الگوریتم بهینه‌سازی خرگوش‌های مصنوعی استفاده شد. روش پیشنهادی مقاله برای تشخیص جوامع شبکه‌های پیچیده در محیط نرم‌افزاری متلب پیاده‌سازی شده و کارایی آن در چهار مجموعه داده حقیقی با شاخص‌های پیمانگی و NMI مورد تجزیه‌وتحلیل قرار گرفت. تجزیه‌وتحلیل داده‌ها برتری روش پیشنهادی در مقایسه با طرح‌های مشابه را اثبات می‌کند.

۷ کارهای آینده

در این مقاله برای تشخیص اجتماع در شبکه های پیچیده از الگوریتم بهینه سازی خرگوش مصنوعی استفاده شد. این مدل با تکیه بر شاخص پیمانگی در محاسبه برازندگی جمعیت اولیه، نتایج بهتری در مقایسه با مدل های مشابه ارائه می دهد؛ ولی باید در نظر داشت که در تشخیص اجتماع علاوه بر شاخص پیمانگی، شاخص های دیگری نیز برای انتخاب راه حل های مطلوب وجود دارد؛ که می تواند در خروجی مدل موثر باشد. بر همین اساس پیشنهاد می شود در کارهای آینده در تابع برازندگی، تاثیر شاخص های دیگر نیز مورد بررسی قرار گیرد. همچنین می توان مدل را با الگوریتم های بهینه سازی دیگری مانند گورکن عسلخوار، عقاب آکیلا، عقاب طلایی، مرغ های دریایی و ... نیز مورد بررسی قرار داد.

مراجع

[1] C. Li, H. Chen, T. Li, and X. Yang, “A stable community detection approach for complex network based on density peak clustering and label propagation”, Applied Intelligence, vol. 52, no. 2, pp. 1188-1208, 2022.

[2] T. Shaik, V. Ravi, and K. Deb, “Evolutionary multi-objective optimization algorithm for community detection in complex social networks”, SN Computer Science, vol. 2, no. 1, pp. 1-25, 2021.

[3] S. T. Shishavan and F. S. Gharehchopogh, “An improved cuckoo search optimization algorithm with genetic algorithm for community detection in complex networks”, Multimedia Tools and Applications, pp. 1-27, 2022.

[4] S. Taheri and A. Bouyer, “Community detection in social networks using affinity propagation with adaptive similarity matrix”, Big data, vol. 8, no. 3, pp. 189-202, 2020.

[5] A. ŞİMŞEK and K. Resul, "Using swarm intelligence algorithms to detect influential individuals for influence maximization in social networks", Expert Systems with Applications, vol. 114, pp. 224-236, 2018.

[6] L. Wang, L. Ma, C. Wang, N.-g. Xie, J. M. Koh, and K. H. Cheong, "Identifying Influential Spreaders in Social Networks through Discrete Moth-Flame Optimization", IEEE Transactions on Evolutionary Computation, 2021.

[7] S. S. Singh, K. Singh, A. Kumar, and B. Biswas, "ACO-IM: maximizing influence in social networks using ant colony optimization", Soft Computing, vol. 24, no. 13, pp. 10181-10203, 2020.

[8] B. Chatterjee, T. Bhattacharyya, K. K. Ghosh, A. Chatterjee, and R. Sarkar, "A novel meta-heuristic approach for influence maximization in social networks", Expert Systems, p. e12676, 2021.

[9] Y. Zhang, Y. Yong, S. Yang, and T. Zhang, "A New Discrete Grid-Based Bacterial Foraging Optimizer to Solve Complex Influence Maximization of Social Networks", Discrete Dynamics in Nature and Society, vol. 2021, 2021.

[10] A. Zareie, A. Sheikhahmadi, and M. Jalili, "Identification of influential users in social network using gray wolf optimization algorithm", Expert Systems with Applications, vol. 142, p. 112971, 2020.

[11] L. Han, K.-C. Li, A. Castiglione, J. Tang, H. Huang, and Q. Zhou, "A clique-based discrete bat algorithm for influence maximization in identifying top-k influential nodes of social networks", Soft Computing, pp. 1-18, 2021.

[12] D. Bucur, G. Iacca, A. Marcelli, G. Squillero, and A. Tonda, "Multi-objective evolutionary algorithms for influence maximization in social networks", in European conference on the applications of evolutionary computation, 2017, pp. 221-233: Springer.

[13] S. Lotfi and F. Karimi, "A Hybrid MOEA/D-TS for solving multi-objective problems", Journal of AI and Data Mining, vol. 5, no. 2, pp. 183-195, 2017.

[14] C. Mu, J. Zhang, Y. Liu, R. Qu, and T. Huang, "Multi-objective ant colony optimization algorithm based on decomposition for community detection in complex networks", Soft Computing, vol. 23, no. 23, pp. 12683-12709, 2019.

نقش باورهای دینی در توانمندسازی خانواده در مواجهه با فضای سایبر

محمدعلی عبدالهی [۱]، مسلم طاهری کل‌کشوندی [۲]، عاطفه اندرزا [۳]

[۱] دانشیار گروه فلسفه، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
abdllahi@ut.ac.ir
[۲] استادیار گروه شیعه شناسی و معارف اسلامی، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
muslimtaheri@ut.ac.ir
[۳] دانشجوی دکتری مدرسی معارف اسلامی، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران
andarza.a313@ut.ac.ir

چکیده

ظهور فناوری‌های نوین ارتباطی در عصر حاضر، به همراه نوآوری‌هایی که در فضای سایبر به وجود آمده، موجب تحولات بنیادی درنهاد خانواده گشته است.در این مقاله کوشیده‌ایم تا نقش باورهای دینی در توانمندسازی خانواده در مواجهه با فضای سایبر را نشان دهیم. سؤال اصلی مقاله این است که، نقش باورهای دینی در توانمندسازی خانواده در مواجهه با فضای سایبر چیست؟ تلاش می‌کنیم در پاسخ این پرسش نشان دهیم که اعتقادات مذهبی می‌تواند نقش مهمی در توانمندسازی خانواده‌ها در مواجهه با فضای سایبر داشته باشد. باورهای دینی در صورتی‌که با بصیرت و آگاهی همراه شود می‌تواند در افراد به‌ویژه هسته‌ی اصلی خانواده احساس هدف‌مندی، امید به کمال انسانی و توجه به جاودانگی ایجاد کند . چنین باورهایی که از منابع دینی سرچشمه می‌گیرد به خانواده‌ها کمک می‌کند تا با حفظ روابط و ارزش‌های قوی، چالش‌های زندگی مدرن را پشت سر بگذارند. پژوهش حاضر به روش توصیفی – تحلیلی ارائه شده است.

کلمات کلیدی: باورهای دینی، توانمندسازی، خانواده، فضای سایبر.

۱ مقدمه

در دنیای معاصر همه چیز با سرعت زیادی در حال دگرگونی و تغییر است به طوری که با ورود دنیای مجازی، سرعت این تحولات با سرعت چند برابر در حال انجام است. این تغییر و دگرگونی‌ها به صورت‌های مختلف حکومت‌ها، جوامع و خانواده‌ها را تحت تأثیر قرار داده و آن‌ها را در برخی زمینه‌ها دچار چالش کرده، و در برخی زمینه‌های دیگر فرصت‌های زیادی برای آن‌ها فراهم آورده است. اما فضای سایبر، دارای ویژگی‌هایی است که می‌توان آن را هم در جنبه‌ی مثبت و هم جنبه‌ی منفی به کار برد. یکی از نهادهایی که می‌تواند

به انسان و خانواده کمک کند تا از جنبه‌های منفی فضای سایبر در امان بماند، نهاد دین است. نهاد دین می‌تواند با توانمندسازی خانواده در سه ساحت بینش، منش، و کنش، به پایداری و دوام آن کمک کند. لذا در ادامه به نحوه‌ی توانمندی خواهیم پرداخت.

۲ مروری بر کارهای دیگران

بررسی صورت گرفته نشان می‌دهد منبعی با عنوان دقیق مقاله‌ی حاضر، که به شکل همه جانبه‌ای به بررسی نقش باورهای دینی در توانمندسازی خانواده در مواجهه با فضای سایبر پرداخته باشد، وجود ندارد؛ اما منابع مورد استفاده هر یک، با توجه به اهدافی که مورد نظر پژوهشگران و نویسندگان آن‌ها بوده است، به بررسی جنبه‌های گوناگون این پدیده پرداخته‌اند. قائمی‌نیا (۱۴۰۰) [۹] در مقدمه‌ی کتاب خود، تحت عنوان «الهیات سایبر» آورده: پیدایش فضای سایبری، موجب ظهور انسان جدیدی در تاریخ شده که انسان مجازی نام دارد. انسان مجازی هویتی سیال دارد؛ چرا که صورت زندگی دیجیتالی هویت‌های ما و نحوه‌ی شکل‌دهی به آن‌ها را نیز تغییر می‌دهد. فضای سایبر ویژگی‌های هستی‌شناختی، معرفت‌شناختی و نشانه شناختی خاصی دارد و جزو ابعاد مختلف انسان مجازی به شمار می‌آید، این ویژگی‌ها سرشت انسان مجازی و نحوه دین‌داری او را تعیین می‌کند. نویسنده بیشتر دنبال مباحث تئوریک فضای مجازی و سایبر است و اشاره ی به نقش باورهای دینی در توانمندسازی خانواده برای مواجهه با فضای سایبر ندارد؛ لذا هدف و رویکرد کتاب با این مقاله متمایز است. براساس تحقیق صورت گرفته توسط آیت‌اللهی (۱۳۹۷) [۱] با عنوان «زندگی دینی در فضای مجازی»، یکی از ویژگی‌های مهم فضای مجازی تعاملی بودن آن است. بهره‌گیری مناسب از این ویژگی موجب خواهد شد که این فضا علاوه بر داشتن تهدید، مزیت‌های فراوانی نیز به همراه داشته باشد. اگر این تعاملات در پرتو آموزه‌های دینی قرار گیرد، می‌تواند محرکی برای تقویت سبک زندگی اسلامی در میان مخاطبان باشد (آیت‌الهی، ۱۳۹۷، ص ۱۲) [۱]. نویسنده در این کتاب بیشتر در حوزه رفتار فرد، کنکاش کرده، و اشاره‌ای به نقش باورهای دینی در توانمندسازی خانواده نداشته است. در کتاب نگاشته شده توسط عاملی (۱۳۹۶) [۷] تحت عنوان « خانواده مسلمان و فضای مجازی»، ظهور فضای مجازی و تغییر الگوی خانواده به الگوی دوفضایی خانواده، برخی فرصت‌ها، تهدیدها، نقاط ضعف و نقاط قوت را برای خانواده مسلمان به همراه دارد (عاملی، ۱۳۹۶، ص ۲۷۹) [۷]. اگر چه کتاب مذکور در برخی از موضوعات با مقاله‌ی نگارش‌شده نزدیک است، اما این کتاب به نقش باورهای دینی برای توانمندسازی خانواده اشاره‌ای ندارد و بیشتر مباحث نظری درباره‌ی فضای مجازی را پیگیری کرده است. در تحقیق صورت گرفته توسط گنجور (۱۴۰۰) [۱۰] تحت عنوان «واقع انگاری فضای مجازی»، ضمن بررسی وجودشناختی و ارائه‌ی تحلیل متافیزیکی از فضای مجازی، با تکیه بر اثربخشی آن بر سرشت و سرنوشت انسان، به اثبات عقلانی این مدعا پرداخته است، که فضای مجازی، امری واقعی و برخوردار از عینیت و واقعیت است (گنجور، ۱۴۰۰، ص ۴۱) [۱۰]؛ این اثر نیز تنها به بررسی فلسفه‌ی فضای مجازی پرداخته است و اشاره‌ای به سایر متغیرهای مقاله، مانند خانواده و توانمندسازی باورهای دینی موثر در آن حیطه توجهی نداشته؛ از این رو هم از بعد رویکردی و هم موضوعی با این مقاله دارای تمایز است. بر اساس پژوهش موسیوند و ساکی (۱۴۰۱) [۱] با عنوان «آسیب‌شناسی فضای سایبر در حوزه همسر گزینی و

خانواده»، فضای مجازی، در بعد خانواده و همسرگزینی در کنار محاسنی که دارد، آثار نامطلوبی را هم از جمله کاهش تعاملات رو در روی والدین و فرزندان، تصویرسازی و الگوسازی کاذب از همسر ایده‌آل برای جوانان، تولید و انتشار مضامین غیر اخلاقی و متباین با ارزش‌های ایرانی-اسلامی دارد (موسیوند و ساکی، ۱۴۰۱، ص ۶۹۹) [۱۲]. طبق تحقیق انجام شده توسط شهریاری (۱۳۹۹) [۴]، تحت عنوان «تأثیر باورهای دینی و اعتقادی در خانواده بر اساس آیات و روایات»، اگر در کانون خانواده، فرهنگ اسلامی و انسانی حاکم باشد و فرزندان مطابق آموزه‌های دینی و تعالیم نجات بخش قرآنی پرورش یافته و تربیت شوند، گذشته از این که در شکل‌گیری شخصیت و ماهیت فرزندان مؤثر خواهد بود، برکات تربیت صحیح خانواده در اجتماع نیز بازتاب شایسته‌ای می‌تواند داشته باشد (شهریاری، ۱۳۹۹، ص ۶۸) [۴]؛ این مقاله نیز به لحاظ موضوعی و اهداف با موضوع مقاله حاضر متفاوت است. در پژوهش صورت گرفته توسط مصباحی جمشید (۱۳۹۹) [۱۱] تحت عنوان «مسائل تربیت دینی در فضای مجازی و نحوه مواجهه با آن»، میان عناصر تربیت دینی و ویژگی‌های فضای مجازی تناظری برقرار است که در برخی موارد، به تحقق تربیت دینی مطلوب یاری می‌رساند، و در مواردی نیز به عنوان مانع عمل می‌کند. تحلیل این تناظر علاوه بر اینکه به شناخت عوامل و موانع تربیت دینی یاری می‌رساند، راهکار مواجهه با مسائل تربیت دینی در فضای مجازی را نشان می‌دهد (مصباحی جمشید، ۱۳۹۹، ص ۸۷) [۱۱]. این اثر نیز اشاره‌ای به سایر متغیرهای مقاله مانند خانواده و توانمندسازی باورهای دینی مؤثر در حیطه‌ی آن توجهی نداشته از این رو هم از بعد رویکردی و هم موضوعی با این مقاله متفاوت است.

۳ مفهوم شناسی

۱.۳ باورهای دینی

مفهوم باور در معرفت‌شناسی، مفهوم محوری است و در بسیاری از مفاهیم بنیادی، معرفت شناسی مانند صدق و کذب، و توجیه صدق و کذب به کار می روند؛ یعنی این باورها هستند که به صدق یا کذب متصف می شوند و از موجه بودن یا موجه نبودن آن‌ها سخن به میان می‌آید؛ باور را مي توان با عقیده مترادف دانست (نظرنژاد، ۱۳۸۱، ص ۵) [۱۳].

اعتقاد به واقعیت، از جنبه‌های اساطیری، فراطبیعی، یا معنوی یک دین است. باور دینی متمایز از عمل دینی یا رفتارهای دینی است چنانچه برخی باورمندان به دین آیین مذهبی به جا نمی‌آورند، و برخی از برپاکنندگان آیین مذهبی، باور به دین ندارند. باورهای دینی، از ایده‌هایی منحصر به فرد به دین مشتق شده است؛ اغلب به وجود، ویژگی و پرستش خدا یا خدایان، مداخله الهی در جهان و زندگی انسان، و یا توضیحات وظیفه‌گرا برای ارزش‌ها و شیوه‌هایی بر محور تعالیم مرتبط با یک رهبر روحانی و یا گروه. در مقابل به سایر سیستم‌های اعتقادی، باورهای دینی معمول مدون است (Wittgenstein, 2007, p 53) [۱۶].

۲.۳ توانمند سازی

توانمندسازی عبارت است از شناختن ارزش افراد و سهمی که می‌توانند در انجام امور داشته باشند .(نیازی و کارکنان نصرآبادی، ۱۳۸۸، ص ۲۲) [۱۴]. برخی نیز نوشته اند: «توانمندسازی یعنی تقویت باورها و افزایش دانش و مهارت‌ها» (بختیاری، احمدی مقدم، ۱۳۸۹، ص ۴۴) [۲].

۳.۳ فضای سایبر

سایبر (cyber) واژه‌ای بر گرفته از لغت cybernetics به معنای سکاندار یا راهنما است. نخستین کسی که واژه فضای سایبر را به کار برد، ویلیام گیتسون نویسنده داستان های علمی- تخیلی، در کتاب نورومنسر (Neuromancer) بود. فضای سایبر یا فضای مجازی (cyberspace) در تعریف برخی نویسندگان عبارت است از: «مجموعه‌ای از ارتباطات درونی انسان‌ها، از طریق رایانه و وسایل مخابراتی، بدون در نظر گرفتن جغرافیای فیزیکی است.» البته شاید بهتر باشد آن را چنین تعریف کنیم: «محیط الکترونیکی واقعی است، که ارتباطات انسانی به شیوه ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص، زنده و مستقیم روی می‌دهد» (طارمی، ۱۳۸۷، صص ۳۲-۳۹) [۶].

۴ ساحت‌های سه‌گانه باورهای دینی

باورهای دینی در واقع فرهنگ حیات انسانی را سامان می‌بخشد؛ هر جامعه‌ای، در سه حوزه‌ی : بینش، منش و کنش، یک الگو و مدلی را ارائه می‌دهد و فرهگ دینی هم بی‌توجه به این سه ساحت نبوده است. در حقیقت این سه ساحت جزء لاینفک فرهنگ دینی است و در زندگی جمعی انسان نیز تأثیرگذار است. تلفیق این سه ساحت موجب می‌شود تا یک زندگی معنادار و هدف‌مند برای انسان ایجاد شود. در ادامه به اختصار توضیحی در ارتباط با ساحت‌های مذکور موثر در حیات جمعی انسان بیان می‌گردد:

الف. **بینش**

بینش، به باورها، ارزش ها و جهان‌بینی اشاره دارد. درک فرد از جهان و جایگاه او در آن را مشخص، و او را در این مسیر هدایت می‌کند. در فرهنگ دینی، بینش اغلب توسط متون مقدس، آموزه‌ها و سنت‌ها شکل می‌گیرد. در فرهنگ اسلامی باور و اعتقاداتی وجود دارد که حس جهت‌گیری و هدف‌مندی را برای افراد و جوامع حتی کوچک‌ترین جامعه که خانواده است، فراهم می‌کند. در ادامه به برخی از آن‌ها اشاره خواهد شد:

* **اعتقاد به خداوند و حضور همه جایی او**

عبارتی مشهور را با تعابیر مختلف به نیچه و داستایوفسکی نسبت می‌دهند و آن، این است که « اگر خدا نباشد همه چیز جایز است». مراد از این عبارت این است که انسان فارغ از دین، خود را ملزم به انجام فعل صحیح نمی‌کند (خزاعی، ۱۳۹۳، ۹۱) [۳]. خداباوری به عنوان اولین

باور دینی در ساحت اعتقادات، نقش مهمی در جهت‌دهی رفتار اعضای خانواده در زندگی دارد و محور ارزش‌گذاری برای عملکرد هر یک از اعضای خانواده می‌باشد؛ زیرا سبب پر رنگ شدن ارزش‌های خانواده می‌شود. خانواده‌ی با ایمان به معنای واقعی عالم را محضر خدا می‌داند و همان‌گونه که تلاش می‌کند در برخورد با اعضای خانواده و انجام وظایف خانوادگی رضایت آن‌ها را جلب کند، در استفاده از فضای سایبر نیز هوشیار است که معصیت نکند و یا حق همسر، فرزندان و پدر و مادر خود را ضایع نکند.

* **اعتقاد به جهان پس از مرگ**

خانواده‌ی معاد باور، زندگی خود را هدف‌مند می‌سازد و باور دارد که لحظه به لحظه عمرش را باید در روز قیامت پاسخگو باشد که در چه راهی صرف کرده است. به عنوان مثال اگر هر یک از اعضای خانواده‌ی معاد باور بخواهند در روز چند ساعت از عمر خود را در فضای سایبر سپری کنند، می‌دانند باید روز قیامت جواب‌گو باشند که چگونه از عمر خود و چگونه از این فضا استفاده نموده‌اند.

ب. **منش**

اخلاق یکی از اجزاء سه گانه آموزه‌های دینی است که در پیوستگی و هماهنگی با عقاید و احکام، زمینه‌ی فعالیت یافتن، رشد اخلاقی و تحقق کامل باورهای دینی را فراهم می‌کند. در ادامه به ذکر چند نمونه از باورهای دینی ناظر به ساحت اخلاقی اشاره خواهد شد:

* **تعهد**

اصل وفاداری و تعهد یکی از ارزش‌های ضروری و بنیادی و پرکاربرد اخلاق در حوزه توانمندسازی خانواده است، و در آموزه‌های وحیانی اهمیت ویژه‌ای دارد. آنچه که در عصر حاضر در خانواده‌ها شاهد آن هستیم، مسأله‌ی خیانت زوجین به یکدیگر از طریق فضای سایبر و سلب اعتماد نسبت به هم است. از این‌رو، با نهادینه کردن اصل وفاداری و پایبندی به قواعد خانواده، می‌توان جلوی آثار نامطلوب و جبران ناپذیر بر نظام خانواده را گرفت و هر یک از اعضای خانواده را در مواجهه با چنین آسیب‌هایی توانمند ساخت.

* **رعایت حقوق اعضای خانواده**

از دیگر گزاره‌های اخلاقی در خانواده، رعایت حقوق اعضای خانواده است. دین اسلام برای هر یک از اعضای خانواده در قبال سایر اعضا، حقوق و وظایفی را معین کرده است: حقوق مشترک میان همسران و حقوق اختصاصی زن و مرد و حقوق متقابل میان والدین و فرزندان. رعایت حقوق خانواده با هدف تقویت ارزش‌های اخلاقی در خانواده، سبب توانمندسازی بنیان خانواده می‌شود و در مقابل، عدم رعایت این حقوق و عدم انجام آن وظایف، به طور قطع کارکردهای اخلاقی و اجتماعی خانواده را تضعیف می‌کند و آن را از کارآمدی لازم می‌اندازد.

* **صداقت**

یکی دیگر از باورهای اخلاقی که انسان را ملزم می‌گرداند تا به وظایف خود متعهد و مسئول باشد، اصل صداقت و صراحت است. صدق و راستی به عنوان یکی از بنیادی‌ترین و پرکاربردترین باورهای اخلاقی در اسلام، سهم به‌سزایی در وحدت‌بخشی، صمیمیت و تقویت و توانمندسازی خانواده، برای تحقق حقوق و وظایف دینی و ایجاد زمینه‌های رشد اخلاقی دارد.

ج. **کنش**

سطح دیگری از باورهای دینی ناظر به مسائل فقهی و بایدها و نبایدها و حلال و حرام است. در ادامه با ذکر نمونه‌ای اشاره خواهد شد:

* **حرمت روابط نامشروع زن و مرد در خانواده**

خانواده‌ی دین‌دار همواره خود را ملتزم به احکام فقهی دین دانسته و خطوط قرمزی را برای زندگی فردی و اجتماعی و خانوادگی خود لحاظ می‌کند؛ وقتی دو فرد از طریق شرعی و قانونی به ازدواج هم در می‌آیند، متعهد می‌گردند که به یکدیگر خیانت نکنند. امروزه با توجه به ناهنجاری‌های اخلاقی در فضای سایبر، هر یک از زوجین به سبب استفاده از این فضا، بعضا ممکن است با شخص سومی ارتباط نامشروع برقرار کنند. زوجین در صورتی می‌توانند کانون خانواده خود را در برابر این هجمه‌ها، توانمند سازند و عشق و وفاداری را به عنوان مهم‌ترین رکن در زندگی خود جاری کنند، که خانواده خود را پایبند به بایدها و نبایدهای شرع بدانند، و خود را از ارتکاب گناهانی مانند نگاه به نامحرم، روابط نامشروع و خیانت، و هر امر حرامی که موجب به سردی گرویدن خانواده و اخلال در روابط زوجین می‌گردد بر حذر دارند.

۵ توانمندسازی خانواده در فضای سایبر مبتنی بر باورهای دینی

فضای سایبر امروزه به یکی از موضوعات پژوهشی و کاربردی در سراسر جهان تبدیل شده است و حوزه‌های متعددی از علوم انسانی و اجتماعی تا علوم فنی و مهندسی را در بر می‌گیرد؛ برای فهم این فضا لازم است به علم پایه‌ی آن که دانش سایبرنتیک است اشراف داشت. فضای سایبر، فضایی است که اطلاعات، در آن به گردش در می‌آید؛ اما این گردش اطلاعات به صورت هدف‌مند و جهت‌مند انجام می‌گیرد و تغذیه می‌شود و این تعبیر، همان چیزی است که در اصطلاح علمی به آن «کنترل» گفته می‌شود. بر این اساس، فضای سایبر، به عنوان فضایی که در آن نوعی کنترل رقم می‌خورد، درک می‌شود؛ این مهم‌ترین و ذاتی‌ترین ویژگی این فضاست که البته در ادبیات عمومی و علمی ما کمتر بدان توجه شده است و باعث شده است جنبه‌ی «مجازی» بودن این فضا در افکار عمومی برجسته‌تر جلوه کند. البته توجه به این نکته نیز مهم است که در اینجا مجازی (virtual) در مقابل واقعی نیست و مجازی بودن، به نوعی واقعیت ناملموس اشاره دارد که در برابر واقعیت ملموس (actual) تعریف می‌شود. همان‌طور که گفته شد فضای سایبر مبتنی بر دانش سایبرنتیک شکل

جدول ۱: فرصت‌ها و تهدیدهای فضای سایبر ناظر به خانواده

فرصت‌های فضای سایبر	تهدیدهای فضای سایبر
تجارت و ایجاد کسب و کار	اتلاف وقت
آگاهی از اخبار روز دنیا	کاهش توجه به زندگی
تسهیل در ارتباطات	بی‌توجهی همسران به یکدیگر
آموزش	دسترسی به محتوای نامناسب
سرگرمی	دگرگونی و فاصله گرفتن از ارزش‌ها

گرفته است و این دانش که دانش سلطه و حاکمیت است، دارای دو مؤلفه مهم، یعنی انسان و ماشین است؛ این حاکمیت نیز از طریق کنترل محقق می‌شود. بر این اساس، فضای سایبر را می‌توان قلمروی حاکمیتی دانست که هر پدیده‌ای که به آن وارد می‌شود، تحت نوعی سلطه از جنس کنترل قرار می‌گیرد (فولادی قلعه، ۱۴۰۱، ص ۵) [۸]. کنش‌گری افراد در این سنخ از محیط (فضای سایبر)، بخش قابل توجهی از ساحات زندگی را به خود اختصاص داده است. لذا می‌توان مدعی شد که فضای سایبر، زمینه‌ی شکل‌گیری فرصت‌ها و تهدیدهایی را در زندگی خانوادگی ایجاد کرده است که به برخی از آن‌ها در جدول ۱ اشاره خواهد شد.

بنابراین عقیده و باور، بالاترین نقش را در زندگی فردی و اجتماعی انسان دارد. اگر باورهای انسان در زندگی، و به ویژه در خانواده صحیح و مطابق با خواسته‌های خالق هستی باشد، زندگی او نیز در مسیر صحیح قرار خواهد گرفت و در نتیجه توانمند خواهد شد؛ همچنین اگر بینش‌های نادرست، جهت‌دهنده زندگی فرد باشد، زندگی را به بی‌راهه برده، آن را ناکارآمد و ناتوان در برابر آسیب‌ها و تهدیدها می‌سازد. از این‌روست که اسلام بیش از هر چیز، به اصلاح شناخت و بینش‌های انسان اهمیت می‌دهد و برترین افراد را از نظر ایمان، کسانی می‌داند که از نظر شناخت بر دیگران برتری دارند. منابع دینی ما، یعنی قرآن و سنت، سرشار از توصیه‌های اثرگذار بر توانمندسازی خانواده است. مجموعه تعالیم اسلامی در مورد خانواده، ما را به نظامی رهنمون می‌کند که توانمندسازی خانواده را دربر دارد و پاسخگوی نیازهای مادی و معنوی خانواده است (صفورایی، ۱۳۹۰، ص ۵۳) [۵]. هرچند باورهای انسان می‌تواند از منابع متعدد نشات گیرد و بر نهاد خانواده اثر بگذارد، اما باورهای دینی بیشترین تأثیر را در زندگی انسان دارد. دین براساس تعریف رایج و مشهور، مجموعه‌ای از باورها وآموزه‌هایی است که از طرف خداوند برای تنظیم حیات انسان فرستاده شده است.

گزاره‌های دینی در قدیمی‌ترین و رایج‌ترین تقسیم، به سه حوزه‌ی اعتقادات، اخلاق و احکام تقسیم می‌شود. براساس منابع دین اسلام، ایمان واعتقاد به توحید، رسالت، امامت و حیات پس از مرگ، به عنوان اصول دین، مهم‌ترین باورهای دینی‌اند که از هر مسلمانی انتظار می‌رود به آن اعتقاد داشته باشد. کاربست این باورها و اعتقادات در بایدها و نبایدهایی که شرع مشخص کرده، به مثابه عامل بازدارنده از کجروی و انحرافات اجتماعی و اخلاقی، می‌تواند در توانمندسازی خانواده نقش به‌سزایی داشته باشد.

۶ نتیجه‌گیری

با توجه به مطالب مطرح شده، می‌توان نتیجه گرفت که باورهای دینی نقش قابل توجهی در توانمندسازی خانواده در مواجهه با فضای سایبر دارد؛ به آن خاطر که شالوده‌ی همه‌ی جهت‌گیری‌های انسان در زندگی، عقاید و باورهای اوست، و عقیده، چیزی است که به ذهن، فکر و جان انسان بسته می‌شود و پیوند می‌خورد. پیوند انسان با باورهایش به گونه‌ای عمیق است که چه بخواهد و چه نخواهد، در رفتار و روابط اجتماعی او اثر می‌گذارد. برای نمونه، وقتی انسان باور پیدا کند به اینکه پس از مرگ زنده می شود و حیاتی ابدی و جاودان خواهد داشت و نسبت به کارهایی که در این جهان انجام می‌دهد باید پاسخگو باشد، تلاش می‌کند خوب و بد اعمال خود را در این دنیا بسنجد، حقوق دیگران را رعایت کند، به والدین احترام بگذارد، و مانند آن. این مسئله نشان می‌دهد که یک باور، نظریه و بینشی که انسان پذیرفته و با ذهن شخص پیوند خورده است، به چه میزان در اعمال و رفتار او اثر دارد.

مراجع

[۱] آیت‌اللهی، زهره، آیت‌اللهی، زینت، «زندگی دینی در فضای مجازی»، انتشارات عترت نو، ۱۳۹۷.

[۲] بختیاری، حسن و احمدی مقدم، اسماعیل، «نقش راهبردهای مدیریتی در توانمندسازی مدیران»، فصلنامه مطالعات مدیریت انتظامی، ۵(۱)، ۱۳۸۹.

[۳] خزاعی، زهرا، «باور دینی انگیزش و التزام اخلاقی»، الهیات تطبیقی، ۵(۱۲)، ۱۳۹۳.

[۴] شهریاری، نهضت، «تأثیر باورهای دینی و اعتقادی در خانواده بر اساس آیات و روایات»، پژوهشنامه فقهی حقوقی زنان و خانواده، ۱۳(۵)، ۱۳۹۹.

[۵] صفورایی، محمدمهدی، «نقش اعتقادات، بینش‌ها و باورهای دینی در کارآمدی خانواده»، معرفت، ش ۱۶۳، ۱۳۹۰.

[۶] طارمی، محمد حسین، «فضای سایبر؛ آسیب ها و مخاطرات»، ره‌آورد نور، ش ۲۲، ۱۳۸۷.

[۷] عاملی، سید سعیدرضا، «خانواده مسلمان و فضای مجازی»، تهران: دفتر نشر فرهنگ اسلامی، ۱۳۹۶.

[۸] فولادی قلعه، کاظم، مجموعه مقالات نخستین کنفرانس ملی فضای سایبر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران، ۱۴۰۱.

[۹] قائمی‌نیا، علیرضا، «الهیات سایبر»، تهران: کتابخانه موزه و مرکز اسناد مجلس شورای اسلامی، ۱۴۰۰.

[۱۰] گنجور، مهدی، «واقع انگاری فضای مجازی»، خردنامه صدرا، دوره ۲۷ (۱۰۵)، ۱۴۰۰.

[۱۱] مصباحی جمشید، پرستو، «مسائل تربیت دینی در فضای مجازی و نحوه مواجهه با آن»، فصلنامه پژوهش در مسائل تعلیم و تربیت اسلامی، ۲۸(۴۸)، ۱۳۹۹.

[۱۲] موسیوند، محبوبه، ساکی، فائزه، «آسیب شناسی فضای سایبر در حوزه همسر گزینی و خانواده»، مجموعه مقالات نخستین کنفرانس ملی فضای سایبر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران، ۱۴۰۱.

[۱۳] نظر نژاد، نرگس، آیا ایمان به خدا عقلانی است، دانشگاه الزهرا، تهران، ۱۳۸۱.

[۱۴] نیازی، محسن، نصرآبادی، محمد، «توانمندسازی بر اساس راهبرد سرمایه اجتماعی»، ماهنامه تدبیر، ش ۲، ۱۳۸۸.

[۱۵] وثوقی، منصور، نیک خلق، علی اکبر، «مبانی جامعه شناسی»، تهران: خردمند، ۱۳۹۷.

[16] Wittgenstein, Ludwig (2007). Lectures and Conversations on Aesthetics, Psychology and Religious Belief. University of California Press. p. 53. ISBN 0520251814

رویکرد فقهی به جامه‌شناسی پیام، با نگاهی به اینستاگرام

ابوالفضل امامی میبدی[۱]، مجتبی شیخی ده‌آبادی[۲]، مصطفی میرزایی فیروزآبادی[۳]

[۱] دانش‌آموخته حوزه و دکترای فقه سیاسی و روابط بین‌الملل، جامعة المصطفی (ص)، قم
abolfazlemami@chmail.ir
[۲] دانش‌آموخته حوزه و دکترای علوم اقتصادی، مؤسسه آموزشی و پژوهشی امام خمینی (ره)، قم
msheikhy97@chmail.ir
[۳] دانشجوی کارشناسی ارشد، علوم تربیتی گرایش برنامه‌ریزی درسی، دانشگاه پیام نور، تفت
mmfabadi@gmail.com

چکیده

همانگونه که برای برآوردن نیاز بدن به آهن، نمی‌توان نبشی را گاز زد، برای نیازهای روان نیز، «جامه پیام» باید با دستگاه گوارش و پردازش روان سازگار باشد. از آنجا که شناخت لایه‌ها و ویژگی‌های انسان و جامعه، فراتر از توان اندیشه و دانش اندک ما است، باید روش فقهی را برای دستیابی به آن برگزید. فقه، ریشه همرسانی دیدپایه را به کژی‌های یهود برمی‌گرداند و بازپخش امروزی آن در اینستاگرام را به ما هشدار می‌دهد. فقه، همچنین «الگوی تراز جامه پیام» را، کاربست متوازن هر پنج لایه «عقل، فکر، قلب، حس و عضو» انسان و هر «پنج حسّ» لایه عضو می‌داند؛ چیزهایی که در «رفتار اسلامی و مخلصانه» یافت می‌شود. دستاورد این نوشته، آشکارسازی «تباهگری پنهان همرسانی دیدپایه» است که به «مهجوریت و هذیان‌پنداری قرآن» و دگرگونی ذائقه همرسانی، از واژه‌پایگی و خودآگاهی به ناخودآگاه‌سالاری می‌انجامد. ازاین‌رو باید در سامانه همرسانی تراز، افزون بر گسترش «رفتارپایگی» در جامعه، در ساماندهی شبکه‌های اجتماعی ملی نیز، از دیدپایگی جلوگیری کرد و توازن عناصر حسی را در جامه پیام سامان بخشید.

کلمات کلیدی: فقه ارتباطات، قالب پیام، جامه‌شناسی اینستاگرام، رسانه دیداری، گناه نگاه، رفتار مخلصانه.

۱ مقدمه

سامانه پیچیده جهان و توان اندک شناختی ما، راه ترازی جز پناه بردن به فقه (راهنمایی خدا و معصومین) بر جا نمی‌گذارد. از این رو، برخی کارهای غیرفقهی یا شبه‌فقهی نمی‌تواند بنیاد و چارچوب سامانه سایبری باشد. این کاستی، با کشف فقهی سامانه سایبری پیشرفته در کتاب «زبرتفقه نظام اسلام» [۱] و دو مقاله «بنیاد و چارچوب دانش سایبری اسلام» [۲] و «بررسی گلوگاه سایبری در ورود به گام دوم انقلاب» [۳] انجام شده است و اینک می‌توان به فقه بخش‌های ریزتری در سامانه سایبری اسلام پرداخت؛ مانند «جامه‌شناسی

همرسانی». یکی از آسیب‌های بنیادین و نهفته در همرسانی، به‌هم‌ریختن تراز دستگاه همرسانی و ذائقه پیام‌گیری است. زیاده‌روی در کاربست فضای مجازی و آن‌گاه بزرگ کردن ضلع دیداری جامه پیام، به دگرگونی ذائقه پیام‌گیری و دورافتادن از همرسانی با جامه واژگانی می‌انجامد. هنگامی که ذائقه مردم از همرسانی رفتارپایه به همرسانی مجازی، و از آنجا نیز از پیام‌های واژه‌پایه به پیام دیدپایه دگرگون شود، هم زمینه «ایمان به غیب و نادیدنی‌ها» کاسته می‌شود و هم معجزه جاوید قرآن که واژه‌پایه است، به گونه سامان‌وار برای ذائقه بشر، ناخوانا می‌شود: و پیامبر فرمود ای پروردگارم! همانا که مردم من این قرآن را [پیامی] پریشان و دورافکنده کردند «وَ قالَ الرَّسُولُ یا رَبِّ إِنَّ قَوْمِی اتَّخَذُوا هذَا الْقُرْآنَ مَهْجُوراً» ([۴]، فرقان، ۳۰). از این‌رو باید به جامه‌شناسی رویکرد بیم‌بار تاریخ یهود در دیدپایه کردن پیام و دنباله کنونی آن در جامه‌سازی صهیونی پیام و آسیب‌شناسی اینستاگرام پرداخت. دست‌یابی به رویکرد جامه‌شناسی فقهی و تاریخی پیام، یکی از نیازهای بسیار پیچیده بود و در دنباله آن، شناخت ویژگی‌های جامه دیداری و سنجش آن با جامه‌واژگانی و نشان دادن «گناه نگاه» و جامه تراز همرسانی و تلاش برای پاسداری از قرآن، دیگر دستاوردهای این نوشته است. در این دنباله، به نیاز فقهی جامه‌شناسی پیام، پیشینه لغزش در جامه دیداری، ویژگی جامه دیداری، تراز کوتاهی و بلندی پیام، «گناه نگاه»، زکات و پاک‌سازی نگاه از آسیب‌های نگاه، رسانه ترازو و دستاورد نوشته پرداخته‌ایم.

۲ نیاز به فقه جامه‌شناسی پیام

انسان برای برآوردن نیازها باید با چیزهای دیگری پیوند بگیرد. بخشی از نیازهای انسان، پیام‌ها هستند که هم محتوا و مایه پیام و هم قالب و جامه پیام، باید با سرشت انسان سازگار باشد. اگر دستگاه دریافت انسان، همانند یک آچار پنج ضلعی باشد و بلندی و کوتاهی ضلع و زاویه آنها گوناگون باشد، قالب و جامه پیام نیز باید یک مُهره پنج ضلعی با طول و زاویه ضلع‌های هم‌ساز با آچار باشد؛ وگرنه پیام به درستی دریافت نمی‌شود. زیرا یک آچار پنج‌گوش نمی‌تواند پیوند درستی با یک مهره چهارگوش بگیرد. حتی یک آچار پنج‌ضلعی با زاویه یا ضلع‌هایی ناساز با زاویه و ضلع‌های مُهره پنج‌ضلعی، نمی‌تواند با آن جفت شود. پس جامه پیام، باید با دستگاه گیرنده پیام سازگار و جفت باشد. این‌که انسان چیست و چند بر و لایه دارد و هر بر و لایه چه اندازه و ویژگی‌هایی دارد و چه پیوندی با دیگر لایه‌ها دارد، برای ما روشن نیست تا بتوانیم پیرامون و پهنه و حجم و دیگر مهندسی‌ها را به گونه «پیشرفته» بر انسان انجام بدهیم. ولی مهندس سخت‌افزار رایانه یا نرم‌افزار آن، به روشنی می‌داند آن رایانه یا آن برنامه، چند بخش دارد و هر بخش چه ویژگی‌هایی دارد. برآوردن نیازها اگر بخواهد به گونه‌ی پیشرفته باشد، باید بر پایه انسان شناسی پیشرفته باشد. پیام نیز اگر بخواهد به گونه پیشرفته همرسانی شود، باید برپایه انسان شناسی پیشرفته باشد؛ هم در مایه پیام و هم در جامه پیام و هم در فرایند همرسانی. مایه پیام باید چه آمیزه‌ای از نیازها را در خود داشته باشد؟ تا پاسخگوی نیازهای پیشرفته امروز ما باشد؟ قالب و جامه پیام باید از هر کدام از گیرنده‌های حواس پنج‌گانه ما چه اندازه بهره ببرد تا جامه آن پیام، تراز و پیشرفته باشد؟ اگر پنج گیرنده‌ی حسی را به سان پنج ضلع یک پنج‌گوش بدانیم، طول هر ضلع و زاویه میان هر دو ضلع، باید چه اندازه باشد؟ کدام ضلع باید پایه اصلی سازنده قالب و جامه پیام باشد؟ یعنی رسانه باید همانند اینستا دیدپایه باشد یا همانند قرآن، واژه‌پایه؟ پیامد دیدپایه یا واژه‌پایه بودن قالب و

شکل ۱: بنیاد فقهی سامانه سایبری اسلام

جامه پیام بر گیرنده‌های پنج‌گانه حسی و نیز بر لایه‌های انسان چیست؟ برای نمونه اگر پیام‌های دریافتی ما دیداری باشند، چه پیامدی بر لایه دل، اندیشه یا خرد خواهند داشت؟ چنین شناخت پیشرفته‌ای از انسان، طول ضلع‌ها و زوایای گیرنده‌های حسی و هم‌رسانی پیشرفته، چیزی فراتر از توان شناختی ما است و از این رو، باید آن را از کسانی آموخت که تنگناهای شناختی ما را ندارند؛ راه رسیدن به چنین شناختی «فقه» است. ازین‌رو روش ما در دستیابی به این نوشتار، بیشتر، فقهی و بر پایه این سخن امیرالمؤمنین (ع) است (شکل ۱): «الْعُقُولُ أَئِمَّةُ الْأَفْكَارِ وَ الْأَفْكَارُ أَئِمَّةُ الْقُلُوبِ وَ الْقُلُوبُ أَئِمَّةُ الْحَوَاسِّ وَ الْحَوَاسُّ أَئِمَّةُ الْأَعْضَاءِ» ([۵]، ج ۱، ص ۲۰۰). عقل‌ها، امامان فکرها هستند و فکرها، امامان دل‌ها هستند و دل‌ها امامان حس‌ها هستند و حس‌ها، امامان عضوها هستند.

این فرمایش نشان می‌دهد که انسان و نیز جامعه، پنج لایه دارد، لایه حیاتی نیز «خرد» است و این خرد، چیزی جز «اندیشه»، و بلکه امام آن است و اندیشه هم امام دل است، دل نیز امام حس (شبکه هم‌رسانی) است و حس نیز امام عضو است ([۱]، ص ۶۸ تا ۸۷).

۳ پیشینه لغزش در جامه دیداری

برای پی بردن به ویژگی‌های جامه «دیداری» و «واژگانی» پیام و پیامدهای دیدپایه یا واژه‌پایه شدن جامه پیام، در آغاز نگاهی به پیشینه پیام‌های «دیدپایه» و ریشه اینستاگرام می‌اندازیم. یادآور می‌شویم که در اینجا به شناخت مایه پیام نمی‌پردازیم و تنها «جامه» پیام را بررسی می‌کنیم. انسان آمیزه‌ای از توانش برانگیزندگی درونی و برانگیختگی از برون است و توازن این دو نباید به هم بخورد. از آنجا که پیام دیداری توان بسیاری در برانگیخته کردن انسان از بیرون دارد، پیامد کاربست زیاد آن، پندار بی‌نیاز بودن از برانگیزندگی درونی و کاهش ورزیدگی پیشران برانگیزاننده درونی است. اینک به دو واکنش حضرت موسی در برابر دو پیام

گوناگون دیداری و نادیداری می‌پردازیم تا توان برانگیزندگی پیام‌های دیداری روشن شود:

۱.۳ ویژگی روان‌تَنی انسان

«شنیدن کی بود مانند دیدن؟» خدای راستگو و آفریدگار جهان، به موسای پیغمبر (درودش باد) فرمود که سامری پس از بیرون آمدن تو، مردمت را گمراه کرد («و أَضَلَّهُم السّامری» [۴]، طه، ۸۵). با این‌که گوینده خدا است و شنونده هم پیغمبر بزرگ خدا است و روش پیام‌رسانی هم وحیانی و استوارترین شناخت است و پیام هم یک سوگ بزرگ است، در اینجا از خشم یا اندوه ویژه حضرت موسی گزارشی نمی‌شود! ولی هنگامی که خدا از بازگشت ([۶]، ج ۸، ص ۵۲). موسی (ع) سخن می‌گوید و ایشان به میان داستان می‌آید و این سوگ بزرگ را به چشم خود می‌نگرد، خشم سترگی از وی گزارش می‌شود: و هنگامی که موسی خشمناک و اندوهناک به سوی مردمش بازآمد... نوشته‌ها را بیفکند و سر برادرش را به سوی خویش کشان، به دست گرفت؛ «وَ لَمَّا رَجَعَ مُوسی إِلی قَوْمِهِ غَضْبانَ أَسِفاً ... أَلْقَی الْأَلْواحَ وَ أَخَذَ بِرَأْسِ أَخیهِ یَجُرُّهُ إِلَیهِ» ([۴]، اعراف، ۱۵۰).

آری این ویژگی روان‌تنی انسان است. هر چند که کسانی مانند أمیرالمؤمنین (ع) و اهل بیت (ع) هم هستند که اگر همه پرده‌ها هم کنار رود، چیزی به باورشان افزوده نمی‌شود. («لَوْ کُشِفَ الْغِطَاءُ مَا ازْدَدْتُ یقِیناً» [۷]، ص ۴۱۵). شیعیان امیرالمؤمنین (ع) و پسینیان سلمان نیز کمابیش به این ویژگی آراسته‌اند: ای علی! شگفت‌ترین مردم از دید ایمان و بزرگترین مردم از دید یقین، گروهی در آخرالزمان هستند که نزد پیامبر (ع) نیستند و حجت خدا (عج) نیز از آنان پوشیده است؛ پس آنان به سیاهی‌ای (نوشته) بر سفیدی (کاغذ) ایمان می‌آورند؛ «یا عَلِیُّ أَعْجَبُ النَّاسِ إِیمَاناً وَ أَعْظَمُهُمْ یقِیناً قَوْمٌ یکونُونَ فِی آخِرِ الزَّمَانِ لَمْ یَلْحَقُوا النَّبِیَّ وَ حُجِبَ عَنْهُمُ الْحُجَّةُ فَآمَنُوا بِسَوَادٍ عَلَی بَیاض» ([۸]، ج ۴، ص ۳۶۶).

۲.۳ یهود، بنیاد صهیونیستاگرام

خدا بنی اسرائیل را با معجزه بزرگ و آشکارِ «شکافتن دریا» از دست فرعونیان رهایی بخشید، ولی آنان پس از گذر از دریا، کسانی را دیدند که درگیر پرستش بت‌های‌شان بودند ([۴]، اعراف، ۱۳۸) آنان به سرورمان موسی گفتند که تو هم چنین خدایی همانند خدای آنان برای ما بیاور!؛ «قالُوا یا مُوسَی اجْعَلْ لَنا إِلهاً کما لَهُمْ آلِهَةٌ» ([۴]، اعراف، ۱۳۸). موسی نپذیرفت و آنان هم گفتند که ما نیز به تو ایمان نمی‌آوریم تا خدا را نمایان به ما نشان بدهی؛ «لَنْ نُؤْمِنَ لَک حَتَّی نَرَی اللَّهَ جَهْرَةً». ([۴]، بقره، ۵۵). این درخواست، نه تنها از سوی مردم، بلکه از سوی هفتاد همراه برگزیده حضرت موسی نیز انجام شد[۱] ([۴]، اعراف، ۱۵۵). خدا

[۱] حضرت موسی نیز درخواست دیدن خدا کرد: «... أَرِنی أَنْظُرْ إِلَیک قالَ لَنْ تَرانی» ([۴]، اعراف، ۱۴۳). المیزان می‌گوید «أرنی انظر» یعنی پی بردن به خدا با علم حضوری؛ مانند دانش ما به خویش و حالات خودمان؛ نه علم حصولی. اگر چنین است، پاسخ نباید نفی همواره و نفی آن در آینده (فسوف) باشد؛ چون به این معنا خدا در مراتب گوناگونی دریافتنی است؛ چنانکه حضرت محمد (ص) در معراج خدا را با دل دید: «ما کذب الفؤاد ما رأی افتمارونه علی ما یری و لقد رَآه نزلة اخری» ([۴]، نجم، ۱۱ تا ۱۳). المیزان می‌گوید «لَن ترانی» یعنی در این دنیا دیدن من شدنی نیست ولی در آخرت می‌بینی. یعنی زمان پسین و پیشین در تراز مقام و عالمیت حضرت موسی کارا است که تا آخر زندگی این جهانی توان دریافت حضوری از خدا ندارد و در رستاخیز به این توان می‌رسد؟ المیزان می‌گوید توبه حضرت موسی هم تنها برای درخواست دیدن در دنیا بود ([۶]، ج ۸، ص ۳۱۳). به هر روی علی

تندری از آسمان بر آنان زد و آنان مردند. پس از مرگ، خدا آنان را زنده کرد ([۴]، بقره، ۵۶) و باز معجزات آشکار بسیاری مانند «مَنّ و سَلوی» برای آنان انجام داد. آری آنان مردند؛ ولی هوس خدای دیدنی در آنان نمرد و خدای نادیدنی را با آن همه معجزه روشن، نپذیرفتند و به جای ایمان به الله، تندیس گوساله‌ای را به خدایی برگزیدند. «ثُمَّ اتَّخَذُوا العِجلَ مِن بَعدِ ما جاءَتهُمُ البَيِّناتُ» ([۴]، نساء، ۱۵۳). از این بالاتر، گفته شد که خدای موسی فراموش شده است. ([۴]، طه، ۸۸) خدا توبه آنان را مرگ و کشتار دانست. «فَتوبوا إِلى بارِئِكم فَاقتُلوا أَنفُسَكم» ([۴]، بقره، ۵۴). خدا تا جایی که می‌شد، نیاز یهود به پیام‌های دیداری را پاسخ داد: «و قالَ لَهُم نَبِيُّهُم إِنَّ آيَةَ مُلكِهِ أَن يأتِيَكمُ التّابوتُ فيهِ سَكينَةٌ مِن رَبِّكُم» ([۴]، بقره، ۲۴۸)؛ ولی باز هم زیاده خواهی کردند. دنباله چنین رویکردی، به گسترش بی‌رویه هنرهای دیداری و برپا کردن شرکت‌های بزرگ «هالیوود» و «دیزنی» می‌انجامد.

۴ ویژگی جامه دیداری

پیام دیداری چیزی است که «دیده» می‌شود ولی آن بخش از پیام که به آن «نگریسته» و «نگاه» شود، کانون آگاهی و پردازش و دریافت ما از پیام است که در عربی به آن «نظر» می‌گویند: «فانظُر ماذا تَرَی» یعنی در آنچه چه «می‌بینی»، «خیره‌شو». «دیدن» یعنی چشم به چیزی افتادن و «نگریستن» یعنی خیره شدن به چیزی که طبعاً با توجه و نیت همراه است. فرق دیدن با نگاه کردن و سودهی نیت به نگاه، در منابع دینی به این گونه خود را نشان داده است: «نگاه کردن مرد به بدن زن نامحرم، چه با قصد لذّت و چه بدون آن، حرام است. نگاه کردن به صورت و دست‌ها، اگر به قصد لذّت باشد حرام است، ولی اگر بدون قصد لذّت باشد مانعی ندارد.»[۲] ([۱۱]، م ۵۱۰).

با این که عضو بینایی، در هر دیدن، صدها داده را به مرکز لایه حس؛ یعنی مغز می‌رساند، ولی این داده‌ها، باید از یک سافی درونی بگذرند تا به چرخه کارایی و کاربرد برود. این سافی گویا در لایه دل ما است و از خرد و نیت ما دستور یافته است. اگر داده دیداری کسی با خواست و نیت او همانند نباشد، دل آن را پس می‌زند و نمی‌تواند وارد چرخه لایه فکر و عقل شود. اگر دل داده‌های دیداری را بپسندد ولی آن داده‌ها با عقل سازگار نباشد، در اینجا لایه فکر و لایه عقل، با آن درگیر می‌شوند؛ ولی گویا در اینجا، آن چشم‌انداز دلخواه، از لایه دل پاک نشود، گاه و بیگاه به ستیز با فکر و عقل برخیزد. اگر داده دیداری با دل و فکر و عقل (نیت) سازگار باشد، آن داده به دانش و منش می‌انجامد و چیزهای ناسازگار با خود را کنار می‌زند.[۳] جامعه دیداری ویژگی‌هایی دارد که نشناختن ویژگی‌های آن و بکارگیری نادرست آن، دستگاه شناخت و زندگی را

(ع) می‌فرماید «ما رایت شیئا الا ورأیت اللّه قبله وبعده» ([۷]، ج ۱، ص ۱۱۵) و نیز «رأیته فعبدته لم أعبد ربّاً لم أره» ([۱۰]، ج ۱، ص ۳۳۱).

[۲] در پیام شنیداری نیز نیت بسیار کارگشا است: «إِذَا طابَقَ الكَلَامُ نِيَّةَ المتَكلِّمِ قَبِلَهُ السّامِعُ و إِذا خالَفَ نِيَّتَهُ لَم يَقَع مَوقِعَهُ». ([۷]، ص ۱۳۱). آن سخن کز دل برآید لاجرم بر دل نشیند.

[۳] چنانکه امیرالمؤمنین (ع) می‌فرماید نگاه نخست بهره تو است و نگاه دوم بر تو است؛ نه بهره تو و نگاه سوم تیری زهرآلود از تیرهای شیطان است. ([۱۲]، ج ۲، ص ۲۰۲). امام صادق (ع): «أَوَّلُ النَّظرَةِ لَک و الثّانِيةُ عَلَيک و لا لَک و الثّالِثَةُ فِيها الهَلاکُ». ([۸]، ج ۳، ص ۴۷۴). امام صادق (ع): «النَّظرَةُ بَعدَ النَّظرَةِ تَزرَعُ فِی الْقَلبِ الشَّهوَةَ و کفَی بِها لِصاحِبِها فِتنَةً». ([۸]، ج ۴، ص ۱۸). نگاهِ پس از نگاه، در دل هوس می‌کارد و برای ایجاد فتنه برای صاحبش بس است.

دچار آسیب‌های بسیاری می‌کند.

۱.۴ مرزشکنی جامه دیداری

خدا در جهان مرزهای گوناگون طبیعی و زبانی آفریده است و بنیاد زبان واژگانی انسان، اختلاف زبان و مرز داشتن زبان‌ها است: «وَ مِنْ آياتِهِ خَلْقُ السَّمَاوَاتِ وَ الْأَرْضِ وَ اخْتِلَافُ أَلْسِنَتِكُمْ وَ أَلْوَانِكُمْ إِنَّ فِي ذَلِكَ لَآيَاتٍ لِلْعَالِمِينَ» ([۴]، روم، ۲۲). در این مرزبندی زبان واژگانی، نشانه‌هایی برای دانایان است. این مرزها واقع‌بینانه و برای کاهش چپاول ستم‌گران بوده است؛ چون واقعیت این بوده است که در بیشتر روزگاران، ستم‌گران بر زمین فرمان می‌رانده‌اند و اگر زبان ستمگر و ستم‌دیده یکی بود، فرهنگ و باور ستم‌گران نیز به سادگی بر فرهنگ ستم‌دیدگان می‌چربید؛ چنان‌که اگر امروز زبان فارسی مرز فرهنگی ما با فرنگ را جدا نمی‌کرد، یورش بی‌فرهنگی آنان به ما بسیار آسیب‌ناک‌تر بود.

زبان و جامه دیداری برای همگان کمابیش یکسان است؛ چون هم دستگاه بینایی ما کمابیش یکسان است و هم دیدنی‌ها یکسان هستند؛ پس اختلاف زبان و مرز زبانی در آنجا برجسته نیست؛ در حالی که اختلاف زبان‌ها، یکی از آیات خدا است. زبان دیداری، کمابیش همگانی است و آن بخش از پیام‌های دیداری که خدا آفریده؛ یعنی آسمان و زمین، بسیار خوب و نشان‌گر خدا و آموزنده هستند. ولی پیام‌های دیداری‌ای ساختگی، همانند تندیس و فیلم‌هایی که دست‌کاری در جهان است، جای بررسی دارد.

۲.۴ پرچرب بودن زبان دیداری

چشم در هر نگاه، با سرعت نور، پیام‌های بسیاری را دریافت می‌کند. شتاب دریافت پیام‌های دیداری و شمار پیام‌های دریافتی در هر نگاه، بسیار بیشتر از شمار پیام‌های دریافتی واژگانی، در یک بازه زمانی یکسان است. از این‌رو پیام‌های دیداری بسیار پرچرب‌تر و سنگین‌تر هستند و به گوارش و پردازش بیشتری نیاز دارند. همان‌گونه که خوردن هر روزه گوشت، سنگ‌دلی می‌آورد، دیدپایه بودن پیام‌ها نیز بر دل، فکر و خرد ما سنگینی می‌کند.

۳.۴ نارسایی جامه دیداری در بنیادهای ارزش انسان و ایمان

جامه دیداری یک کاستی بزرگ دارد؛ این‌که در برابر چیزهای نادیدنی مانند خدا و گستره چیزهای پنهان و غیب و ارزش‌های معنوی و کیفی، لال و یا دچار کاستی بسیار است و این یعنی اساس شخصیت انسان که روح و ارزش‌های معنوی و ایمان به غیب است، در این جامه یا نمی‌آید یا فروکاست می‌شود. بنیاد دین «ایمان به غیب» است و غیب، نهان از چشم است! آیا با پیام دیداری می‌توانیم از «الذینَ یُؤمِنونَ بالغَیب» بهره‌مند شده، ایمان به غیب را بهینه گسترش داد؟ جامه دیداری پیوند ما با غیب را نیرومند نمی‌کند؛ بلکه روزبه‌روز غیب را از ما دورتر می‌کند.

۴.۴ زبان‌آوری ستم‌گران در پیام‌های دیداری

خدا ما را آفریده است و زبان دارا و ندار و زبان شاه و داه (بنده) کمابیش یکسان است. زبان موسی و فرعون کمابیش هم‌توانش است. ولی در دیداری، توانش زبانی یکسان نیست. آیا زبان دیداری یک ستم‌دیده‌ی نادار با زبان دیداری یک ستمگرِ دارا یکی است؟ زبان دیداری فلسطین با زبان دیداری صهیون‌ها و هالیوود یکی است؟ اگر جامه‌ی پایه برای زبان، جامه دیداری باشد، ستم‌گران زبان‌دان و زبان‌دار هستند و ستم‌دیدگان، بی‌زبان! و این بزرگترین ستم است! بی‌گمان شرکت‌های بزرگ دارای زبان دیداری مانند «دیزنی» و «هالیوود» را نمی‌توان با زبان دیداری مستضعفان جهان یکسان پنداشت. مستکبران به گونه آگاهانه یا در بافت طبیعی گمراه‌گری، در پی کاهش هر چه بیشتر زبان واژگانی از بافت پیام دیداری هستند و برخی از پویانمایی‌ها؛ همانند «پلنگ صورتی» و «موش و گربه» را می‌توان در این راستا بررسی کرد. صهیونیزم روزبه‌روز در حال گسترش داده‌نگاری (Infography) و کاهش زبان واژگانی و برچیدن مرزهای زبانی هستند. آنان جامه‌های دیداری را با سوگیری‌ها ویران‌گر فرنگی، بر تن پیام‌ها می‌کنند و این زبان را در همه جا می‌گسترانند.

اگر به جای میان‌داری و استخوان‌بندی جامه واژگانی در جامعه، جامه دیداری میان‌دار بشود، دیگر قرآن نمی‌تواند معجزه کند و معجزه‌های دیداری به میان می‌آید و پیغمبران آن جامعه نیز، چهره‌هایی خواهند بود که معجزه آنان جادوی دیداری است: «سَحَروا أعيُنَ النّاس» با میان‌داری جادوی هری‌پاتر، مرد عنکبوتی و بازی‌های رایانه‌ای.

۵.۴ بررسی تابانی جامه واژگانی و تاری جامه دیداری

در زبان و جامه واژگانی هر واژه تعریف و بوم و مرز ویژه‌ای دارد. ولی در جامه دیداری، زمینه برداشت‌های گوناگونِ برآمده از سلیقه‌های رنگی و شکلی و پس زمینه‌های درونی بسیار گسترده می‌شود. پیام کوتاه، روشن و بُرّا، برتر از پیام دراز و آزارنده است و سخن باید سدید، استوار و بی‌رخنه باشد. «وَ قولوا قَولاً سَديداً» ([۴]، احزاب، ۷۰). این در حالی است که جامه دیداری؛ به‌ویژه در چیزهای ارزشی و معنوی بسیار مبهم است. این تاری و «بَهْم»، هم‌رسانی ما را «بهائمی» می‌کند. بی‌اعتنایی به دیدپایه شدن پیام در پرتو این آیه نیز یافت می‌شود: آیا می‌پنداری بیشترشان می‌شنوند و می‌خِرَدند؟ آنان جز همانند چارپایان نیستند؛ بلکه گمراه‌تر. «أَم تَحسَبُ أَنَّ أَكثَرَهُم يَسمَعونَ أَو يَعقِلُونَ إِن هُم إِلاّ كالأَنعامِ بَل هُم أَضَلُّ سَبيلا» ([۴]، فرقان، ۴۴). چنان‌که در آیه دیگری یکی از رازهای دوزخی شدن برخی، نشنیدن پیام‌های شنیداری است: و گفتند اگر می‌شنیدیم یا خردورزی می‌کردیم، از گروه دوزخیان نبودیم. «وَ قالُوا لَوْ كُنَّا نَسمَعُ أَو نَعقِلُ ما كنَّا فی أَصحابِ السَّعير» ([۴]، ملک، ۱۰). در اینجا نیز پیام دیداری رکن رستگاری نیست.

از این زاویه بهتر می‌توان هنر و معماری اسلامی و غربی را بازخوانی کرد. هنر اسلامی بیشتر واژه‌پایه است؛ چنان‌که خطاطی کانون زیور ساختمان‌های دینی است و هنر است و آهنگ و آواز نیز بر کانون واژگان و سخن رشد می‌کند؛ چه در تلاوت قرآن و چه در ستایش خاندان پیغمبر و چه در مهر و شوقی پاک میان انسانها؛ نه این که خود آهنگ و نوا، جای خود واژه بنشیند و موسیقی بی‌کلام پی گرفته شود. مسیحیتِ دچار برخی کژی‌ها و یا دین‌واره‌های ساختگی بشری، اگر بخواهند به‌گونه واژه‌پایه هم‌رسانی کنند، کاستیها و

تناقضات آنها (مانند یک خدایی در عین سه خدایی) رو می‌آید و ناگزیرند که بر جهان مفاهیم و منطق گفتگو، تاری و ابهام بپاشند. ولی پیام اسلام، کوتاه، روشن و گویا است. اسلام، «مایه» درست را در «جامه» روشن واژگانی پیشکش می‌کند. زبان اسلام، «اذان» و واژگانی است و زبان ترسایی، «ناقوس» و آهنگ. در حرم‌ها و مسجدهای اسلامی بیشتر، از جامه واژگان و نوشته برای پیام‌ها بهره می‌برند و در دیرها از جامه دیداری و نگارگری و تندیس (التماثیل) که دید سه‌بُعدی (سه‌بر) می‌دهد. هنگامی که به دیرها می‌روی، یورش جامه دیداری پردازشگر مغز را پر می‌کند تا توان ارزیابی برخی باورهای نادرست ترسایان کاهش یابد. آهنگ هم همین آگاهی‌کاهی و به‌خود واداشتن را دارد. از این‌رو اسلام با آهنگ، نقاشی و تندیس‌سازی به گونه سنجیده روبرو شده است؛ نه ولنگارانه.

۶.۴ مرزبانی انسان در زبان دیداری و زبان واژگانی

دانستیم که پیام‌های دیداری بسیار پرمایه هستند و هزاران مایه را با یک دیدن به سرعت نور، به درون انسان می‌برند؛ مانند این که ما یک دهان داریم ولی با چندین قاشق و با شتاب بسیار بخواهیم خوراک را در آن بفشاریم. ازین‌رو خدا مرزبانی پیام‌های دیداری را پلک چشم و گُمرک و مرزبانی بیرونی گذاشته است. چون هنگامی که صدها و هزاران پیام به درون ما می‌رود، کار پردازش درونی بسیار دشوار می‌شود و ما به پردازش و پیرایش و ویرایش بخشی از مایه‌های دریافت شده نمی‌رسیم و این پیام‌ها بخش خودآگاه ما را کوچک کرده، مهندسی سازندگان پیام‌های دیداری را در درون ما افزایش می‌دهند و ناخودآگاه ما را در چنبره مهندسی بیرونی دیگران گذاشته ما را دچار نسنجیدگی و ناهماهنگی می‌کند و کمابیش رفتارمان مانند «الَّذِي يَتَخَبَّطُهُ الشَّيْطَانُ مِنَ الْمَسِّ» ([۴]، بقره، ۲۷۵) می‌شود. جامعه‌ای که بیش از اندازه دچار زبان دیداری بشود، به آسانی دچار یورش نرم دشمنانش شده است.

ما اگر قرمه سبزی بخوریم، توان شناخت خودآگاه ما این است که بگوییم خیلی خوشمزه بود یا چند مزه جداگانه را هم بربشمریم، ولی شکم ما ده‌ها و صدها چیز را بی‌آنکه ما آگاه باشیم، گوارش کرده و به تن ما روانه می‌کند؛ حتی اگر زهری در خوارک باشد که ما مزه‌اش را نشناخته‌ایم. در دریافت پیام دیداری نیز ما ده‌ها چیز را با هم دریافت می‌کنیم؛ هر چند داوری آگاهانه ما درباره آن، این باشد که این چشم‌انداز زیبا بود؛ ولی در دلِ زیبایی این چشم‌انداز، ده‌ها پیام دیگر نیز دریافت شده است که برای ما کمابیش ناخودآگاه است. ولی در زبان و جامه شنیداری، مرزبان، درونی است و گوش ما پلک ندارد. زیرا هم شتاب دریافت امواج شنیداری ۸۷۵ هزار برابر کمتر از شتاب پرتوهای دیداری است و هم انباشت پیام‌هایی که در یک بار شنیدن دریافت می‌کنیم، بسیار کمتر از پیام‌های دیداری است.

پیام واژگانی را می‌توان مانند مرزبانی درون کشور (فرودگاهی) دانست که شمار مسافران اندک است و آنان باید از جای ویژه مرزبانی فرودگاه بگذرند ولی پیام دیداری همانند سرازیر شدن انبوهی از بیگانگان به مرزهای کشور است که اگر وارد کشور بشوند، دیگر نمی‌توان به سادگی آنان را یافت و شناخت و باید دم مرز این کار را انجام داد؛ یعنی مرزبانی بیرونی در اینجا کارامد است.

یورش انبوه داده‌های پیام دیداری به ذهن و تغذیه ناخودآگاه ذهن از این داده‌ها، آفرینش چشم و گوش را نیز دگرگون کرده است؛ به‌گونه‌ای که گوش را نمی‌توان به سادگی بست ولی چشم را می‌توان با پلک بست.

خدا به فرزندان آدم می‌فرماید: اگر چشمت تو را به‌ستوه آورد که به آنچه ناروا است بنگری، خدا تو را با دو پوشش (پلک) یاری کرده است؛ پس پلک فروبند و ننگر!؛ «إِنْ نَازَعَکَ بَصَرُکَ إِلی بَعْضِ مَا حَرَّمْتُ عَلَیک، فَقَدْ أَعَنْتُک عَلَیهِ بِطَبَقَینِ، فَأَطْبِقْ وَ لَا تَنْظُرْ» ([۱۳]، ج ۱۵، ص ۵۰۲).

۵ تراز کوتاهی و بلندی پیام

جامه تراز باید روشن، بُرّا و کوتاه باشد و با درازگویی سازگار نیست. ازین‌رو شیوه تراز گزارش یاری بینوایان، شیوه قرآن («وَ یُطْعِمُونَ الطَّعامَ عَلی حُبِّهِ مِسْکیناً وَ یتیماً وَ أَسیراً إِنَّما نُطْعِمُکُمْ لِوَجْهِ اللَّه» [۴]، انسان، ۸ و ۹). است تا شیوه ویکتور هوگو. البته گاهی نیاز است که چیزها را بسیار باز کرد که آن نیز جای خود دارد؛ ولی رویه نباید به گونه‌ای شود که ذائقه زبانی مردم از دریافت پیام تراز («أحسَنَ الحَدیثِ». [۴]، زمر، ۲۳) وازده شود. یکی از لغزش‌گاه‌های کلاب‌هوس، همین درازگویی بسیاری از برنامه‌ها از ۱۰ تا ۲۰ ساعت[۴] و سِرتِقی در آن است. شیب‌گذاری «کلاب‌هوس» به سوی درازگویی و ستیزگویی و بازوسازی برای شیطان است: «وَ إِنَّ الشَّیاطینَ لَیوحُونَ إِلی أَوْلِیائِهِمْ لِیُجادِلُوکم». ([۴]، انعام، ۱۲۱) خدا نمی‌فرماید خواست شیاطین «لِیقاتِلوکم» و جنگ و کشتار شما است؛ بلکه می‌فرماید خواست آنان «لِیُجَادِلوکم» و ستیزگویی است. چون ستیز، تن کسی را می‌زند و ستیزگویی، روان و ایمان وی را می‌زند و ستیزگویی خوی ابلیس است. (الْمِرَاءُ ... خُلُقُ إِبْلِیسَ). ([۱۵]، ص ۱۷۱) [۵]

کوتاه بودن پیام‌ها در ساختار توئیتر، بسا از درازگویی کلاب‌هوس هم بیمبارتر باشد؛ چون در آنجا افزون بر این که تبیین انجام نمی‌شود، ادعاکده است و شیب این ساختار ادعاپایه، به سوی دنباله‌رو پروری است (و الشُّعَراءُ یَتَّبِعُهُمُ الغاوُونَ أَ لَم تَرَ أَنَّهُم فی کُلِّ وادٍ یَهیمونَ و أَنَّهُم یَقُولونَ ما لَایَفعَلون. [۴]، شعراء، ۲۲۴ تا ۲۲۶). پس باید در پی ساختار تبیین‌پایه و بدون کم‌گویی یا زیادگویی بود؛ چیزی که کمابیش در ساختار «ایتا» می‌توان یافت.

۶ گناه نگاه

چشم تنها دیدنی‌ها را می‌بیند و این یک کاستی است و می‌تواند سبب دور شدن از اصل باشد؛ زیرا خداوند دیدنی نیست؛ در این راستا، سخن امام حسین (ع) را می‌توان بررسی کرد: «تَرَدُّدِی فِی الآثَارِ یوجِبُ بُعْدَ الْمَزَارِ ... أَ یَکونُ لِغَیرِک مِنَ الظُّهُورِ مَا لَیسَ لَک حَتَّی یکونَ هُوَ الْمُظْهِرَ لَک ... عَمِیَتْ عَینٌ لَا تَرَاکَ عَلَیهَا

---

[۴] امیرالمؤمنین: «إِذَا تَمَ الْعَقْلُ نَقَصَ الْکَلَام» ([۱۴]، ص ۴۸۰). «وَ مَنْ کَثُرَ کَلَامُهُ کَثُرَ خَطَؤُهُ وَ مَنْ کثُرَ خَطَؤُهُ قَلَّ حَیاؤُهُ وَ مَنْ قَلَّ حَیاؤُهُ قَلَّ وَرَعُهُ وَ مَنْ قَلَّ وَرَعُهُ مَاتَ قَلْبُهُ وَ مَنْ مَاتَ قَلْبُهُ دَخَلَ النَّارَ» ([۱۴]، ص ۵۳۶ و [۵]، ج ۲، ص ۱۴). یکی از رازهای ناسزاگویی‌های بسیار در کلابهوس، همین پرگویی و لغزش بسیار و به دنبال آن، بی‌آزرمی است. برنامه‌های کلابهوس ساعت‌ها به درازا می‌کشد، ۵، ۱۰ و گاه تا ۲۰ ساعت که چه بسا آمیخته به ناسزاهای بسیار زشت است.

[۵] «ستیز»، تخم شر است (المراءُ بذرُ الشَّر. [۷]، ص ۳۳) و پیامد آن هم کورتر شدن گره‌ها و کینه‌ورزی بیشتر است (ثَمَرَةُ الْمِرَاءِ الشَّحْنَاءُ؛ [۷]، ص ۲۰۸). سِرتِقی، تباهی و حبط خوبی‌های گذشته و گناهی در رده پس از بت‌پرستی است: «حضرت محمد (ص): أَوَّلُ مَا نَهَانِی عَنْهُ رَبِّی بَعْدَ عِبَادَةِ الْأَوْثَانِ الْمِرَاءُ» ([۱۶]، ج ۲، ص ۱۳۹) بسیاری از دشمنان اسلام، مشکل فکری ندارند، کینه قلبی یا عناد عقلی دارند: «لَقَدْ حَقَّ الْقَوْلُ عَلیَ أَکثرَهِمْ فهُمْ لَا یُؤْمِنُون». ([۴]، یس، ۷).

رَقِیبا» ([۱۷]، ج ۱، ص ۳۴۸)؛ سرگشتگی در آفریدگان، دوری دیدار را درپی دارد ... آیا برای دیگران چیزی از آشکاری هست که تو نداشته باشی؟ تا او نمایاننده تو باشد؟ ... کور است چشمی که همواره درگیر دیدن آفریدگان است!

از این نگاه، هر چه تراز ایمان کسی بالاتر برود، دیدنی‌ها، می‌توانند به دوری وی از مهر ویژه الهی بینجامند؛ زیرا سنخ رحمت بیشینه، دیدنی نیست و هر کس به دیدن پناه ببرد، از مهر بیشینه خدا دور می‌شود؛ به‌ویژه اگر هویت وی، «هویت نِگَرا» (الناظر) یا «هویت نگریسته» (المنظور) بشود؛ چنان‌که برخی چهره‌های اینستاگرامی چنینند:

پیامبر خدا (ص) می‌فرماید: «لَعَنَ اللَّهُ النَّاظِرَ وَ الْمَنْظُورَ إِلَیهِ» ([۱۸]، ج ۲، ص ۲۸). خدا از مهر خود دور می‌کند آنکه [هویتش] نگرنده یا نگریسته شده باشد. همین روایت، از امیرالمؤمنین (ع) هم آمده است. ([۱۹]، ج ۱۴، ص ۲۷۱) این فرمایش در برابر «أَفَلا یَنظُرونَ إِلَی الإِبِلِ کیفَ خُلِقَت» ([۴]، غاشیة، ۱۷) نیست؛ زیرا در اینجا هویت بیننده «الناظر: نگرا» نمی‌شود، بلکه «نظر» و نگاه ما برای دیدن چیز درست و نیز درست دیدن؛ یعنی گذر از دیده و رسیدن به ندیده (خدا و توان آفرینش‌گری خدا) است.

۷ زکات نگاه

چشم، دهش نیک خدا به ما است و چشم نداشتن چیز خوبی نیست، ولی باید چشم را از کاستی سرشتی و «گناه نگاه» و دورشدن از تراز رشد، پاک کرد. در اینجا منظور از «گناه نگاه»، نگاه کردن به چیز حرام نیست؛ بلکه نگاه‌پایه شدن جامه پیام و همرسانی است. راه پاک‌سازی و زکات چشم و رهایی از لعنت گناه نگاه چیست؟ حضرت امام صادق (ع) می‌فرماید: «فَزَکاةُ الْعَینِ النَّظْرَةُ بِالْعِبْرَةِ» ([۲۰]، ص ۵۱)؛ پاک‌سازی نگاه، در نگاه کردن همراه با گذر [از دیده‌ها] است. زکات چشم، نگاهی است که در پس آن پردازش دیده‌ها و خردورزی باشد و از پوسته محسوسات بگذرد و به مغز و معنا برسد. بهترین راه گذر از پوسته محسوسات آن است که اندازه دریافت‌های دیداری را با «چشم‌پوشی و غض بصر» بکاهیم و بیشتر به پیام واژگانی؛ مانند قرآن پناه ببریم.

افزون بر کاستی «گناه نگاه»، کاستی دیگر نگاه آن است که خدا به چشم، توان دیدن «غیب» و «خدا» را نمی‌دهد؛ آری، دیده‌ها او را در نمی‌یابند و او دیدگان را درمی‌یابد (لا تُدْرِکُهُ الْأَبْصارُ وَ هُوَ یُدْرِکُ الْأَبْصارَ. [۴]، انعام، ۱۰۳). پس باید به اندازه بایسته و برای بالا رفتن از نردبان نگاه و رسیدن به مغز و معنا، از آن بهره برد؛ نه این که هویت‌مان نگاه‌پایه بشود. شاید از همین رو حضرت یحیی (ع) می‌فرماید که مرگ در نزد من، خواستنی‌تر از نگاه نابایسته است «الْمَوْتُ أَحَبُّ إِلَیَّ مِنْ نَظْرَةٍ بِغَیرِ وَاجِبٍ». ([۲۰]، ص ۱۰).

پس خود نگاه، نخجیرگاه اهریمن است. («الْعُیونُ مَصائِدُ الشَّیطانَ» ([۷]، ص ۴۱. و [۲۱]، ص ۲۶۰) و «لَمْحَ الْعُیونِ مَصَائِدُ الشَّیطَان» [۲۲]، ص ۱۵۱). نگاه تیری از تیرهای اهریمن است («النَّظَرُ سَهْمٌ مَسْمُومٌ مِنْ سِهَامِ إِبْلِیس». [۲۳]، ص ۹۳)؛ زیرا نگاه، بستر سطحی‌شدگی است و اگر زکات آن پرداخت نشود، به سطحی شدن ذائقه شناختی (پزیتیویزم) و نیز ذائقه گرایشی می‌انجامد. پس هر کس که بخواهد با سلامت از این شکارگاه بگذرد، باید زره زکات نگاه را بر چشم کند. به هر میزان که از داده‌های نگاهی بکاهیم، از آسیب نگاه

در سطحی‌شدن ما نیز کاسته می‌شود و بستر ژرفنگری و درک شگفتی‌های عالم برای ما فراهم می‌شود. از این‌رو حضرت محمد (ص) می‌فرماید چشمان‌تان را درویش کنید تا بی‌گمان شگفتی‌ها را بنگرید. [۶] «غُضُّوا أَبْصَارَكُمْ تَرَوْنَ الْعَجَائِبَ» ([۲۰]، ص ۹).

کارکرد «ناظر» و دیداری شدن کسی در بستر رسانه‌های دیداری مانند اینستاگرام، تنگ شدن زمینه برای اندیشیدن و سطحی نگری است و ترویج این رسانه در درون جامعه یعنی اسارت اندیشه و آزادی و جلوگیری از پرورش کسانی مانند ابوذر و تبعید آنان از جامعه! چون بیشترین پرستش ابوذر، «اندیشیدن و عبرت گرفتن» بود. «كَانَ أَكثَرُ عِبَادَةِ أَبِي‌ذَرٍّ خَصْلَتَينِ؛ التَّفَكُّرَ وَ الِاعْتِبَارَ» ([۲۵]، ج ۱، ص ۴۲).

چشم دهش خدا است؛ چنان‌که دیگر اعضای تن نیز دهش خدا است، ولی «چیزی در تن، کمتر از چشم، سپاس‌برانگیز نیست؛ پس خواسته‌اش را ندهید که شما را از یاد خدای عزیز و جلیل باز می‌دارد!». «لَيسَ فِي الْبَدَنِ أَقَلُّ شُكراً مِنَ الْعَينِ فَلَا تُعْطُوهَا سُؤْلَهَا فَتَشْغَلَكُمْ عَنْ ذِكرِ اللَّه عَزَّ وَ جَل» ([۲۵]، ج ۲، ص ۶۲۹).

چرا باید دیده را درویش کرد؟ چون «هر چه دیده بیند دل کند یاد» چنان‌که امام صادق (ع) می‌فرماید که چشم جاسوس دل و پیام‌رسان عقل است؛ پس چشم را از آنچه سزاوار دین نیست و دل آن را ناخوش می‌دارد و عقل آن را پس‌می‌زند، فروبند؛ «العَينُ جَاسُوسُ الْقَلْبِ وَ بَرِيدُ الْعَقْلِ فَغُضَّ بَصَرَكَ عَمَّا لَا يَلِيقُ بِدِينِك وَ يَكرَهُهُ قَلْبُك وَ يُنْكِرُهُ عَقْلُك» ([۲۰]، ص ۹).

بر پایه سخن معصوم (ع)، برخی از پیامدهای مهار چشم، آسودگی دل («مَنْ غَضَّ طَرْفَهُ اَراحَ قَلْبَهُ».[۲۶]، ص ۶۶۳) و کاهش اندوه («مَنْ غَضَّ طَرْفَهُ قَلَّ أَسَفُهُ وَ أَمِنَ تَلَفَه». [۲۶]، ص ۶۶۳) است و برخی از آسیب‌های چشم، آشفتگی خاطر و رشک («مَنْ أَطْلَقَ نَاظِرَهُ أَتْعَبَ خَاطِرَهُ مَنْ تَتَابَعَتْ لَحَظَاتُهُ دَامَتْ حَسَرَاتُهُ». [۲۳]، ص ۹۳)، تباهی («مَنْ أَطْلَقَ طَرْفَهُ جَلَبَ حَتْفَهُ». [۲۶]، ص ۶۶۳)، در پی داشتن رشک دیرپا («كَمْ مِنْ نَظْرَةٍ أَوْرَثَتْ حَسْرَةً طَوِيلَةً». [۲۷]، ج ۱، ص ۱۰۹) و برپا کردن کشتگاه هوس است. [۷]

۸ رسانه تراز؛ رفتار پنج لایه

افزون بر بهینگی مایه پیام، جامه پیام نیز باید به سوی بهینگی برود. هر یک از جامه‌های پیام، گستره‌ها و تنگناهای ویژه‌ای دارند که اگر در هم بپیوندند، ما را به جامه تراز هم‌رسانی می‌رسانند.

جامه تراز برای هم‌رسانی همگانی، جامه رفتار است که می‌تواند با بکارگیری همه لایه‌های نظام انسان و جامعه، بهترین، ژرف‌ترین و ماناترین پیام‌ها را هم‌رسانی کند. جامه رفتار، بسیار نیرومندتر از جامه واژگانی است؛ تا جایی که جامه گفتار در برابر آن، نکوهش می‌شود و حتی قرآن نیز بدون کارکرد و رفتار خاندان پیغمبر (درودشان باد) ترازبخش هدایت نیست. امام صادق (ع) بر رسانه تراز پافشاری می‌فرماید که برای مردم با چیزی جز زبانتان به سوی حق فراخواننده باشید؛ چرا که مردم باید تکاپو و راستی و پرهیز شما را بنگرند. «كونُوا دُعَاةً لِلنَّاسِ بِغَيرِ أَلْسِنَتِكمْ؛ لِيَرَوْا مِنْكمُ الِاجْتِهَادَ وَ الصِّدْقَ وَ الْوَرَعَ» ([۲۹]، ص ۳۵۹). اگر آن

[۶] چون علی (ع) مظهر عجایب است (یا مَظْهَرَ الْعَجَائِبِ. [۲۴]، ص ۲۰۸)، طبعاً چشم فروبندی می‌تواند سبب دیدار امیرالمؤمنین شود؛ چنانکه مشهور است علامه جعفری پس از ترک تماشای عکس ملکه زیبایی، توانست چهره امیرالمؤمنین (ع) را بنگرد.

[۷] امام صادق (ع): «النَّظْرَةُ بَعْدَ النَّظْرَةِ تَزْرَعُ فِي الْقَلْبِ الشَّهْوَةَ وَ كَفَى بِهَا لِصَاحِبِهَا فِتْنَةً». ([۸]، ج ۴، ص ۱۸). امام صادق (ع) از حضرت مسیح (ع): «إِيَّاكمْ وَ النَّظْرَةَ فَإِنَّهَا تَزْرَعُ فِي قَلْبِ صَاحِبِهَا الشَّهْوَةَ وَ كَفَى بِهَا لِصَاحِبِهَا فِتْنَةً». ([۲۸]، ص ۲۰۸).

گونه که دین می‌فرماید، ما خوش‌پوش و خوشرو باشیم، بوی خوش بزنیم، سخن نیکو و خوش‌آهنگ به زبان برانیم، «گوش خوبی» باشیم، مهمان دوست باشیم و با هم دست بدهیم، می‌توانیم با هر پنج حس لایه عضو هم‌رسانی کرده، دیگر لایه‌های سامانه هم‌رسانی (حس، قلب، فکر و عقل) را نیز با «صله رحم»، دوستی، هم اندیشی و اخلاص بیفزاییم و بدانیم که دیدار برادران ایمانی (مُلاقاةُ الإخوان) داروی بیمار عقل و باروری آن است؛ هر چند که بسیار کوتاه باشد ([۳۰]، ص ۹۴). از این نگاه همرسانه تراز، در جهان بیرون است نه تنگنای مجازی. چه رسد به دنیای مجازی دچار پیام‌هایی با جامه دیدپایه و آن هم «صهیونیستاگرام» با آن تباهی و آلودگی در مایه پیام‌ها. هر چند که خودِ فضای مجازی، دهشی خدایی است و باید به نیکی از آن بهره برد ولی بریدن از طبیعت، خانواده و جامعه و افتادن در جادوی مجازی و اعتیاد به آوردگاه جنگ‌های پیشرفته رسانه‌ای و نیز شناختی، چیزی است که حتی در شبکه‌های اجتماعی خوب نیز، در کمین ما است.

۹ نتیجه‌گیری

دستاورد پیشرفته این نوشته، کاربست روش فقهی و بهره از سخن خدا و معصومین (ع) است. بنیادهای استوار فقه نشان می‌دهد که نگاه تراز و راهبردی در طراحی شبکه هم‌رسانی، برپا داشتن صله رحم و زیارت رودررو در جامعه است و در آن جایی که باید از توانش شبکه‌های اجتماعی بهره برد، باید اندازه دیدپایگی جامه پیام‌ها را شناخت و از درافتادن در نخجیرگاه اهریمنی دیدپایگی جامه دیداری، پرهیز کرد. گسترش «نگارداده» و خلیج کردن پیام‌های واژگانی، زدودن ذائقه هم‌رسانی واژگانی را در پی خواهد داشت! تا جایی که نه تنها نمی‌توان «مظهر العجائب» را دید و سخن پیامبر خدا (ص)، «هجر» و هذیان پنداشته می‌شود؛ بلکه دیگر «حسبُنا کتابُ الله» هم گفته نخواهد شد؛ بلکه قرآن خدا و معجزه جاوید و جهانی نیز «هذیان»گویی و گفتاری «مهجور» پنداشته خواهد شد! این است بهای دیدپایه کردن هم‌رسانی و آلودگی ذائقه‌ها به صهیونیستاگرام. از این‌رو باید با پژوهش‌های ریزکاوانه فقهی، طول هر یک از ضلع‌های جامه پیام را باید اندازه‌گرفت و هندسه منتظم جامه درست پیام را به‌دست آورد، رسانه تراز را پایه گذاشت.

مراجع

[۱] امامی میبدی، ابوالفضل، زبرتفقه نظام اسلام، میبد: نشر میبد، اول، ۱۴۰۰.

[۲] امامی میبدی، ابوالفضل و شیخی ده‌آبادی، مجتبی، بنیاد و چارچوب دانش سایبری اسلام، کتاب مجموعه‌مقالات نخستین کنفرانس ملی فضای‌سایبر، تهران: دانشگاه تهران، اول، ۱۴۰۱، صص ۴۰۹- ۴۱۸.

[۳] شیخی ده‌آبادی، مجتبی و امامی میبدی، ابوالفضل، بررسی گلوگاه سایبری در ورود به گام دوم انقلاب، مجموعه مقالات نخستین کنفرانس ملی فضای‌سایبر، دانشگاه تهران، ۱۴۰۱، صص ۵۶۳-۵۷۲.

[۴] قرآن کریم.

[۵] کراجکی، محمد بن علی، کنز الفوائد، قم: دارالذخائر، اول، ۱۴۱۰ ق.

[۶] طباطبایی، سیدمحمدحسین، المیزان فی تفسیرالقرآن، قم: دفترانتشارات اسلامی جامعه‌مدرسین، ۱۴۱۷ق.

[۷] لیثی واسطی، علی بن محمد، عیون الحکم و المواعظ، قم: دار الحدیث، اول، ۱۳۷۶.

[۸] ابن بابویه، محمد بن علی (شیخ صدوق)، من لا یحضره الفقیه، سوم، قم: مؤسسه انتشارات اسلامی، ۱۴۱۳ق.

[۹] حسینی همدانی نجفی، محمد، درخشان پرتوی از اصول کافی، قم: چاپخانه علیمه، اول، ۱۳۶۳.
[۱۰] صدرالدین شیرازی، محمد بن ابراهیم، شرح أصول الکافی، تهران: مؤسسه مطالعات و تحقیقات فرهنگی، اول، ۱۳۸۳.
[۱۱] موسوی خمینی، [امام] سید روح اللّه، توضیح المسائل، تحقیق و تصحیح قلی‌پور گیلانی، مسلم، قم: دفتر مؤسسه تنظیم و نشر آثار امام خمینی، اول، ۱۴۲۶ق.
[۱۲] ابن‌حیون، نعمان‌بن‌محمد تمیمی مغربی، دعائم الإسلام، قم: مؤسسة آل البیت علیهم السلام، دوم، ۱۳۸۵ق.
[۱۳] کلینی، محمد بن یعقوب، الکافی، قم: تحقیق و نشر دارالحدیث، اول، ۱۴۲۹ق.
[۱۴] ابن ابی طالب، علی (امیر المؤمنین) علیه السلام، نهج البلاغة، جمع آوری محمد بن حسین شریف الرضی، تحقیق صبحی صالح، قم: هجرت، اول، ۱۴۱۴ق.
[۱۵] عاملی، زین الدین بن علی، شهید ثانی، منیة المرید، قم: مکتب الإعلام الإسلامی، اول، ۱۴۰۹ق.
[۱۶] مجلسی، محمدباقر، بحار الأنوار الجامعة لدرر اخبار الائمة الاطهار، بیروت: مؤسسة الوفاء اول،۱۴۰۴ق.
[۱۷] ابن طاووس، علی بن موسی، إقبال الأعمال، تهران: دار الکتب الإسلامیه، دوم، ۱۴۰۹ق.
[۱۸] ابن أبی جمهور إحسائی، محمد بن زین الدین، عوالی اللئالی العزیزیة فی الأحادیث الدینیة، تحقیق و تصحیح عراقی، مجتبی، قم: دار سید الشهداء للنشر، اول، ۱۴۰۵ق.
[۱۹] نوری، میرزاحسین، مستدرک‌الوسائل و مستنبط‌المسائل، قم: مؤسسة آل‌البیت لإحیاءالتراث، اول، ۱۴۰۸ق.
[۲۰] جعفر بن محمد، امام ششم علیه السلام (منسوب)، مصباح الشریعة، بیروت: اعلمی، اول، ۱۴۰۰ق.
[۲۱] تمیمی‌آمدی، عبدالواحد بن‌محمد، تصنیف غررالحکم و دررالکلم، قم: دفتر تبلیغات اسلامی، اول، ۱۳۶۶.
[۲۲] حرانی، حسن بن علی (ابن شعبه)، تحف العقول، قم: مؤسسه انتشارات اسلامی، دوم، ۱۴۰۴ق.
[۲۳] شعیری، محمد بن محمد، جامع الأخبار، نجف: مطبعة حیدریة، اول، بی‌تا.
[۲۴] ابن مشهدی، محمد بن جعفر، المزار الکبیر، قم: دفتر انتشارات اسلامی، اول، ۱۴۱۹ق.
[۲۵] ابن بابویه، محمد بن علی (شیخ صدوق)، الخصال، تحقیق علی اکبر غفاری، قم: جامعه مدرسین، ۱۳۶۲.
[۲۶] تمیمی‌آمدی، عبدالواحد بن‌محمد، غرر الحکم و درر الکلم، قم: دفتر تبلیغات اسلامی حوزه علمیه، اول، ۱۳۶۶.
[۲۷] برقی، ابو جعفر احمد بن محمد بن خالد، المحاسن، قم: دار الکتب الإسلامیة، دوم، ۱۳۷۱ق.
[۲۸] مفید، محمد بن محمد، مفید، محمد بن محمد، الأمالی، قم: کنگره شیخ مفید، اول، ۱۴۱۳ق.
[۲۹] عده‌ای از علماء، الأصول الستة عشر، قم: دار الحدیث، اول، ۱۳۸۱.
[۳۰] توسی، محمد بن حسن، الأمالی، قم: دارالثقافة، اول، ۱۴۱۴ق.

تشخیص بدافزارهای اندرویدی با استفاده از روش یادگیری ترکیبی پشته‌ای

مونا زارع[۱]، علیرضا رضوانیان[۱]

[۱]گروه مهندسی کامپیوتر، دانشگاه علم و فرهنگ، تهران
monazare754@gmail.com، rezvanian@usc.ac.ir

چکیده

بدافزارها، برنامه‌هایی هستند که رفتار مخربی دارند و برای آسیب رساندن به سیستم‌ها و شبکه‌های کامپیوتری طراحی شده‌اند. بدافزارها، تنوعی از کارهای مخرب از سرقت اطلاعات حساس تا از بین بردن کل سیستم‌ها را با اهداف مختلفی چون تجاری، اجتماعی، اقتصادی، سیاسی، نظامی یا شخصی را انجام می‌دهند. با توجه به پیچیده‌تر شدن ساختار و رفتار بدافزارها در سیستم‌های اندروید، رویکردهای سنتی، تکرارگرا و آماری عملاً کارساز نبوده و در گذر زمان منسوخ شده است. در این مقاله، بعد از آماده سازی و نرمالسازی داده‌ای، از یک روش یادگیری ترکیبی به صورت پشته‌سازی برای تشخیص بدافزارهای اندرویدی استفاده شده است؛ به این صورت که درخت تصمیم (DT)، بیز ساده (NB) و رگرسیون خطی (LR) به‌عنوان یادگیرنده‌های ضعیف و ماشین بردار پشتیبان (SVM) به‌عنوان یادگیرنده قوی منظور شده است. نتایج آزمایش‌ها بر روی داده‌های سیستم‌های اندرویدی براساس معیارهای دقت، بازخوانی و صحت حاکی از بهبود نتایج روش پیشنهادی نسبت به نتایج روش‌های پایه و چند روش اخیر دارد.

کلمات کلیدی: تشخیص بدافزار، اندروید، یاد گیری ماشین، پشته‌سازی، درخت تصمیم، ماشین بردار پشتیبان.

۱ مقدمه

فایل‌های اجرایی مخرب، برنامه‌هایی هستند که جهت نفوذ و آسیب به شبکه‌های کامپیوتری بدون اجازه و اطلاع کاربر طراحی شده‌اند و امروزه به‌عنوان یک تهدید جدی برای امنیت این شبکه‌ها به شمار می‌روند. این برنامه‌های مخرب که در اصطلاح بدافزار نامیده می‌شوند، قادر هستند که انواع کارهای مخرب از سرقت اطلاعات حساس گرفته تا از بین بردن کل سیستم‌ها یا دستگاه‌ها را انجام دهند. نفوذ بدافزارها در اکثر حملات سایبری از طریق سرقت داده‌ها، منجر به سرقت هویت و حتی نقض گسترده داده‌ها می‌گردد. امروزه بدافزارها با استفاده از روش‌های مبهم‌سازی، پیچیده‌تر شده به گونه‌ای که تشخیص آن‌ها نیز دشوارتر شده

است. بنابراین، بدافزارها و تهدیدهای آن‌ها یکی از بزرگترین چالش‌ها در امنیت شبکه‌های کامپیوتری به شمار می‌رود [۱]. یکی از مشکلات اساسی برای درک صحیح رفتارهای مخرب و نسخه‌های جدید در توسعه بدافزارها، تغییرات زیاد آن‌ها است. از این‌رو، روش‌های سنتی مانند تطابق چند رشته کد از امضای بدافزارها به تنهایی کافی نیستند. استفاده از روش‌های مبتنی بر امضا نیز کند و گران هستند و در مقابل فایل‌های مخرب ناشناخته و دستکاری شده مؤثر نیستند [۲]. بنابراین، همزمان با توسعه‌ی بدافزارها و پیچیده‌تر شدن فرآیند تشخیص آن‌ها، روش‌های سنتی مبتنی بر آمار و مبتنی بر امضا نیز نمی‌تواند به خوبی عمل کند، که تلاش برای استفاده از روش‌های مبتنی بر یادگیری ماشین وجود دارد.

در این مقاله یک روش یادگیری ترکیبی پشته ساز با ترکیب درخت تصمیم، بیز ساده و رگرسیون خطی به عنوان یادگیرنده‌های ضعیف و ماشین بردار پشتیبان به عنوان یادگیرنده قوی به منظور تشخیص بدافزارهای اندرویدی طراحی شده است. در بخش پایانی، ارزیابی روش پیشنهادی در مقایسه با چند روش پایه و اخیر گزارش خواهد شد.

۲ پیشینه‌ی پژوهش

به صورت کلی دو روش، به صورت روش‌های ایستا و روش‌های پویا برای استخراج رفتار بدافزار وجود دارد. در روش‌های ایستا، کد باینری بدافزار بدون اینکه اجرا شود، (مثلا براساس گراف کنترل جریان و گراف فراخوانی توابع) استفاده شده است. بزرگ‌ترین مزیت روش‌های ایستا این است که به دلیل طی کردن تمامی حالت‌های ممکن، مشخص می‌شود که بدافزار مورد نظر در شرایط غیر معمول به چه شکلی رفتار خواهد کرد. همچنین چون در این روش بدافزار در هیچ سیستمی اجرا نمی‌شود، خطر آلودگی سیستم میزبان حداقل ممکن است. بزرگترین عیب روش ایستا این است که ممکن است در مقابل مبهم‌سازی دچار مشکل شود و در تشخیص درست عمل نکند. در روش‌های پویا، تشخیص بدافزار در زمان اجرای آن صورت می‌گیرد و در برابر مبهم‌سازی کد مقاوم است، بزرگترین مشکل روش‌های پویا این است که چون در یک محیط و یک بار اجرا می‌شود، فقط همان یک مسیر بررسی می‌شود و مسیرهای دیگر قابل تشخیص نخواهد بود. برای رفع این مشکل روش، بدافزار را در محیط‌های مختلف و روی داده‌های مختلف چندین بار اجرا می‌کنند [۳]. در ادامه، برخی از روشهای معروف ارائه شده در سال‌های اخیر معرفی شده است.

در مرجع [۴]، با هدف پیش‌گیری از ورود به حریم خصوصی و سرقت اطلاعات حساس در دستگاه‌های تلفن همراه، یک چارچوب یادگیری تجمعی انباشته به‌نام SEDMDroid برای تشخیص بدافزارها ارائه شده است. هم‌چنین، روش ماشین بردار پشتیبان به منظور طبقه‌بندی تلفیقی به کار برده شده است تا اطلاعات تکمیلی ضمنی را از خروجی اعضای گروه بیاموزد و نتیجه پیش‌بینی نهایی را ارائه دهد. نتایج شبیه‌سازی بیان‌گر دقت بیش از ۹۰ درصدی روش SEDMDroid در تشخیص بدافزار نسبت به مجموعه ارزیابی است. در [۵]، برای طبقه‌بندی برنامه‌های مخرب اندروید، استفاده از ترکیب شبکه‌های عصبی بازگشتی و پیچشی پیشنهاد شده است که هدف آن، یادگیری ارتباط کلی بین الگوهای رشته مبهم از نام بسته برنامه و نام صاحب گواهی است. این مدل ویژگی‌های یادگیری ماشین را استخراج می‌کند و یک واحد شبکه عصبی

پیچشی اضافی نیز فرایند استخراج ویژگی را بهبود می‌دهد. نتایج شبیه سازی بیانگر این است که رویکرد ترکیبی نسبت به مدل‌های مبتنی بر Ngram از کارایی بالاتری برخوردار است.

در مرجع [۶]، نویسندگان دو روش مبتنی بر یادگیری تجمعی با داده‌های مقیاس بزرگ طراحی و ارائه کرده‌اند. روش اول براساس استراتژی رای‌گیری وزنی یادگیری تجمعی استوار است و روش دوم مجموعه بهینه‌ای از طبقه‌بندی کننده‌های اصلی را برای انباشت انتخاب می‌کند. نتایج شبیه‌سازی اثربخشی روش‌های ترکیبی را تایید می‌کند. در مرجع [۷]، رویکردی با استفاده از هم‌افزایی ویژگی‌های شمارنده‌های سخت‌افزاری و طبقه‌بندی شبکه عصبی پرسپترون چندلایه بهینه ارائه شده است. در این روش استخراج ویژگی‌هایی با قابلیت تفکیک‌پذیری بالا و نیز از شبکه عصبی بهینه شده بوسیله‌ی الگوریتم سنجاقک، استفاده داده شده است. نتایج حاصل از شبیه‌سازی‌ها، کارایی بالاتر طبقه‌بندی ارائه شده برای تشخیص فایل‌های آلوده شده به بدافزار را نشان می‌دهد. در مرجع [۸]، روشی جهت تشخیص بدافزارها با استفاده از رویکرد داده کاوی معرفی شده است. ایده اصلی روش پیشنهادی ترکیب انتخاب رای اکثریت برای دسته‌بندی و میانگین مقادیر تخمینی است. که در این راستا، روش ارائه شده بیانگر دقت بالای دسته‌بندی و نرخ صحیح تشخیص بدافزارها به بالای ۹۸ درصد است. در مرجع [۹]، روشی ارائه شده که هدف آن، تشخیص عوامل و ویژگی‌ها به صورت ایستا است و همچنین به کمک یک سیستم تصمیم‌یار هوشمند به تشخیص و هشدار این بدافزارها، پرداخته شده است. دقت روش ارائه شده در تشخیص بدافزارها بیش از ۹۷ درصد است. در مرجع [۱۰]، تمرکز بر تشخیص بدافزار از طریق مقایسه‌ی اطلاعات موجود در ساختارهای داده فضای حافظه کاربر است. برای تسریع و تضمین صحت اطلاعات استخراج شده، هم‌زمان از اطلاعات موجود در چندین ساختار مدیریت حافظه در فضای کاربر و هسته استفاده می‌گردد. سپس، برای ارزیابی ویژگی‌های استخراج شده، نمونه‌ها براساس ویژگی‌های انتخاب شده دسته‌بندی می‌شوند. بهترین نتایج شامل نرخ تشخیص ۹۸% و نرخ مثبت کاذب ۱۷% هستند.

۳ روش پیشنهادی

در این مقاله یک روش یادگیری ترکیبی به صورت پشته‌ای شامل ۵ مرحله به شرح زیر ارائه می‌شود.

۱.۳ پیش‌پردازش بر روی داده‌ها

در این مرحله، نمونه‌های پرت از داده‌ها حذف می‌گردد. برای پاک‌سازی داده‌ها، حذف نمونه‌های پرت و داده‌های غیر مرتبط مدنظر است. داده‌های غیرمرتبط، سطرهایی از مجموعه داده است که تهی بوده یا دارای مقدار نامشخص است. همچنین، در این مقاله، از روش پاک‌سازی داده‌ها استفاده شده است، بدین صورت که داده‌ها مورد بررسی قرار گرفته تا در صورتی‌که سطر یا ستونی دارای مقادیر تهی یا غیرمرتبط است، مشخص گردد. سپس مقادیر قبل و بعد از نمونه‌ای که دارای مقدار تهی یا غیرمرتبط است را مورد بررسی قرار داده و میانگین آن‌ها جایگزین می‌گردد.

۲.۳ آماده‌سازی داده‌ها

پس از حل مشکل نمونه‌های پرت، آماده‌سازی داده‌ها انجام گیرد. بدین منظور، داده‌های پیش‌پردازش شده به قالب قابل قبول برای استفاده در ابزارهای موردنیاز تبدیل می‌شود تا در سرورهای اصلی شبکه و در پس‌زمینه، کل داده‌ها که به منظور آموزش روش پیشنهادی جهت تشخیص بدافزارهای تروجانی استفاده شده، به یک فرمت قابل قبول برای نرم‌افزارها و ابزارهای شبکه تبدیل شوند. پس از اینکه به‌صورت سطحی مجموعه داده، مورد بررسی قرار داده شد، در صورت بایستی نرمال‌سازی انجام شود.

۳.۳ نرمال‌سازی داده‌ها

در این مرحله، مقادیر هر ویژگی استفاده شده از مجموعه داده بین ۰ تا ۱ نرمال شده، سپس کلیه مجموعه داده در قالب یک ماتریس نگاشت شده و با تغییر سطرهای ماتریس، عملیات نرمال‌سازی صورت می‌گیرد. برای نرمال‌سازی مقادیر هر مجموعه داده پیوسته، از رابطه (۱) استفاده شده است.

$$Normalize(x) = \frac{x - X_{minP+}}{X_{max} - X_{min}} \quad (۱)$$

به طوریکه X_{max} و X_{min} به ترتیب مقدار بیشینه و کمینه در دامنه‌ی ویژگی X است. پس از نرمال‌سازی داده‌ها، مقادیر کلیه ویژگی‌ها در بازه‌ی $[۰, ۱]$ قرار گرفته و یک پیش‌پردازش به روی نمونه‌های موجود اعمال شده و داده‌هایی که دارای مقادیر پرت استفاده هستند، حذف می‌گردند. علاوه‌بر این، نمونه‌هایی که هیچ فعالیت و عملکردی از آن‌ها ثبت نشده است، از مجموعه داده اصلی پاک‌سازی می‌شود. برای نرمال‌سازی مجموعه داده گسسته از رابطه (۲) استفاده می‌شود.

$$Z_{iF} = \frac{r_{iF-۱}}{M_{F-۱}} \quad (۲)$$

۴.۳ حذف نمونه‌های پرت

در این مرحله با کمک الگوریتم خوشه‌بندی DBScan، داده‌ها تفکیک شده و داده های پرت حذف می‌شود تا بتوان از نتایج مناسبی برخوردار شد.

۵.۳ سیستم یادگیری ترکیبی پشته‌ساز

در روش یادگیری پشته‌ساز پیشنهادی از سه الگوریتم یادگیری ماشین درخت تصمیم (DT)، بیز ساده (NB) و لاجستیک رگرسیون (LR) به عنوان یادگیرنده ضعیف استفاده می‌گردد و خروجی این سه الگوریتم به همراه داده اولیه به‌عنوان ورودی الگوریتم ماشین بردار پشتیبان (SVM) به عنوان یادگیرنده قوی بکار گرفته می‌شود. ساختار کلی این سیستم پشته‌سازی در شکل ۱ نمایش داده شده است.

همانطور که در شکل ۱ مشاهده می‌گردد، مجموعه داده ابتدا به الگوریتم‌های یادگیری ماشین درخت تصمیم، الگوریتم بیز ساده و الگوریتم لاجستیک رگرسیون وارد می‌شود. داده‌های آموزشی به‌عنوان ورودی این الگوریتم‌ها جهت آموزش و تولید مدل استفاده می‌شود. سپس خروجی مدل این سه الگوریتم و داده‌های آزمایشی به عنوان داده‌های آموزشی به ماشین بردار پشتیبان برای تولید مدل نهایی جهت تشخیص بدافزار، داده می‌شود. بطور کلی مراحل انجام روش پشته‌ساز پیشنهادی به شرح ذیل است:

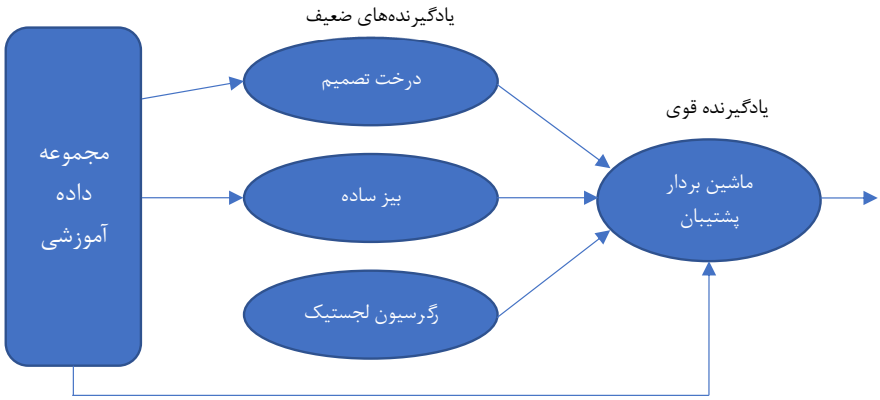
۱. ابتدا مجموعه داده مربوط به بدافزارها به سیستم پشته‌ساز به‌عنوان ورودی داده می‌شود. لازم به ذکر است که مجموعه داده استفاده شده از قبل به دو بخش آموزشی و آزمایشی تقسیم‌بندی شده است.

۲. نمونه‌های آموزشی به هسته اصلی الگوریتم درخت تصمیم با رویکرد آنتروپی، بیز ساده با رویکرد تحلیل گسسته و رگرسیون خطی داده می‌شود. در این مرحله هر کدام از الگوریتم‌های ذکر شده به ترتیب مدل خود را بر اساس نمونه‌های آموزشی دریافتی آموزش داده و مدلی را تولید می‌کنند. بنابراین، تا این مرحله سه مدل مربوط به درخت تصمیم، بیز ساده و رگرسیون خطی تولید شده است.

۳. در مرحله بعد خروجی سه مدل تولید شده به همراه داده اولیه به‌عنوان ورودی به الگوریتم ماشین بردار پشتیبان دو کلاسه با هسته داده شده و ماشین بردار پشتیبان نیز مدل برداری خود را بر اساس این سه مدل تولید می‌کند.

۴. پس از تولید کلیه مدل‌ها، نمونه‌های آزمایشی به هر کدام از مدل‌ها وارد شده و جداگانه طبقه‌بندی می‌شوند.

۵. در نهایت مدل نهایی پشته‌ساز تصمیم می‌گیرد که نمونه مورد نظر که از نمونه‌های آزمایشی وارد شده است یک نمونه نرمال یا بدافزار است.



شکل ۱: روش پشته‌ساز پیشنهادی جهت تشخیص بدافزار

۴ ارزیابی

در این بخش، ابتدا مجموعه داده‌ها، سپس معیارهای ارزیابی و در نهایت نتایج شبیه‌سازی آزمایش‌ها ارائه می‌شود.

۱.۴ مجموعه داده

در این مقاله از مجموعه داده بدافزارهایی که امنیت سیستم‌های اندروید را تحت تاثیر قرار می‌دهد، استفاده شده است. تعداد نمونه‌های مورد استفاده برابر با ۲۳۲.۱۷ نمونه و تعداد ویژگی‌ها برابر با ۸۶۹ ویژگی است[۱]. مجموعه داده به دو دسته داده‌های آموزشی و آزمایشی تقسیم شده است. ۶۰% از کل داده‌ها به‌عنوان داده‌های آموزشی و ۴۰% دیگر به‌عنوان داده‌های آزمایشی در نظر گرفته شده است.

۲.۴ معیارهای ارزیابی

معیارهای مورد استفاده جهت ارزیابی روش پیشنهادی به صورت Precision، Recall، Accuracy عبارتند از:

$$Precision = \frac{TP}{(TP + FP)} \quad (۳)$$

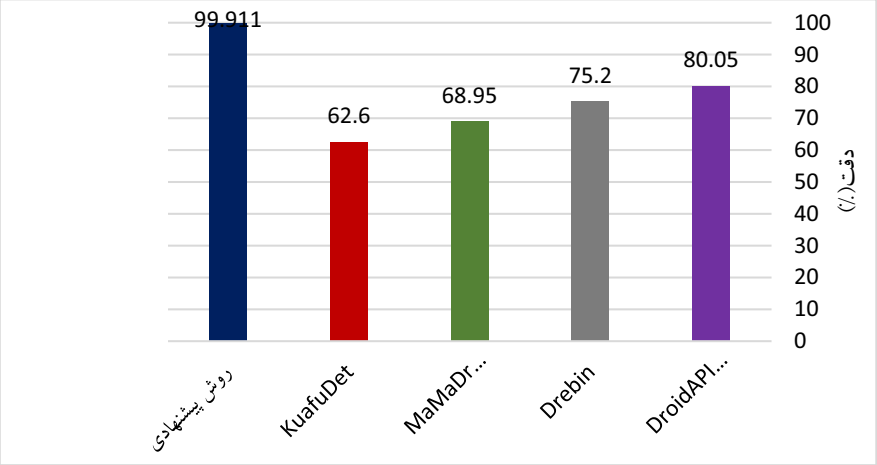
$$Recall = \frac{TP}{(TP + FN)} \quad (۴)$$

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (۵)$$

به طور یکه پارامتر TP بیانگر تعداد نمونه‌هایی است که به درستی، بدافزار، تشخیص داده شده‌اند. پارامتر FP نیز بیانگر تعداد نمونه‌هایی است که به اشتباه، بدافزار، تشخیص داده شده‌اند. پارامتر FN بیانگر تعداد نمونه‌هایی است که به اشتباه نرمال تشخیص داده شده‌اند. TN بیانگر تعداد نمونه‌هایی است که به‌درستی نرمال تشخیص داده شده‌اند.

۳.۴ مقایسه نتایج روش پشته‌ساز پیشنهادی با سایر روش‌ها

برای مقایسه نتایج روش پیشنهادی، پیاده‌سازی انجام شده در محیط نرم‌افزاری MATLAB نسخه R2022b در شرایط یکسان با نتایج [۴]، [۱۱] استفاده شده است. در شکل ۲ دقت تشخیص بدافزار با استفاده از روش



شکل ۲: مقایسه دقت تشخیص بدافزار روش پشته‌ساز پیشنهادی با سایر روش‌ها

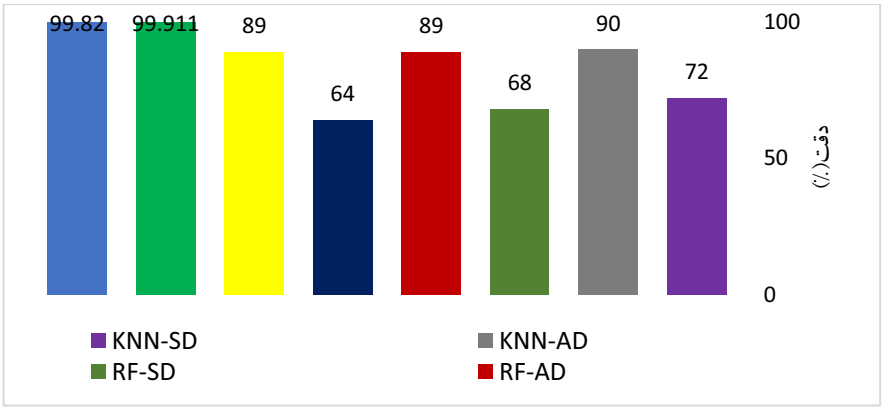
پشته‌ساز پیشنهادی و سایر روش‌هایی همچون KuafuDet، MaMaDroid، Drebin و DroidAPIMiner که مبتنی بر طبقه‌بندی و یادگیری ماشین نیستند، نشان داده شده است.

با توجه به نتایج شکل ۲، روش پیشنهادی توانسته نسبت به روش‌های KuafuDet، MaMaDroid، Drebin و DroidAPIMiner به ترتیب ۳۷٫۳۱%، ۳۰٫۹۶%، ۲۴٫۷۱% و ۱۹٫۸۶% دقت را بهبود ببخشد، که دقت بهبود قابل توجهی داشته است. در شکل ۴ دقت تشخیص بدافزار با استفاده از روش پشته‌ساز پیشنهادی و سایر روش‌های دیگر همچون KNN، Random forest و SVM، نشان داده شده است. در شکل ۳ روش‌های نام برده شده، به دو دسته کلی AD و SD تقسیم‌بندی شده‌اند. SD بیانگر روش‌هایی است که به صورت تشخیص خصمانه عمل می‌کنند و روش‌های AD مبتنی بر تشخیص بدون استراتژی خصمانه است که در مقاله [۱۱] مورد بررسی قرار گرفته است. همانطور که در شکل ۳ مشاهده می‌گردد، میانگین دقت روش پیشنهادی با سطح اجرا و بدون سطح اجرا برابر با ۹۹٫۸۶% است. میزان بهبود دقت تشخیص بدافزار در روش پیشنهادی نسبت به روش‌های SVM-AD، SVM-SD، RF-AD، RF-SD، KNN-AD و KNN-SD به ترتیب برابر با ۱۰٫۸۶%، ۳۵٫۸۶%، ۱۰٫۸۶%، ۳۱٫۸۶%، ۹٫۸۶% و ۲۷٫۸۶% است. از نتایج بدست آمده می‌توان این‌گونه استنتاج کرد که روش‌هایی که بدون تشخیص خصمانه عمل می‌کنند دارای دقت کمتری نسبت به روش‌هایی هستند که با تشخیص خصمانه عمل می‌کنند.

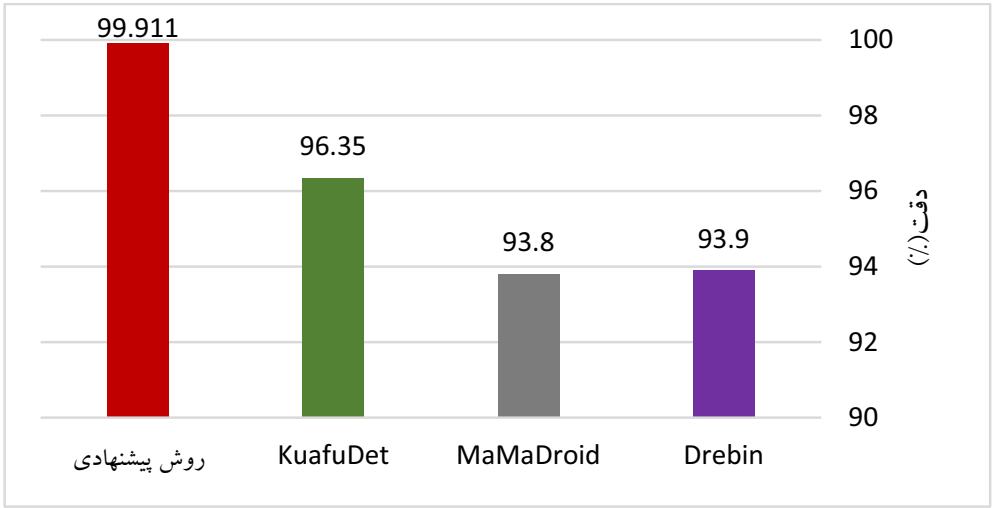
در شکل ۴ دقت روش پیشنهادی و روش‌های KuafuDet، MaMaDroid و Drebin با استفاده از الگوریتم‌های انتخاب ویژگی به منظور تشخیص بدافزارها نشان داده شده است.

همانطور که از نتایج شکل ۴ مشاهده می‌گردد، میزان دقت روش پیشنهادی با سطح اجرا و الگوریتم شبکه عصبی عمیق GMDH برابر با ۹۹٫۹۱% است. از این رو، میزان دقت روش پیشنهادی نسبت به روشهای KuafuDet، MaMaDroid و Drebin به منظور تشخیص بدافزارها به ترتیب برابر با ۳٫۵۶%،

[1]https://ieee-dataport.org/documents/dataset-malwarebeningn-permissions-android



شکل ۳: مقایسه دقت تشخیص بدافزار روش پشته‌ساز پیشنهادی با سایر روش‌های دیگر



شکل ۴: مقایسه دقت تشخیص بدافزار روش پیشنهادی با روش‌های KuafuDet، MaMaDroid و Drebin

جدول ۱: مقایسه دقت روش پیشنهادی با سایر روش‌های دیگر و روش SEDMDroid

روش	ApkAuditor	ACTS	DroidOL	NSCG	OmniDroid	SEDMDroid
دقت (%)	۸۸	۸۷٫۰۹	۸۴٫۲۶	۸۷٫۰۳	۸۹٫۰۷	۹۱٫۹۹

۶٫۱۱% و ۶٫۰۱% است. در جدول ۱، دقت روش پیشنهادی با روش SEDMDroid مطرح شده در مرجع [۴] که برای تشخیص بدافزار در دستگاه‌های اندروید استفاده شده و سایر روش‌های دیگر مقایسه شده است، که دقت روش پیشنهادی جهت تشخیص بدافزارها برابر با ۹۹% ۹۱. است. روش پیشنهادی در مقایسه با روش‌های ،ApkAuditor، ACTS، DroidOL، NSCG OmniDroid و SEDMDroid توانسته دقت را به ترتیب ۱۱٫۹۱%، ۱۲٫۰۱%، ۱۵٫۶۵%، ۱۲٫۶۱%، ۱۰٫۲۱% و ۷٫۹۱% بهبود دهد.

۵ نتیجه‌گیری

بدافزار به هر نرم‌افزار رایانه‌ای گفته می‌شود که رفتار مخرب داشته باشد و به رایانه میزبان صدمه بزند و با توجه به پیچیدگی رفتار بدافزارها، تشخیص بدافزارهای اخیر با روش‌های سنتی، مبتنی بر فراوانی و مبتنی بر الگو به سادگی امکان پذیر نیست. بنابراین در این مقاله، یک روش ترکیبی پشته سازی با ترکیب درخت تصمیم، رگرسیون خطی و بیز ساده به عنوان یادگیرنده های ضعیف و ماشین بردار پشتیبان به عنوان یادگیرنده قوی ارائه شد. نتایج شبیه سازی بر روی داده‌های سیستم‌های اندرویدی در مقایسه با چند روش پایه و اخیر حاکی از بهبود نسبی نتایج روش پیشنهادی است. به عنوان کارهای آینده شاید بتوان از روش‌های نوین یادگیری عمیق بهره برد.

مراجع

[1] M. S. Rana and A. H. Sung, “Evaluation of Advanced Ensemble Learning Techniques for Android Malware Detection,” Vietnam Journal of Computer Science, vol. 7, no. 2, pp. 145–159, 2020.

[2] A. Mahindru and A. L. Sangal, “MLDroid—framework for Android malware detection using machine learning techniques,” Neural Computing and Applications, vol. 33, no. 10, pp. 5183–5240, 2021.

[3] A. Damodaran, F. D. Troia, C. A. Visaggio, T. H. Austin, M. Stamp, “A comparison of static, dynamic, and hybrid analysis for malware detection.” Journal of Computer Virology and Hacking Techniques, vol. 13, pp. 1-12, 2017.

[4] H. Zhu, Y. Li, R. Li, J. Li, Z. You, and H. Song, “SEDMDroid: An Enhanced Stacking Ensemble Framework for Android Malware Detection,” IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 984–994, 2021.

[5] W. Y. Lee, J. Saxe, and R. Harang, “SeqDroid: Obfuscated android malware detection using stacked convolutional and recurrent neural networks,” Adv. Sci. Technol. Secur. Appl., pp. 197–210, 2019.

[6] D. Gupta and R. Rani, “Improving malware detection using big data and ensemble learning,” Comput. Electr. Eng., vol. 86, p. 106729, 2020.

[7] F. Idrees, M. Rajarajan, M. Conti, T.M. Chen and Y. Rahulamathavan, “PIndroid: A novel Android malware detection system using ensemble learning methods,” Elsevier, vol. 68, pp. 36–46, 2017.

[8] A. Martín, R. Lara-Cabrera, and D. Camacho, “Android malware detection through hybrid features fusion and ensemble classifiers: The AndroPyTool framework and the OmniDroid dataset,” Inf. Fusion, vol. 52, pp. 128–142, 2019.

[9] P. Feng, J. Ma, C. Sun, X. Xu, and Y. Ma, “A novel dynamic android malware detection system with ensemble learning,” IEEE Access, vol. 6, pp. 30996–31011, 2018.

[10] N. Potha, V. Kouliaridis, and G. Kambourakis, “An extrinsic random-based ensemble approach for android malware detection,” Connection Science, vol. 33, no. 4, pp. 1077–1093, 2020.

[11] R. M. Yadav, “Effective analysis of malware detection in cloud computing,” Comput. Secur., vol. 83, pp. 14–21, 2019.

حق دسترسی به فضای سایبری در تکوین افکار عمومی

ندا رستگاران[۱]، عبدالحمید فرزانه[۲]، روح الله رحیمی[۳]، مهدی شیخ موحد[۳]

[۱]دانشجوی دکتری حقوق عمومی، دانشگاه آزاد اسلامی واحد شیراز، شیراز، ایران
neda_rastegaran@yahoo.com
[۲]استادیار فقه و مبانی حقوق اسلامی، دانشگاه آزاد اسلامی واحد شیراز، شیراز، ایران
farzaneh2139@gmail.com
[۳]استادیار حقوق عمومی، دانشگاه آزاد اسلامی واحد شیراز، شیراز، ایران
mr5661@gmail.com ،rahimi.mehr48@yahoo.com

چکیده

ظهور و گسترش فضای سایبری مشارکت عموم در گفتمان حوزه عمومی را فراهم نموده است این امر تأثیرگذاری افکار عمومی در کنترل قدرت را منجر شده است. شناخت حق دسترسی به فضای سایبری، باعث مطالبه‌گری عموم می‌گردد و نقش کارگزاری سیاسی عموم را برجسته‌تر می‌سازد. خلاء تعریف دقیق فضای سایبری در نظام حقوقی جمهوری اسلامی ایران مشهود می‌باشد. با الگوبرداری از قوانین و مقررات سایبری در کشورهای موفق و بومی‌سازی آن مبتنی بر ویژگی‌های فرهنگی-حقوقی جمهوری اسلامی ایران، می‌توان فقدان قوانین بنیادین در این حوزه را مرتفع نمود. بر طبق یافته‌ها توجه به قوانین بنیادین و مقررات‌زدایی از سایر قوانین و مقررات در حوزه فضای سایبری پیشنهاد می‌گردد. زیرا در پارادایم لیبرالیسم امکان تکوین افکار عمومی در معنای علمی محتمل‌تر است. حاکمیت موظف است به صورت مستمر قوانین و مقررات را مطابق با نوآوری‌های این فضا بررسی نموده و با تفوق مقررات‌زدایی و خط‌مشی گذاری مبتنی بر نیاز، سیر استعلایی جامعه را در راستای گسترش حقوق و آزادی‌های بنیادین تأمین نماید.

کلمات کلیدی: افکار عمومی، حقوق عمومی، حوزه عمومی، فضای سایبری.

۱ مقدمه

حق دسترسی به فضای سایبری با ایجاد فضای گفتمان حقوق عمومی، باعث تکوین افکار می‌گردد. در جامعه مدرن به دلیل کثرت جمعیت، فضای سایبری جایگزین ارتباطات چهره به چهره شده است. هدف از این پژوهش، شناسایی قوانین و مقررات مرتبط با حوزه سایبری در جمهوری اسلامی ایران و تحلیل و بررسی آن در گفتمان حوزه‌ی عمومی است. محمل عملی پژوهش، بازشناسی حق دسترسی به فضای مجازی و اهتمام به کارکرد این فضا در کنترل قدرت می‌باشد.

به استناد پایگاه‌های اسنادی تاکنون هیچ پژوهش کاربردی در حوزه حقوق عمومی در خصوص نقش فضای سایبری در تکوین افکار عمومی صورت نگرفته است. نوآوری‌های پژوهش عبارتند از:

- این پژوهش اولین مطالعه در حوزه حقوق عمومی در خصوص نقش فضای سایبری بر تکوین افکار عمومی در کشور می‌باشد. پژوهش‌های پیشین تنها به شناخت افکار عمومی پرداخته‌اند یا این موضوع را به‌صورت غیر متمرکز از ابعاد جامعه‌شناسی بررسی نموده‌اند.
- ارائه راهکارهای حقوقی در جهت گسترش نقش مشارکتی افکار عمومی از مهمترین جنبه‌های نوآورانه این پژوهش می‌باشد.

در پژوهش پیشِ رو ابتدا مروری بر پیشینه‌ی کارهای دیگران صورت پذیرفته است، پس از آن حق دسترسی به فضای سایبری مورد مطالعه قرار گرفته شده است. در بخش بعدی نیز به تشریح نقش فضای سایبری در تکوین افکار عمومی پرداخته شده است و در انتها موضوعات مورد بحث جمع‌بندی و نتیجه‌گیری صورت گرفته است.

۲ مروری بر کارهای دیگران

نقش رسانه بر افکار عمومی جامعه ایران، عنوان پایان‌نامه کارشناسی ارشد محمدمهدی مزینانی است که در سال ۱۳۸۹ در دانشگاه آزاد واحد تهران مرکزی از آن دفاع شده است. این پژوهش به یکی از ابزارهای تأثیرگذار بر افکار عمومی پرداخته است. پایان‌نامه مذکور به تعریف افکار عمومی پرداخته است، نظریات فلاسفه و نظریه پردازان اجتماعی در خصوص افکار عمومی را جمع‌آوری و کارکردهای رسانه را در جامعه ایران تحلیل نموده است.

تأثیر رسانه‌های نوین بر ساخت قدرت سیاسی در ایرانِ دهه هشتاد خورشیدی، عنوان رساله دکتری عباس سهراب‌زاده دانشجوی دانشگاه علامه طباطبایی در سال۱۳۹۳می‌باشد. رساله به تفاوت رسانه‌های دولتی و انحصاری با رسانه‌های غیردولتی پرداخته و آزادی در بیان علایق، عقاید، خواسته‌ها و انتقاداتِ مورد نظر را بررسی نموده است. از این رو در بررسی نقش رسانه‌های نوین در سیاست و ساخت قدرت به مؤلفه‌هایی که این نقش را متفاوت و معنادار می‌نمایند، در جامعه ایران و در محدوده دهه هشتاد خورشیدی پرداخته شده است.

تأثیر شبکه‌های اجتماعی برخط بر دیپلماسی عمومی و بازتاب آن در سیاست خارجی دولت، مطالعه موردی ایالات متحده امریکا، عنوان پایان‌نامه ارشد رشته روابط بین‌الملل دانشگاه اصفهان است که در سال ۱۳۹۲توسط ذکیه طلوع مورد دفاع واقع شده است. این پژوهش به مطالعه‌ی چگونگی تأثیرگذاری شبکه‌های اجتماعی برخط بر دیپلماسی عمومی و سیاست خارجی دولت پرداخته است. در پایان، خواننده را بدین رهیافت معطوف می‌نماید که دولت‌های دموکراتیک از جمله ایالات متحده آمریکا در راستای افزایش قدرت نرم خود در پیشبرد هماهنگی در سیاست خارجی به فرهنگ و اطلاعات، دو عامل عمده و تأثیرگذار بر افکار عمومی، توجه نموده و با درک چگونگی ظهور عوامل مؤثر در دیپلماسی عمومی، شبکه‌های اجتماعی برخط را

در راستای هدایت و نظارت بر افکار عمومی جهانی، افزایش قدرت نرم، تحقق منافع ملی وسیاست خارجی‌شان، مورد بهره‌برداری قرار می‌دهند.

روش‌های سنجش افکار عمومی (افکار عمومی در قرن بیست و یکم) عنوان پژوهشی راسل. جی بروکر است که در دانشگاه مرکزی واشنگتن در کالج آلورنو به زبان لاتین به‌صورت کتابچه منتشر شده است. در این پژوهش، روش‌های بروز و اندازه‌گیری افکار عمومی و نحوه‌ی صحیح نظرسنجی‌های سیاسی به تفصیل بیان شده است. پژوهش با ذکر مصادیق به تفصیل خطاهایی که نتایج نظرسنجی را غیر واقعی می‌نماید و درک صحیح از افکار عمومی را مشکل می‌نماید، می‌پردازد.

بررسی نقش رسانه در سیاست‌گذاری مبارزه با فساد مبتنی بر رویکرد نظام ملی درستکاری، عنوان مقاله‌ای است که در پاییز سال ۱۳۹۹ در فصلنامه نظارت و بازرسی منتشر گردیده است. در این پژوهش به نقش پراهمیت رسانه‌ها در بهبود عملکرد دولت و بازدارندگی از فساد اداری، مبارزه با فساد، شکل‌دهی افکار عمومی در مخالفت با فساد در دستگاه‌های دولتی و حتی اعمال فشار افکار عمومی به منظور تغییر قوانین و مقررات پرداخته شده است.

۳ حق دسترسی به فضای سایبری

حق دسترسی به فضای سایبری از حقوق بنیادین بشر در جامعه مدرن می‌باشد. فضای سایبری را «محیطی تشکیل یافته از سامانه‌ها و شبکه‌های ارتباطی» [۱] تعریف می‌نمایند. مفهوم فضای سایبری با حوزه‌ی عمومی تعریف‌شده توسط هابرماس همپوشانی دارد. «نقش فضای سایبر در ممکن‌سازی ابتکارات، تصادفی نیست؛ بلکه از معماری آن مشتق شده است» [۲]. حق دسترسی به فضای سایبری به مفهوم اعمال کلیه حقوق مرتبط با این فضا اعم از دریافت اطلاعات و تبادل آراء را در بر می‌گیرد.

در جمهوری اسلامی ایران نیز اصل، بر حق دسترسی به فضای سایبری می‌باشد. طبق ماده ۳۳ منشور حقوق شهروندی، حق شهروندان است که آزادانه و بدون تبعیض از امکان دسترسی و برقراری ارتباط و کسب اطلاعات و دانش در فضای مجازی بهره‌مند شوند. این حق از جمله شامل احترام به تنوع فرهنگی، زبانی، سنت‌ها و باورهای مذهبی و مراعات موازین اخلاقی در فضای مجازی است. در ادامه بیان شده است که ایجاد هرگونه محدودیت (مانند فیلترینگ، پارازیت، کاهش سرعت یا قطعی شبکه) بدون مستند قانونی صریح ممنوع می‌باشد. در حالی که منشور حقوق شهروندی از صیانت حوزه‌ی عمومی دفاع می‌نماید، پاسدار حوزه خصوصی نیز می‌باشد. ماده ۳۵ منشور حقوق شهروندی در ارتباط با صیانت از حوزه خصوصی بیان می‌دارد: حق شهروندان است که از امنیت سایبری و فناوری‌های ارتباطی و اطلاع‌رسانی، حفاظت از داده‌های شخصی و حریم خصوصی برخوردار باشند. حق دسترسی به فضای سایبری را با تسامح، آزادی اطلاعات نیز می‌گویند. در معنای موسع، علاوه بر آزادی دریافت، توانایی انتقال و انتشار اطلاعات را آزادی اطلاعات می‌گویند. این در حالی است که معنای مضیق حق دسترسی به فضای سایبری، استفاده از پلتفرم‌ها و ابزارهای فناوری به منظور دسترسی به اطلاعات به وسیله عموم، بالاخص اطلاعات سیاسی یا در دسترس حاکمیت تعریف می‌گردد.

«دسترسی به اطلاعات موجود در دستگاه‌های حکومتی، مقدمه پاسخگویی حکومت‌ها به افکار عمومی است» [۳]. با توجه به اینکه تنها راه محدودیت و کنترل قدرت همانا قدرت می‌باشد. این توانایی بالقوه وجود دارد که حق دسترسی به فضای سایبری با پیش فرض سواد رسانه‌ای عموم در این فضا را قدرت عمومی نامید.

بلوغ سیاسی عامه زمینه مشارکت را فراهم می‌سازد. این بلوغ از مجرای حق دسترسی به اطلاعات و پردازشگری اطلاعات به‌دست‌آمده حاصل خواهد شد. مشارکت عموم بر مبنای اصل پارکینسون، مستلزم حق دسترسی عادلانه و بدون تبعیض به اطلاعات در حوزه‌ی عمومی می‌باشد. مطابق منطوق ماده ۳۴ منشور حقوق شهروندی، حق شهروندان است که از مزایای دولت الکترونیک و تجارت الکترونیک، فرصت‌های آموزشی و توانمندسازی کاربران، به‌صورت غیر تبعیض‌آمیز برخوردار شوند. در جامعه‌ای که وسایل دسترسی دارای محدودیت‌های طبقاتی باشد یا دسترسی کامل به پهنای باند سایبری گران قیمت و در توان اقشار خاص باشد، اجرای عدالت در این حوزه محقق نخواهد شد. بر مبنای اصل نهم قانون اساسی نیز هیچ مقامی حق ندارد به نام حفظ استقلال و تمامیت ارضی کشور، آزادی‌های مشروع را، هر چند با وضع قوانین و مقررات، سلب کند؛ بنابراین ایجاد تبعیض در دسترسی به فضای سایبری ممنوع می‌باشد.

در این خصوص عنوان شده است: «آگاهی، شرط ضروری ادراک آزادی انتخاب است. مردم ناآگاه هیچ‌گونه امکانی برای انتخاب آزاد ندارند» [۴]. حق دسترسی به اطلاعات، روند مردم‌سالاری در جامعه را تسریع بخشیده و با ایجاد شفافیت در حوزه‌ی عمومی از بسیاری از ناکارآمدی‌های دولت جلوگیری به عمل می‌آورد. «آزادی کامل رسانه‌ها، موجب آگاهی کامل شهروندان، نظارت بر فعالیت‌های دولت، انعکاس افکار عمومی، انتقادها و توسعه اقتصادی و اجتماعی خواهد بود» [۵]. مشاهده می‌گردد که روند احقاق حقوق عمومی در جامعه به مانند گره‌هایی در هم تنیده می‌باشد. حق دسترسی به فضای سایبری بدون پیش‌شرط سایر حقوق امکان‌پذیر نمی‌باشد و ایجاد این حق نیز بهره‌مندی از سایر حقوق و آزادی‌ها را منتج می‌گردد.

«بهره‌مندی دولت از امکان مداخله نظریات در اخذ بهترین تصمیمات، موضع دولت را از موضع واکنشی به موضع فعالانه تغییر می‌دهد و مشروعیت مضاعف را به ارمغان می‌آورد» [۶]. عدم دسترسی آسان به وسایل ارتباطی منجر می‌گردد که در گروهی از جامعه این حق اجرایی نگردد. فضای سایبری با قابلیت حضور فعال شهروندان در تولید و بازنشر اطلاعات در تکوین هرچه سریع‌تر افکار عمومی با توجه به گستره‌ی تعداد اعضای جامعه در دولت مدرن، حائز اهمیت می‌باشد. در این راستا شفاف‌سازی و قابل فهم‌سازی اطلاعات، نقش مهمی را ایفا می‌نمایند. امروزه «توانایی مشارکت در اطلاعات و اقناع دیگران نسبت به اهداف خود، منبع مهمی برای جذابیت و قدرت مبدل می‌گردد» [۷].

عدم تطابق ظرفیت فهم شهروندان با مفهوم گسترش یافته در سطح فضای سایبری موجب تفسیرهای ناصواب شده و به گسترش شایعه دامن می‌زند. بنابراین علاوه بر شفافیت، ساده‌سازی مطالب از وظایف مطبوعات اصیل می‌باشد. در این میان نمی‌توان از نقش فضای سایبری در اهمیت دادن به موضوع و احیاء آن در بازه زمان و یا عدم پرداختن به موضوع در شکل‌گیری افکار عمومی غافل شد. افکار عمومی این قابلیت را دارا می‌باشند تا لوایح و مقررات خودسرانه و مخالف با نفع عمومی را از طریق وسایل ارتباط جمعی به چالش کشیده و حداکثر نظارت خود را در مرحله قانون‌گذاری و شبه قانون‌گذاری، که از طریق مقامات دولتی اعمال می‌گردد، داشته باشند. تلقین، تکرار و استفاده از ویژگی‌های روانشناختی مخاطب از روش‌های معمول فعالان

فضای سایبری جهت القای مفاهیم و ارزش‌ها به مخاطبین می‌باشد. اگرچه در برخی موارد، نتایج مطلوبِ نظر آنان حاصل نخواهد شد. انتخاب محتوا و رسانه، ناشی از حق انتخاب و آزادی شهروندان می‌باشد که در اعلامیه جهانی حقوق بشر مورد تصریح و تأکید واقع شده است. حق آزادی انتخاب به عنوان یکی از حقوق فطری از اهداف اعلامیه حقوق بشر است که در ذیل مقدمه این اعلامیه تصریح شده است. دکتر کاتوزیان معتقدند: «تمام قوای مملکت ناشی از ملت است و دولت‌ها وظیفه دارند که هرچه بیشتر آزادی افراد را تأمین کنند. آزادی پیشه و بیان و قلم، از حقوق فطری و تغییرناپذیر بشر است و هیچ قاعده‌ای نمی‌تواند به این حقوق عالی تجاوز کند» [۸]. تضمین این آزادی‌ها در قانون اساسی ضامن ایجاد و اثرگذاری افکار عمومی است. با گسترش آزادی‌ها و بهره‌مندی از سواد حقوق عمومی، گفتمان حقوق عمومی بین شهروندان گسترش می‌یابد، در این برهه قدرت شکل‌گیری افکار عمومی به اوج می‌رسد. «در واقع مشروعیت سیاسی در پسامدرنیته، اغلب درون انواع مختلف و متفاوت خرده گفتمان‌هایی قرار دارد که متضمن کثرت‌گرایی موضوعات و مسائل محلی و گروه‌های هویتی و غیره است» [۱۷] حق دسترسی به فضای سایبری، به عنوان یکی از طرق تضمین حق دسترسی به اطلاعات، امکان گفتمان کثرت‌گرا، آزاد، برابر و تخصصی را فراهم می‌سازد.

۴ نقش فضای سایبری در تکوین افکار عمومی

فضای سایبری به عنوان بستر گفتگو در جامعه مدرن نقش اساسی را ایفا می‌نماید. همان‌طور که بیان گردید؛ اصل برحق عموم در دسترسی آزاد به فضای سایبری می‌باشد و موارد استثنا به موجب قانون معین می‌گردد. اهمیت حق دسترسی به اطلاعات به منظور تکوین افکار عمومی به مثابه مصالح ضروری یک سازه‌ی معماری می‌باشد. در کنار ارکان اصلی دموکراسی که عبارتند از: «مشارکت شهروندان، پاسخگویی حاکمیت و شفافیت امور حکومتی، رسانه به عنوان رکن چهارم دموکراسی می‌تواند زمینه‌ای برای کنترل سه رکن دیگر باشد» [۹]. از این رو فضای سایبری دارای اهمیت بسیاری می‌باشد.

«میزان حساسیت افکار عمومی نسبت به مسائل اجتماعی در ارتباط با میزان شیوع مسأله در هر منطقه قرار دارد» [۱۰]. فضای سایبری امکان بازنشر و شیوع مسائل را فراهم می‌سازد. اطلاع‌رسانی عمومی و شفاف‌سازی که شامل قابل فهم‌سازی مسائل برای عموم می‌باشد، از ویژگی‌های دولت‌های مبتنی بر دموکراسی می‌باشد. پاسخگویی به عموم باعث گسترش بحث‌های حوزه‌ی عمومی و به تبع آن افزایش سواد در حوزه‌ی عمومی گردید. این پاسخگویی به دلیل مدرناسیون مستلزم استفاده از ابزارهای متناسب با دولت مدرن است و فضای سایبری ابزار همگرایی و ایجاد روابط در سطح وسیع، متناسب با شرایط دولت مدرن می‌باشد. با توجه به گسترش فضای سایبری، نقد سیاست‌های دولتی در دستور مباحثات برنامه‌های رسانه‌ای قرار گرفت که این امر خود مستلزم سواد رسانه‌ای شهروندان می‌باشد.

مردم در خصوص موضوعاتی که اطلاعی ندارند یا اطلاع‌رسانی در آن خصوص صورت نمی‌گیرد، توانایی اظهار عقیده نداشته؛ بنابراین افکار عمومی نیز در این زمینه شکل نمی‌گیرد. «وضعیت‌های کنشی، تبلیغات رسانه‌های گروهی و قوانین اجتماعی هر یک در کم و کیف دخالت مردم در سرنوشت خود تأثیر گذارند» [۱۱]. به‌گونه‌ای که گاه رسانه‌های دولتی به‌صورت زنجیره‌ای، فضایی ایجاد می‌کنند که دولت‌ها از شنیدن

صدای واقعی مردم و افکار عمومی محروم می‌گردند و گاهی نیز موفق می‌شوند افکار عمومی را در جهت خاصی هدایت کنند. فضای سایبری در این جوامع بیشتر در دسترس حاکمیت بوده و در موضوعات محدودی افراد خصوصی امکان فعالیت دارند. پارادایم حاکم بر این جوامع پاترنالیست سایبری می‌باشد. به‌صورت کلی «پارادایم‌های حاکم بر فضای سایبری بر دو رویکرد اساسی پاترنالیست سایبری و لیبرتالیسم (لیبرالیسم) سیاسی استوار است» [۱۲]. در پارادایم لیبرتالیسم، آزادی فضای سایبری حاکم است. در این جوامع دولت به جای تنظیم‌گری فضای سایبری، اهتمام خویش را در راستای برخورداری از حق آموزش سواد رسانه‌ای معطوف می‌نماید. حق برخورداری از سواد رسانه باعث ارتقاء سطح پردازشگری شهروندان شده و نفوذ تبلیغات را به حداقل می‌رساند.

عراقی در کتاب بررسی و شناخت افکار عمومی، عنصر فرهنگ را مهمتر از تبلیغات دانسته و بیان می‌دارد: «تبلیغات غالباً تنها افراد را به انجام عمل تحریک می‌کند ولی جهت این عمل بیشتر به تمایل قبلی افراد بستگی دارد تا محتوای تبلیغات» [۱۳] در جوامع مذکور، تبلیغات به‌صورت روایتِ یک واقعیت بیان می‌شود و مخاطب در جریان محتوای تبلیغاتی پیام قرار نمی‌گیرد. این روش، اگرچه مخالف با اخلاق فضای سایبری می‌باشد اما کماکان مورد استفاده در سراسر جهان واقع می‌شود. در تبلیغاتی که با هدف وارونه جلوه دادن واقعیت و تحریف عمدی و مغرضانه صورت می‌گیرد، در صورتی که مخاطب آگاهی کافی نداشته باشد و از منابع متعدد جهت بهره‌مندی از اطلاعات محروم باشد، نتیجه‌ای جز تحریف واقعیت و تغییر افکار عمومی نخواهد داشت.

فضای سایبری با عملکرد جمع‌آوری و بازنشر اطلاعات و رویدادهای اجتماعی ممکن است باعث همبستگی بخشی از جامعه در واکنش به آن گزارش گردد، این همبستگی می‌تواند اولین قدم در ایجاد افکار عمومی باشد. این همبستگی با توجه به مخاطبین می‌تواند پهنایی به وسعت یک شهر از یک کشور و یا فرای مرزها باشد. «در بررسی نقش رسانه‌های نوین در سیاست و ساخت قدرت، اصلی‌ترین مؤلفه که این نقش را متفاوت و معنادار می‌کند همین رهایی از سیطره‌ی قدرت است» [۱۴]. فضای سایبری به دلیل فاقد مرز بودن این ویژگی منحصر به فرد را دارا شده است.

فضای سایبری باعث گردیده است: «اولاً افکار عمومی حالت ملموس‌تری به خود بگیرد و ثانیاً به عنوان یک نیروی سیاسی در جامعه ایفای نقش کنند» [۱۵]. «با گسترش حاکمیت قانون و کاهش روابط خصمانه در پی کاستن از هزینه‌های سیاسی و اجتماعی و افزایش نقش افکار عمومی در تصمیم‌گیری دولت‌ها، دولتمردان تلاش خود را در به‌کارگیری توان نرم معطوف ساخته و از توجه بیش از اندازه نسبت به توان سخت خود کاستند» [۱۶].

با ارتقاء جایگاه افکار عمومی و نقشی که فضای سایبری در ایجاد و اثرگذاری آن ایفا می‌کند، این امر را نمی‌بایست از نظر دور داشت که حتی در صورت تضمین حق دسترسی به فضای سایبری، حاکمیت در روابط نابرابر خود با داشتن بودجه‌ی عمومی و بهره‌مندی از نفوذ خود پیروز میدان خواهند بود. همین امر در ارتباط با افکار عمومی در جهان نیز مصداق دارد. دولت‌ها با هزینه کردن بودجه‌هایی متفاوت و در اختیار داشتن متخصصین برای رقابت با هم، به مسابقه‌ای نابرابر دعوت شده‌اند.

فضای سایبری به عنوان ابزار شکل‌گیری افکار عمومی با بهره‌گیری از نخبگان سیاسی و روش‌های تبلیغاتی، قدرت هدایت افکار عمومی در سطح بین‌المللی را نیز دارا می‌باشد. این تأثیرگذاری در جوامع توسعه

نیافته مؤثرتر خواهد بود؛ زیرا بین عزت نفس افراد یک جامعه و ثبات نسبی افکار عمومی رابطه‌ای مثبت و اثبات شده وجود دارد.

حق دسترسی به فضای سایبری شامل حق برابری افراد در حوزه مشارکت به دور از سلطه قدرت در جهت توازن منافع است. تولید محتوا توسط مخاطبین و تسهیل در ارسال بازخورد، ارتباط دوسویه جهت گفتگویی عمیق و متکثر که دارای قدرت نفوذ بالاتری در کنترل قدرت است، از نتایج بهره‌مندی از حق دسترسی به فضای سایبری می‌باشد. حوزه‌ی عمومی در جوامعی که اطلاعات به عموم به‌صورت یک طرفه به مخاطبینِ منفعل انتقال پیدا می‌کند، بسیار کم‌رنگ می‌باشد. این فضا که تولید محتوا توسط عموم صورت می‌گیرد، با مفهوم جهان زیست هابرماس تقارن پیدا می‌نماید.

۵ نتیجه‌گیری

تبیین حق برخورداری از فضای سایبری و بهره‌مندی از خرد جمعی در قالب افکار عمومی از الزامات دولت مدرن در راستای تعادل قدرت است. در جمهوری اسلامی ایران مرکز ملی فضای مجازی به موجب ابلاغیه مقام معظم رهبری مسئول خط‌مشی‌گذاری در حوزه فضای سایبری و تبیین اولویت‌ها و سیاست‌های راهبردی است. نتایج، نشان دهنده‌ی رابطه مستقیم افزایش سواد حقوقی و شرکت در مباحثات عقلائی توسط عموم است. همچنین سطح مطالبه‌گری عموم و شناخت حقوق عمومی نیز در ارتباط مستقیم با یکدیگر قرار دارند. تشریح حق برخورداری از فضای سایبری و پیامد مطلوب آن در گفتمان حوزه‌ی عمومی به عنوان پیش‌شرط تکوین افکار عمومی حائز اهمیت است. در دولت مدرن مهمترین بستر شکل‌گیریِ حوزه‌ی عمومی، فضای سایبری می‌باشد. امکان تبادل افکار، وجه افتراق حق برخورداری از فضای سایبری با سایر حقوق از جمله حق برخورداری از اطلاعات است.

مراجع

[۱] میرعباسی، سیدباقر و مجید کورکی‌نژاد قرایی، قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی دفاع مشروع مقرر در ماده ۵۱ منشور سازمان ملل متحد، فصلنامه مطالعات حقوق عمومی، دوره ۴۸، شماره ۲، ۱۳۹۷، صص ۲۶۱-۲۸۰.

[۲] رهایی، سعید و محسن متاجی، تأملی بر مقررات‌گذاری خودتنظیمی در فضای سایبر، فصلنامه مطالعات حقوق عمومی، دوره ۵۲، شماره۴، ۱۴۰۱، صص ۲۱۲۷-۲۱۴۸.

[۳] محسنی، وجیهه و همکاران، تحلیل حقوقی نسبت سنجی حق دسترسی عموم به اطلاعات با تحقق حقوق شهروندی با تأکید بر نظام حقوقی ایران، فصلنامه پژوهش حقوق عمومی، شماره ۶۲، ۱۳۹۸، صص ۳۲۱- ۳۵۴.

[۴] پورعزت، علی‌اصغر، مبانی دانش اداره دولت و حکومت، تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها، ۱۳۸۷.

[۵] مالکی، جلیل و زهرا واعظی، آزادی مطبوعات در منظر حق دسترسی آزاد به مطبوعات، رسانه، سال بیست و سوم، شماره ۴، ۱۳۹۱، صص ۵-۲۳.

[۶] رستگاران، ندا و همکاران، تأثیر افکار عمومی در نظارت سیاسی بر دولت، فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ۱۴۰۲.

https://doi.org/10.22059/jplsq.2021.306695.2500

[۷] شهرام‌نیا، سیدامیر مسعود و همکاران، واکاوی مفهومی قدرت نرم و راهکار (فرصت)های ایران در قبال آن، مجله دانش سیاسی و بین المللی، شماره سوم، ۱۳۹۱، صص ۷۱-۸۸.

[۸] کاتوزیان، ناصر، کلیات حقوق: نظریه عمومی، تهران: شرکت سهامی انتشار، چاپ دوم، ۱۳۷۹.

[۹] نواح، عبدالرضا و همکاران، پیامدهای جامعه‌شناختی سواد رسانه‌ای بر آگاهی از حقوق شهروندی و دموکراسی خواهی، فصلنامه مطالعات رسانه‌های نوین، سال پنجم، شماره هشتم، ۱۳۹۸، صص ۲۰۳-۲۲۸.

[۱۰] رشوند، علی‌اکبر، مقایسه عوامل موثر بر حساسیت افکار عمومی نسبت به مسائل اجتماعی در مناطق شهری و روستایی استان قزوین، پایان‌نامه کارشناسی ارشد، دانشگاه قزوین: گروه علوم اجتماعی، ۱۳۸۰.

[۱۱] لازار، ژودیت، ۱۳۸۰، افکار عمومی، ترجمه مرتضی کتبی، تهران: نشر نی، ۱۳۸۰.

[۱۲] حسینی، محمدرضا، الگوی مقررات‌گذاری در فضای سایبر: ارائه چارچوب جامع تنظیم‌گری برای محیط ملی، فصلنامه مطالعات حقوق عمومی دانشگاه تهران، ۱۴۰۲.

https://doi.org/10.22059/jplsq.2023.344418.3102

[۱۳] عراقی، مهدی، اهمیت و کارکردها؛ بررسی و شناخت افکار عمومی، تهران: انتشارات فجر، ۱۳۸۳.

[۱۴] سهراب‌زاده، عباس، تاثیر رسانه‌های نوین بر ساخت قدرت سیاسی در ایران دهه‌ی هشتاد خورشیدی، رساله دکترای تخصصی، دانشگاه علامه طباطبایی، ۱۳۹۳.

[۱۵] نقیب‌زاده، احمد، درآمدی بر جامعه‌شناسی سیاسی، تهران: سمت، چاپ هفتم، ۱۳۸۸.

[۱۶] طلوع، ذکیه، تاثیر شبکه‌های اجتماعی بر خط بر دیپلماسی عمومی و بازتاب آن در سیاست مطالعه‌ی موردی ایالت متحده آمریکا، پایان‌نامه کارشناسی ارشد، دانشگاه اصفهان: گروه روابط بین الملل، ۱۳۹۲.

[17] Fairfield, Paul, Lyotard and Politics, Discours, 2004, www:mises.com.

نیهلیسمِ فضای سایبری در همسخنی با نیچه

مرتضی سعیدی ابواسحاقی[۱]، راضیه سعیدی ابواسحاقی[۲]

[۱]دانشجوی دکتری فلسفه دانشگاه تهران، پژوهشگر پژوهشگاه فضای مجازی
morteza.saeidi@ut.ac.ir
[۲]دانش‌آموخته کارشناسی تعلیم و تربیت، دانشگاه فرهنگیان
raziyesaeedi9819@gmail.com

چکیده

نیچه در اشاره به زمانه‌اش می‌گوید: ما در عصری آشفته زندگی می‌کنیم، و به همین خاطر، شورانگیز نیست. این عصر مدام خودش را گرم می‌کند، زیرا احساس می‌کند گرم نیست، بلکه اساساً یخزده است. در زمانه‌ی ما رویدادها یا وقایع صرفاً با استفاده از پژواک روزنامه‌ها [یا رسانه‌ها] عظمت [پوشالی‌شان] را به دست می‌آورند. در این مقاله تلاش بر این است که این سخن نیچه در نسبت با فضای سایبری و اینترنت و شبکه‌های مجازی بررسی شود و پوچ‌گرایی و نیست‌انگاری یا نیهلیسمی که در فضای سایبری و شبکه‌های مجازی شدت یافته را متذکر شویم و در ادامه در همسخنی و همدلی با نیچه و هایدگر این امر بیان شود که رخداد نیهلیسم و ظهورات کامپیوتر و فضای سایبری برآمده از تاریخ غرب است و در صورتی که این امر در ادامه تاریخی غرب دیده نشود امکان فهم درست آن نخواهد بود. در انتها راه برون‌رفت از این مهلکه را از نظر نیچه و هایدگر در هنر معرفی کردیم، از نظر هایدگر هنر بزرگ امکان گذار و تغییر را فراهم می‌کند و می‌تواند جهانی نو بسازد که انسان را از نیهلیسم و پوچ‌گرایی نجات دهد. این تحقیق در حیطه مطالعات بنیادین قرار دارد و روش آن از سنخ روش‌های پژوهش کیفی است که روش تحلیل مضمون یا تحلیل تم (Thematic Analysis) برای آن به کار می‌رود. از آنجا که تحلیل مضمون هم برای بیان واقعیت و هم برای تبیین آن به کار می‌رود و در این پژوهش به‌دنبال تبیین و توصیف درست و عمیقی از نتایج فضای سایبری هستیم، روش تحلیل مضمون مناسب آن است.

کلمات کلیدی: نیچه، فضای سایبری، نیهلیسم، هنر، شبکه های مجازی، تخدیر.

۱ مقدمه

صداهایی که شنیده نشد؟!! چرا صداهای افرادی که از ترنس و تغییر جنسیتشان پشیمان شدند هرگز شنیده نشد؟ و چه بسیار از ترنس‌ها و تغییر جنسیت و همجنس‌بازی و ... در همین رسانه گفته شده است؟ نمونه آن را در تغییر جنسیت بازیگران می‌بینیم که با چه غوغایی در رسانه‌ها برگزار می‌شود، و چه بسیار صداهایی که از بی‌عدالتی و جنگ و ... در قاب رسانه و فضای مجازی نشست، اما خودش عین بی‌عدالتی بود، چون

یک پست یا استوری‌ای مثل همه پست و استوری‌های دیگر بود و در هیاهوی آنها گم شد، همچون سوزنی در کاهدان؛ و عملاً شنیده نشد و به دیده‌ها نیامد. شاید اصلاً وضعیت از این هم پیچیده‌تر و قابل تأمل‌تر و خطرناک‌تر باشد، یعنی آنجایی که این فضای مجازی و فضای سایبری و رسانه‌ها و گیم و شبکه‌های مجازی و اینترنت و روزنامه و رادیو و ... باعث شد که صدای درون و فطرت خودمان را نشنویم و حتی اگر شنیدیم در میان هیاهوی آنها طوری گم شد که انگار نبوده است و حتی بدتر اینکه خیلی وقت‌ها شنیدیم اما هراسیدیم که به ندای فطرتمان گوش دهیم.

جدایی از اصالت انسانیت و جدایی از خدا و نیهلیسم یا نیست‌انگاری‌ای که بشر کنونی در آن گم شده است –و ویژگی جهان کنونی است–. در بیشتر موارد انسان بدون اینکه خودش بفهمد زیر چرخ آن در حال لِه شدن است و گه‌گاه از روی فطرت ندایی از او برمی‌خیزد و فریادِ «کمک کنید» سر می‌دهد؛ هر چند در بیشتر موارد همین فریاد نیز در غوغا و همهمه‌های عصر کنونی گم شده است. چه اکنون که شبکه‌های اجتماعی با همهمه اجازه نمی‌دهند که فریاد اصیلی شنیده شود و چه پیشترها در رسانه‌ها و روزنامه‌ها و تلویزیون‌ها و رادیوها و ...؛ یکی از کسانی که احتمالاً زودتر از بقیه فریاد نیهلیسم و نیست‌انگاری را سرداده بود، نیچه است. سخنی که نیچه درباره روزنامه‌ها می‌گوید آن‌قدر قابل تأمل است که ما بعد از ۱۲۰ سال نیز می‌توانیم با آن درباره فضای مجازی و رسانه‌ها و شبکه‌های اجتماعی به‌صورتی دقیق اظهار نظر کنیم:

نیچه در اشاره به زمانه‌اش می‌گوید: «ما در عصری آشفته زندگی می‌کنیم، و به‌همین خاطر، شورانگیز نیست. این عصر مدام خودش را گرم می‌کند، زیرا احساس می‌کند گرم نیست، بلکه اساساً یخ زده است..... در زمانه ما رویدادها یا وقایع صرفاً با استفاده از پژواک روزنامه‌ها [یا رسانه‌ها] عظمت [پوشالی شان] را به‌دست می‌آورند.» (Heidegger, 1979, p. 47).

این سخن نغز و پرمغز نیچه را از چند جهت بررسی می‌کنیم: اولاً از حیث رخدادها و ظهوراتی همچون روزنامه و اینترنت و شبکه‌های مجازی و ...؛ و ثانیاً از جهتی عمیق‌تر که نیچه این عصر بدون شورانگیزی را عصر افلاطون‌زده یا نیهلیسم یا عصر متافیزیک می‌داند.

۲ ظهورات نیهلیسم در فضای سایبری

نیچه در کتاب اراده معطوف به قدرت می‌گوید آنچه درباره آن می‌گویم، در حقیقت تاریخ دو سده آینده است و آن هم چیزی نیست جز برآمدن نیهیلیسم یا نیست‌انگاری (نیچه، ۱۳۷۷، صص ۱۳–۱۹). و البته پُر بیراه نگفته است، و اکنون که بیش از یک قرن از آن زمان می‌گذرد، نهیلیسم خودش را در چهره عجیب و غریب رسانه و شبکه‌های مجازی و هویت‌های مجازی بروز داده است. البته ژیل دلوز به‌درستی تذکر می‌دهد که از نظر نیچه نیست‌انگاری نه به معنای ناموجود، بلکه به آن معناست که زندگی و انسان‌ها در آن خوار پنداشته شوند و زندگی در آن ارزش هم‌تراز با نیستی بیابد (دلوز، ۱۳۹۳، ص ۲۵۳) و در حقیقت در نیست‌انگاری شعار اصل انکار زندگانی است (دلوز، ۱۳۸۶، ص ۱۱۵). یعنی زندگی‌ها در نیهلیسم آنچنان پست و بی‌معنا و خوار می‌شوند که عنوانی همچون نیست‌انگاری و پوچ‌گرایی می‌تواند آن را بیان کند.

اساساً زندگی‌هایی که مدرنیته ساخته است و تشدید و اوج آن را می‌توانیم در فضای سایبری ببینیم،

بیشتر از نظم بیرونی‌اش شاید آشفتگی درونی‌اش به چشم نیچه آمده است. در این عصر هنگامی که نمونه‌های مشترکی از بزرگی یا عظمت نباشد که دغدغه‌ها و تعهد اجتماعی را برجسته کند، مردم صرفاً برای هیجان و تخدیر روحی خود، تماشاگران مدها (یا هوس‌ها یا علاقه دمدمی) و زندگی عمومی می‌شوند. وقتی هیچ عمل دینی وجود نداشته باشد که فداکاری ، رعب و وحشت را به همراه داشته باشد ، مردم همه چیز را مصرف می‌کنند ، از مواد مخدر گرفته تا اقدامات مدیتیشن (meditation یا تخیل)، تا نوعی تجربه والا را به خود بدهند غافل از اینکه در توهم تجربه والا هستند. در حقیقت این دوران دورانی است که انسان چون دستمایه خوبی برای زندگی در حقیقت و واقعیت ندارد همواره سعی دارد خود را تخدیر کند، این تخدیر گاهی با مواد مخدر است و گاهی با رسانه و فضای سایبری.

در این زندگانی چون تجربه والا و عظمت انسانی از دست میرود، ماهیت انسان نیز به نحوی دیگر تعریف می‌شود. ماهیت انسان در کامپیوتر و عصر کامپیوتر همچون کامپیوتر شده است، یعنی اینکه در علوم شناختی ذهن انسان را همچون دستگاهی محاسباتی مانند کامپیوتر می‌دانند (Loftus, 2019, pp 1-13) و منطق را به منطق ریاضی برمی‌گردانند و سعی بر آن دارند که همه رفتار انسان و زبان انسان را به‌صورت الگوریتمی و منطق ریاضی تفسیر کنند، همه نشان از آن دارد که انسان در حال ماشین شدن و ریاضی شدن است؛ و این امری است که فیلسوفان بزرگی چون دکارت و اسپینوزا و هابز و ... ایده آن را نوشته بودند، یعنی دکارتی که می‌گفت جهان همچون ماشینی بزرگ است و اسپینوزایی که می‌گفت: «من اعمال و امیال انسان را همان‌طور ملاحظه کردم که خطوط و سطوح و اجسام را ملاحظه کردم» (اسپینوزا، ۱۳۹۲، ص ۱۴۲) و این نگرش مکانیستی درباره جهان و انسان در هابز به‌نحوی دنبال می‌شود که او انسان را جسمی همچون دیگر اجسام می‌داند (هابز، ۱۳۹۳، ص ۵۴۳). این اتفاق در قرن بیستم با اختراع کامپیوتر و ماشین‌های پیشرفته به‌صورت جدی‌تری رخ می‌دهد تا جایی که وینر –همو که دانش سایبرنتیک را مطرح ساخت و بعدها واژه سایبر و مشتقات آن همانند فضای سایبری از سایبرنتیک گرفته شد– بر آن شد که با توجه به تشابهات خاصی از رفتار بین ماشین و موجود زنده مشاهده می‌شود، مشکل زنده بودن یا نبودن ماشین برای ما سمانتیک (معنایی) است و می‌توان از شر آن خلاص شد (Wiener, 1951, pp 31-32) و انسان را همچون پیام [یا اطلاعات] تصور می‌کرد (Wiener, 1951, p 100). وقتی انسان همچون ریاضیات و محاسبات شد، دیگر نیازی به قلب نیست که احساسی شود و عاطفه داشته باشد و برای خانواده دلسوزی کند و محبت بورزد و محبت ببیند و عاشق شود و زنده باشد. اکنون زمانه‌ای است که انسانِ بدون قلب و همانند یک کامپیوتر برای سیستم عظیم سرمایه‌داری کارآمدتر است و انسان همانند پیچ و مهره‌های این سیستم عمل می‌کند.

این الگوی ریاضی شدن انسان و هک شدن مغز انسان و بر اساس الگوی خاصی عمل کردن در فضای سایبری به‌طرز وحشتناکی انسان را از اصل و حقیقت خودش دور می‌سازد. در زمانه‌ای که فضای سایبری در شئونات مختلف آن حضور دارد و زندگی بدون فضای سایبری در آن غیرممکن است و به ادبیات دقیق تر تقدیر تاریخیِ انسان‌ها در فضای سایبری در حال رقم خوردن است، و این تقدیر چه بخواهیم و چه نخواهیم برای ماست، سعی بر آن دارد که انسان در الگوی ریاضیاتی‌اش عمل کند و به‌همین دلیل برای انسان الگوریتم‌های پیچیده‌ای طراحی می‌کنند که مثلاً هنگامی که در اینستاگرام یا یوتیوب یا ... هست، برای ساعت‌ها در آن حضور داشته باشد. در حقیقت انسان در این فضا به‌نحوی جادو می‌شود و برای انسان تخدیری در آن رخ

می‌دهد که از آنچه هست لذت ببرد و نخواهد به اصل و حقیقتش فکر کند.

انسان با این مشخصات تا جایی و تا حدومرزی می‌تواند همانی باشد که که آنها می‌خواهند، اما همین انسان نمی‌تواند همواره اینگونه باشد، چون بر اساس خلقتی آفریده شده که قلب و فطرت دارد و گاهی ندای این قلب و این فطرت او را بدخواب می‌کند، یعنی از این خوابی که برای او دیده اند می‌خواهد بیدار شود. نیچه از آن به عدم شورانگیزی در این زندگی اشاره می‌کند، این عدم شورانگیزی باعث می‌شود که انسان احساس افسردگی و سرما و یخزدگی کند، و احساس تحقیر و پوچی و نیستی؛ اما در عصر رسانه و فضای مجازی آن را با پژواک‌های متعددی که عظمتی پوشالی را نشان می‌دهند، سعی می‌کنند به انسان‌ها این باور را القا کنند که این جهان گرما و سرزندگی دارد، اما این عظمت پوشالی تنها انسان‌ها را تخدیر می‌کند و این باعث می‌شود که حقیقت را آنچنان که هست درنیابند.

انسانی که در فضای اطلاعات قرار می‌گیرد، لحظه به لحظه و آن به آن خبرها را دریافت می‌کند و ناعدالتی‌ها را نه در واقعیت بلکه در قاب رسانه تماشا می‌کند و لحظه به لحظه با پژواک‌های مختلفی از اطلاعات برخورد می‌کند، این برخورد شاید لذت‌آور باشد و انسان را تخدیر کند، اما بعد از مدتی نمی‌داند که کدام دروغ بوده است و کدام راست؟ کدام‌یک اهمیت بیشتری برایش داشته است؟ و چرا همه خبرها برایش به یک نحو است و هیچ‌کدام برایش دلهره و ترس و محبت و کینه و ... ایجاد نمی‌کند؟ بدتر اینکه این اطلاعات به‌صورت پژواکی بزرگ در حال بازتولید هستند و این پژواک رسانه‌ها همه هم و غم و دغدغه انسان ها را تصرف می‌کند تا جایی که در زمانه تلویزیون زن‌ها به مردهایشان می‌گفتند: تو با تلویزیون ازدواج کرده‌ای یا با من؟ بدتر اینکه خود انسان اگر به‌صورت اطلاعات فهمیده شود و برایش برنامه‌ریزی شود یعنی الگوریتمی برای کنترل انسان از طریق اطلاعات ایجاد شود، انسان خودش اسیر در اطلاعات می‌شود و همچون برده‌ای در فضای این اطلاعات با او برخورد خواهد شد و سعی می‌کنند اراده انسان را تسخیر کنند و البته پیش از آن انسان باید در این فضا تخدیر شده باشد.

تسخیر شدن اراده انسان توسط انسان‌های دیگر یا توسط ماشین و کامپیوتر باعثِ یک مرگ و یک زندگی می‌شود. مرگی که از آن سخن می‌گوییم منظورمان از دست دادن اراده و حقیقت انسانی برای کسانی است که تسخیر شده‌اند (و البته این مرگ می‌تواند مراتب داشته باشد و هرچه کمتر اراده انسانی در تسخیر بیفتد مرگ او کمتر است) و البته یک زندگی که از آن مرگ برآمده است، یعنی قلب و اراده انسان از او گرفته می‌شود و در عوض انسان همچون برده‌ای در خدمتِ اراده دیگری (انسان یا ماشین) قرار می‌گیرد و زندگی‌ای که تحت کنترل دیگری است و بر او دیکته می‌شود و این زندگی جدیدی است با قواعدی که برای کنترل انسانِ تسخیر شده نوشته شده است. مثال آن را می‌توانیم در فیلم ماتریکس ببینیم که اراده انسان از او گرفته شده است و او را در مخزنی لزجی که از آن تغذیه می‌شود نگهداری می‌کنند و در عوض به‌عنوان انرژی و باتری برای بقای ماتریکس از او استفاده می‌کنند، و در فضای ماتریکس به او زندگی جدیدی می‌بخشند و انسان‌ها بدون اینکه خبر داشته باشد در ماتریکس زندگی جدیدی را آغاز کرده‌اند و همه تحت کنترل ماتریکس قرار دارند.

این حالت‌هایی که برای انسان گفتیم، در حقیقت همانی است که انسان به پوچی و نیستی می‌رسد و این حالت را کم و بیش در فضای سایبری و اینترنت و فضای مجازی داریم که انسانیت انسان‌ها در خطر

قرار می‌گیرد و سعی می‌کنند او را به‌صورت کامپیوتر و ماشین ببینند، در حقیقت اصالت و حقیقت انسان (قلب و اراده) او را سعی دارند تسخیر کنند و این‌گونه مرگی برای انسان‌ها رقم خواهد خورد که آن را می‌توان نیستانگاری و نیهیلیسم عصر کنونی دانست. اما چون انسان‌ها قلب دارند و حس و عاطفه و محبت را می‌فهمند احساس پوچی می‌کنند، اما به قول مک‌لوهان در رسانه و به طور عام‌تر در فضای سایبری لحظه به لحظه سعی دارند که الگوهای احساسی انسان را به‌صورت مستمر و بدون مقاومت تغییر دهند (آوینی، ۱۳۹۳، ص ۶۳) و الگوهای احساسی انسان را به‌صورت الگوریتمی و ریاضیاتی درآورند و با بازتولید مدام این کار اجازه بیرون رفتن از تخدیر انسان را ندهند.

۳ عصر متافیزیک‌زده، عصر نیهلیسم و اینکه آیا فضای سایبری برخاسته از متافیزیک است؟

عصر آشفته‌ای که نیچه از آن سخن می‌گوید، همان عصر نیهلیسمی است که ظهور و نمود آن در روزنامه و اینترنت و فضای سایبری به چشم می‌خورد و این عصر به نظر نیچه عصر متافیزیک‌زده‌ای است که از افلاطون شروع شده است. در حقیقت نیچه و هایدگر عصر مدرن را نتیجه و برآمد تاریخی می‌دانند که از افلاطون آغاز شده و تمامی تاریخ را تحت تأثیر خودش قرار داده است و این‌گونه همه تاریخ را افلاطونیسم یا افلاطون‌زده می‌دانند. بر این اساس برای یافتن معنای عمیق نیهلیسم و فهم تاریخ غرب نیازمند آن هستیم که بدانیم در چه فضایی شکل گرفته است و خاستگاه نیهلیسم چیست و کجاست؟ شروعی که از افلاطون بوده و با ارسطو ادامه پیدا کرده و همه تاریخ فلسفه و تاریخ را تحت تأثیر خودش قرار داده است از نظر نیچه بنیاد و اساس نیهلیسم است، به این ترتیب متافیزیک اساس نیهلیسم است. متافیزیکی که به نظر وایتهد چیزی جز حاشیه‌نگاری بر افلاطون نبوده است (مگی، ۱۳۷۲، ص ۵). این افلاطون‌زدگی را نیچه در کتاب غروب بتان در ۶ مرحله تصویر کرده است (نیچه، ۱۳۸۶، ص ۲۸) و نشان داده است چگونه به نیهلیسم انجامیده و البته سعی نیچه بر آن بوده است که از چنبره آن رهایی یابد.

اما اینکه آیا فضای سایبری و مظاهر آن را باید در ادامه متافیزیک و فلسفه غرب بدانیم یا نه؟ باید گفت که اگر اینگونه نباشد، یعنی مظاهر تمدنی غرب را جدای از تاریخ آن فهم کنیم، اساساً در فهم فضای سایبری و اینترنت و ... با مشکلی بزرگ روبرو خواهیم بود و امکان فهم دقیق آن را نخواهیم یافت؛ در حقیقت اینها به یکباره به وجود نیامدند و برآمده از تاریخ غرب هستند. خاستگاه برخی از مهم‌ترین چیزهایی که به کامپیوتری شدن جهان امروز انجامیده است در افلاطون و ارسطو قابل پیگیری است، مثلاً بر کسی پوشیده نیست که منطق ریاضی باعث شده که ایده‌های کامپیوتری شدن به وجود آید و منطق ریاضی مدیون منطق صوری ارسطو است که سعی داشته است تفکر آدمی را به‌صورت قواعدی درآورد و عرضه کند و منطق ریاضی نیز به دنبال قاعده‌سازی برای تفکر انسان است، همین ایده قاعده‌مندسازی و الگوریتم‌سازی و صوری‌سازی برای تفکر و استدلال انسان نمونه‌ای است که نشان می‌دهد چگونه جهان کامپیوتری شده برآمده از خاستگاهی است که از یونان شروع شده است. همین ایده‌های صوری‌سازی و متافیزیکی کردن جهان باعث می‌شود که حقیقت و اصل و اراده انسان از او گرفته شود و دچار نیهلیسم شود.

از طرفی مباحثی مانند سایبرنتیک کاملاً برگرفته از مهندسی کنترل هستند که مهندسی کنترل ادامه منطقی سیر فیزیک نیوتون است و خاستگاه فیزیک نیوتونی همان نگرش ماشینی به عالم است که از دوره رنسانس در غرب ایجاد شده است و پس از آن در فلسفه دکارت و اسپینوزا و هابز و ... مشاهده می‌شود.

از اینها مهم‌تر و اساسی‌تر الگوی ریاضیاتی شدن جهان است (هیدگر، ۱۳۹۵). ریاضیاتی شدن جهان در حقیقت آن اصل و اساس مهمی است که جهان جدید با آن شکل گرفته و مثلاً نتیجه آن را در فیزیک نیوتونی و سایبرنتیک و کامپیوتر و حتی فضای سایبری می‌بینیم، به این ترتیب نتیجه ریاضیاتی شدن جهان چیزی جز آن نیست که همه عالم به‌صورت ابژه درآورده شوند و این‌گونه امکان عددی شدن و کامپیوتری شدن آنها فراهم شود و حتی انسان را به‌صورت کامپیوتر و ماشین تصویر کنند و مثلاً نوربرت وینر انسان را همچون پیام و اطلاعات تصور می‌کرد و زنده بودن انسان را با توجه به شباهت انسان به ماشین بی‌وجه قلمداد می‌کرد (Wiener, 1951, pp 31-32) که نتیجه آن ابژه شدن انسان و از دست رفتن اراده و حقیقت اوست.

۴ برون‌رفت از نیهلیسم با هنر بزرگ

هیدگر معتقد است نگرش تکنولوژیکی به جهان هستی به جایی رسیده است که باعث بی‌معنا شدن زندگی و از دست رفتن ارزش‌ها شده (Dreyfus, 1993, p 303) و این امر در فضای سایبری و شبکه‌های مجازی گویاتر و آشکارتر است.

اما راه حل غلبه بر نیستانگاری چیست؟ و چگونه می‌توان از این افسردگی و نیهلیسم رهایی یافت؟ نیچه و پس از او هیدگر در مواجهه با نیهلیسم به هنر توجه کردند و امکان گذار و غلبه بر این مهم را در هنر یافتند (ذاکری، سعیدی، ۱۳۹۹، ص۷). هنری که می‌تواند پیکربندی جدیدی از جهان ارائه دهد و عالم فرهنگی دیگری بسازد (Dreyfus, 2005, p 416). به این ترتیب هیدگر معتقد است: «هنر باید حرکت مخالف نیستانگاری یعنی تثبیت‌کننده عالی‌ترین ارزش‌های نوین باشد؛ هنر باید معیارها و قوانین هستیِ روحیِ تاریخی را به دست دهد و بنیاد گذارد» (هایدگر، ۱۳۸۷، صص ۴-۲۲۳). هنر همان پناهگاهی است که می‌تواند بنیان‌های جدیدی برای این این عالم بگذارد و بنیان جهان افلاطون‌زده را تخریب کند، و درست‌تر اینکه می‌تواند با در انداختن طرحی نو انسانها را از چنگال نیهلیسم نجات دهد (ذاکری، سعیدی، ۱۳۹۹، ص ۲۱). اما هنری که هیدگر مدنظر دارد آن هنری است که از دام متافیزیک و نگرش افلاطونی به آن رها شده باشد، یعنی در حقیقت هنری که این امکان را فراهم آورد که انسان از این افسردگی و سردی و خمودگی نجات یابد و جهانی غیرمتافیزیکی بیافریند که در آن انسان و جهان ریاضیاتی و متافیزیکی نباشند و امکان آفرینش‌گری و خلاقیت از طریق آن فراهم شود تا قوم و جامعه و جهان جدیدی را بسازد.

هنری که می‌تواند چنین کند تنها هنر بزرگ است زیرا «هنر بزرگ قومی را به وجود می‌آورد یعنی عالم آن قوم را می‌سازد و تاریخ آن را رقم می‌زند، پس می‌توان گفت هنر بزرگ تاریخی را ایجاد می‌کند و بنیان‌گذار تاریخی خاص خواهد بود. برای اینکه عالمی فراهم شود، باید تصمیم‌های اصیل تاریخی گرفته شده و پرسش و دغدغه افراد آن قوم شوند. هایدگر باور دارد که کار هنری می‌تواند از این طریق سنت و فرهنگ و ادب یک قوم را عوض کند. در حقیقت کار هنری آنگاه که تحقق پذیرد، اگر پیوندی با عرف نداشته باشد یا اینکه

پیوندش ضعیف و گسسته بنماید، به همان نسبت تکان‌دهی و سهمگینیِ خلاف آمد عادت آن بیشتر است و آنچه برای مردم و عرف عادی جلوه می‌کرد، در کار هنری دگرگون می‌شود. هرگاه هنر روی می‌دهد، آغازی درکار است، و تاریخی نو تأسیس می‌کند. تاریخ پناهگاهی است که هر قومی در آنچه از وجود به او حوالت شده است استقرار می‌یابد؛ و به همین دلیل است که پرسش از هنر و دغدغه کار هنری هایدگر مهم و اصیل است» (ذاکری، سعیدی، ۱۳۹۹، ص۲۱).

۵ نتیجه‌گیری

فضای سایبری و شبکه‌های مجازی و اینترنت با همه مزیت‌هایی که ایجاد می‌کند، باعث تشدید نیهیلیسم یا نیستانگاری در زندگی انسان شده است، و حتی برخی گفته‌اند که اینترنت انسان را احمق کرده است و انسان از فطرت و اصالت خویش به دور افتاده است.

فضای سایبری و اینترنت و شبکه‌های مجازی که ظهورات نوین در تمدن غرب هستند از خاستگاه و سرچشمه‌ای نتیجه شدند که بر اساس آن جهان و انسان به صورت ریاضیاتی درآمدند و نهایتاً انسان‌ها را به‌صورت کامپیوتر و ابژه تصویر می‌کنند و اراده و تصمیم انسان را کنترل می‌کنند.

حال دوباره می‌توان این سؤال را مطرح کرد که آیا هنر بزرگ می‌تواند سردی برآمده از فضای سایبری و روزنامه و تلویزیون را بشکند؟ در حقیقت این سردی و یخزدگی به‌نوعی جهش و جرقه و رعد و برق لازم دارد تا تاریخ جدید و عالم جدید رقم بخورد، عالمی که دکارت و هگل و ... صورت‌بندی آن را در فلسفه آورده‌اند و پیش از آنها در زندگی‌های جدیدی که از رنسانس به بعد شکل گرفته بود، به نمایش درآمد. شاید هنر بزرگ بتواند برای غلبه به آن کمک کند!!!

مراجع

[۱] آوینی، مرتضی (۱۳۹۳)، آینه جادو، ج۱، تهران، نشر واحه.
[۲] اسپینوزا، باروخ (۱۳۹۲)، اخلاق، ترجمه محسن جهانگیری، تهران، مرکز نشر دانشگاهی.
[۳] دلوز، ژیل (۱۳۹۳)، نیچه و فلسفه، ترجمه عادل مشایخی، تهران، نشر نی.
[۴] دلوز، ژیل، نیچه (۱۳۸۶)، ترجمه پرویز همایون‌پور، تهران، نشر قطره.
[۵] ذاکری، مهدی، سعیدی، مرتضی (۱۳۹۹)، چگونگی غلبه هنر بر متافیزیک غرب در تفکر هایدگر، نقد و نظر، سال بیست و پنجم، زمستان، شماره ۱۰۰.
[۶] مگی، براین (۱۳۷۲)، فلاسفه بزرگ، ترجمه عزت‌الله فولادوند، تهران، انتشارات خوارزمی.
[۷] نیچه، فریدریش (۱۳۷۷)، اراده قدرت، ترجمه دکتر مجید شریف، تهران، انتشارات جامی.
[۸] نیچه، فریدریش (۱۳۸۶)، غروب بت‌ها، ترجمه داریوش آشوری، تهران، نشر آگاه.
[۹] هابز، لویاتان (۱۳۹۳)، تهران، نشر نی، ترجمه حسین بشیریه.
[۱۰] هایدگر، مارتین (۱۳۸۷)، نیچه، ج ۱، ترجمه ایرج قانونی، تهران، نشر آگه.
[۱۱] هیدگر، مارتین (۱۳۹۵)، عصر تصویر جهان، ترجمه یوسف اباذری، مجله ارغنون شماره ۱۱ و ۱۲.

[12] Dreyfus, H. L. (1993), Heidegger on the connection between nihilism, art, technology, and politics, in Charles Guignon (ed), The Cambridge Companion to Heidegger, Cambridge: Cambridge University Press.

[13] Dreyfus, H. L. (2005), "Heidegger's Ontology of Art", in H. L. Dreyfus and M. A. Wrathall (eds), A Companion to Heidegger, Oxford: Blackwell.

[14] Heidegger, Martin (1979), Nietzsche, Volume One, Harper and Row.

[15] Loftus ,Geoffrey R., Loftus, Elizabeth F. (2019), Human Memory: The Processing of Information, New York, Psychology Press.

[16] Wiener, Norbert (1951), THE HUMAN USE OF HUMAN BEINGS, MIT Press.

نقش میدان‌های الکترومغناطیس درون‌زاد و برون‌زاد در پیشبرد تکوین جنین

سمیرا کاتبی کوشالی [۱]

[۱] دکتری زیست‌شناسی گرایش سلولی تکوین، دانشگاه اصفهان
sahab135@gmail.com

چکیده

درک عوامل موثر در تکوین سلول تخم از دیرباز ذهن محققان را به خود مشغول داشته است . آنچه طی سالیان دراز از فرایندهای دخیل در قطبیت، ریخت‌زایی و اندام‌زایی جنین به‌دست آمده، ناشی از تلاش بی‌وقفه‌ی محققان در عرصه زیست‌شناسی مولکولی، بیوشیمی و ژنتیک بوده است. در این میان میدان‌های الکترومغناطیس و تابش‌ها به‌عنوان یکی از شاخه‌های مهم بیوفیزیک در رابطه با جنین‌شناسی نادیده گرفته شده است. به‌موازات پیشرفت علوم سلولی مولکولی و الکتروفیزیولوژی، دریچه‌ای تازه به‌روی محققان زیست‌شناسی تکوینی گشوده شد که به نقش بسیار مهم میدان‌های الکترومغناطیس در پیشبرد صحیح فرایندهای تکوین در موجودات زنده اشاره داشت. آزمایش‌های انجام شده طی نیم قرن بیانگر این است که جنین قادر به تولید میدان‌های الکترومغناطیس و تابش‌هایی بسیار ضعیف است که در ایجاد قطبیت، مهاجرت سلول‌ها و ریخت‌زایی فوق العاده حائز اهمیت‌اند. در مقاله حاضر به اهمیت میدان‌های الکترومغناطیس طبیعی و مصنوعی در پیشبرد فرایندهای تکوین جنین پرداخته شده است.

کلمات کلیدی: میدان‌های الکترومغناطیسی، جنین، تکوین، ریخت‌زایی.

۱ مقدمه

یکی از جذاب‌ترین مباحث زیست‌شناسی تکوینی، ریخت‌زایی است. ریخت‌زایی پدیده‌ای است که به خودسازمان‌یافتگی سیستم‌های زنده اشاره دارد. در این فرایند از سلول‌های ابتدایی جنین، ساختارهایی پیچیده و عملکردی ایجاد می‌شود. ژنتیک مولکولی و بیوشیمی در جهت درک مکانیسم‌های دخیل در ریخت‌زایی و کشف مولکول‌ها و پیام‌رسان‌های سلولی نقش به‌سزایی داشته‌اند. در این میان میدان‌های الکترو مغناطیسی و تابش‌ها به‌عنوان یکی از شاخه‌های مهم بیوفیزیک در جنین‌شناسی مدرن نادیده گرفته شده است. بسیاری از فرایندهای تکوینی همانند قطبیت، اطلاعات وابسته به مکان، اندام‌زایی و ارتباطات سلولی رابطه‌ی تنگاتنگی با فیزیک الکترو مغناطیس دارند (Levin, 2003). شواهد حاکی از آن است که

میدان‌های الکتریکی، مغناطیسی و تابش‌های فوتونی بسیار ضعیف درون‌زاد سلول‌ها، در واقع همانند نوعی سیستم اطلاعاتی عمل می‌کنند (Basset, 1993). در این بازنگری سعی بر آن است تا به نقش غیرقابل انکار میدان‌های الکترو مغناطیس طبیعی، میدان مغناطیسی درون‌زاد سلول‌ها و میدان مغناطیسی کره‌ی زمین در فرایندهای دخیل در تکوین جنین بپردازیم.

۲ پیشینه‌ی پژوهش

در مطالعات بی‌شماری به اثرات میدان های الکترومغناطیسی در ایجاد و تکامل حیات اشاره شده است. می‌توان این مطالعات را در دو شاخه‌ی بایومگنتیزم[۱] و مگنتوبیولوژی[۲] تقسیم‌بندی کرد. در حوزه‌ی بایومگنتیزم به میدان‌های الکترومغناطیسی تولید شده توسط سلول و بافت‌های بدن موجود زنده، پرداخته می‌شود؛ در حالی که در حوزه‌ی مگنتوبیولوژی اثر میادین الکترومغناطیسی خارجی بر سیستم‌های زنده مورد بررسی قرار می‌گیرد (Marko and Markov, 2011). دانشمندان در این دو حوزه، از شواهد همبستگی[۳]، به‌دست آوردن عملکرد[۴] و فقدان عملکرد[۵]، به منظور کشف اهمیت میادین الکترو مغناطیسی بر فرایندهای زیستی بهره می‌برند (Levin, 2001).

بزرگی و مقیاس‌سنجی میدان الکترو مغناطیسی با واحد تسلا بیان می‌شود. از آنجا که واحد مذکور بسیار بزرگ است، از سایر واحدهای کوچکتر همانند گاوس، میلی تسلا و میکرو تسلا استفاده می‌شود. هر تسلا معادل ۱۰.۰۰۰ گاوس است. میدان مغناطیسی کره‌ی زمین ناشی از هسته‌ی آهنی آن است و در محدوده‌ی ۵۰ میکرو تسلا شدت دارد. این میزان ناچیز در حفظ هومئوستاز بدن جانوران بسیار ضروری است (Funk, 2009).

گلد در سال ۱۹۸۴ در گزارش خود بیان داشت که موجودات زنده –از باکتری تا پستانداران– همگی به میدان–های مغناطیسی حساس‌اند (Gould, 1984). میدان مغناطیسی (GMF) و میدان الکتریکی کره‌ی زمین (GEF) بخش اعظم اطلاعات موجود در یونوسفر را شامل می‌شوند (Cole, 1974). با توجه به جدول ۱ می‌توان دریافت که حذف میدان مغناطیسی زمین باعث ایجاد طیف وسیعی از ناهنجاری‌ها و تغییرات فیزیولوژیک در موجودات زنده می‌شود (Levin, 2003). این ایده که ریخت‌زایی موجودات با واسطه‌ی میدان‌های الکترومغناطیسی درون‌زاد آنها تعیین می‌شود برای نخستین بار توسط بور Burr et, 1937) al) و لاند (Lund, 1947) مطرح شد. هر دو گروه، آزمایش‌های وسیعی را بر طیف وسیعی از موجودات انجام دادند و به این نتیجه رسیدند که تغییرات میدان‌های الکتریکی طبیعی با فرایندهای تکوین و ترمیم موجودات زنده رابطه‌ی تنگاتنگی دارد. در واقع آنها برای اولین بار این مطلب را اثبات کردند که میدان‌های الکترومغناطیسی خارجی می‌توانند ریخت‌زایی و عملکرد طیف وسیعی از موجودات را تغییر دهد.

[1] Bio magnetism
[2] Magneto biology
[3] Correlative evidence
[4] Gain of function
[5] Loss of function

میدان‌های الکتریکی بر یون‌های موجود در سلول نیرو وارد می‌کنند در حالی که میادین مغناطیسی بر ذرات مغناطیسی درون سلول و یون‌های در حال حرکت نیرو وارد می‌کنند. در کل باید گفت میدان‌های الکترو مغناطیسی قادر هستند واکنش‌های بیوشیمیایی و رفتار مولکول‌های باردار سلول را تغییر دهند (Barnes, 1992)، میدان‌های مغناطیسی اثر خود بر سلول را از چند مسیر اعمال می‌کنند؛ تولید میدان‌های الکتریکی در هادی، وارد کردن نیرو بر حامل‌های باردار در حال حرکت، وارد کردن فشار بر دو قطبی‌های مغناطیسی دائم و ذرات دیامغناطیس یا پارامغناطیس غیر کروی (درصورت اعمال میدان مغناطیسی ناهمگن) و تغییر نرخ انتشار غشای سلولی (Barnothy, 1999).

۳ ادبیات پژوهش

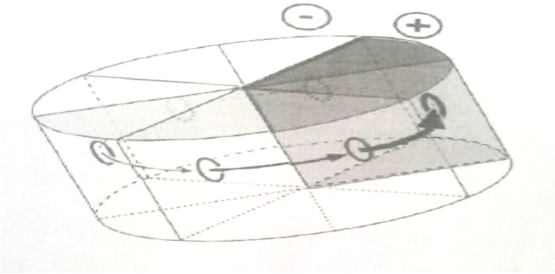
۱.۳ تابش‌های میتوژنیک درون‌زاد

سلول‌ها و بافت‌های زنده طیف وسیعی از فوتون‌های فوق ضعیف را در محدوده‌ی فرابنفش و فروسرخ تابش می‌کنند. مطالعات نشان می‌دهند این امواج در فرایندهای تکوینی نقش بسیار مهمی دارند و قادر هستند بدون وجود ارتباطات شیمیایی از سلولی به سلول دیگر منتقل شوند و در جهت پیام‌رسانی اقدام کنند.

لوین اولین کسی بود که بر روی تابش‌های میتوژنیک سلول‌ها مطالعه کرد. او دریافت که این تابش‌ها با چرخه‌ی تقسیم سلول و متابولیسم آن در ارتباط است. در سال ۱۹۸۳ الگویی مبتنی بر برهم‌کنش بین بیوفوتون‌ها و DNA ارائه شد. در این مدل حلقه‌ی بازخورد منفی بین کانفورماسیون DNA و بیوفوتون‌های نشر شده از سلول در نظر گرفته می‌شود چیروت[۶] در سال ۱۹۸۶ بیان داشت که تابش‌های میتوژنیک به‌عنوان حامل‌های اطلاعاتی بین سلولی عمل می‌کنند. بیوفوتون‌ها بر بیومولکول‌هایی چون DNA اثر می‌گذارند و امواج فروسرخ نیز ناشی از فعالیت سانتریول‌ها هستند. با گسترش علوم سلولی – مولکولی و کشف اهمیت کانال‌های یونیِ سدیم، پتاسیم، کلسیم و گیرنده‌های وابسته به ولتاژ، نقش میدان‌های الکتریکی درون‌زاد در فرایندهای مهم زیست‌شناسی روز به روز پررنگ‌تر شد. میدان‌های الکترومغناطیسی درون‌زاد، در نتیجه‌ی حرکت بارهای الکتریکی یون‌ها و دوقطبی‌ها در عرض غشاء و یا بین سلول‌ها ایجاد می‌شوند (Funk, 2009, Marco, 2011).

مطالعات وسیع دو گروه مک‌کیاگ و لوین ثابت کرد میدان‌های الکترومغناطیسی به‌طور مستقیم با پدیده‌های مهم زیست‌شناسی در ارتباط هستند. لوین در گزارشی شرح داد که میدان‌های الکتریکی تولید شده توسط کانال‌های یونی هیدروژن پتاسیم و به خصوص کلسیم، سیگنال‌های خاصی را ایجاد می‌کنند که رفتار سلول را طی رشد جنینی، تغییرات طبیعی بافتی و فرایندهای ترمیمی تنظیم می‌کند. میدان‌های الکترومغناطیسی درون‌زاد، طی مراحل مختلف جنینی به‌طور طبیعی ظاهر می‌شوند. برای مثال طی رشد اولیه‌ی جنین دوزیست و جوجه میدان‌های الکتریکی درون‌زاد در نتیجه‌ی جذب غیر فعال سدیم از محیط تولید شده و منجر به ایجاد اختلاف پتانسیل مثبت بین سلول‌های اپی‌تلیوم (TEP) می‌گردد. اختلاف TEP

[۶] Chwirot



شکل ۱: شیب غلظت مولکول‌های کوچک در اثر میدان الکتریکی درون‌زاد

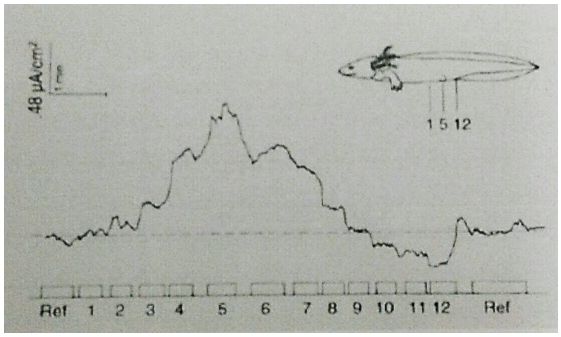
در نواحی مختلف، شیب ولتاژ داخل جنینی را ایجاد می‌کند. بزرگی این میادین الکتریکی درون‌زاد در حدود ۱ تا ۵ ولت بر سانتی‌متر گزارش شده است که این مقدار برای اثر گذاشتن بر مورفولوژی سلول و مهاجرت آن در شرایط آزمایشگاهی بسیار مناسب است.

باید توجه داشت میدان‌های الکتریکی تولید شده با پتانسیل عمل سلول‌های عصبی کاملاً متفاوت است زیرا پتانسیل عمل کاملاً در غشاء سلولی محصور شده است؛ در حالی که میدان‌های الکتریکی درون‌زاد، قادر هستند تا صدها میکرومتر حتی در فضای خارج سلولی به خوبی گسترش یابند. در واقع این میادین در مقایسه با پتانسیل‌های عمل کم‌دوام قادر هستند شیب‌هایی از ولتاژ را طی چند روز ایجاد کنند. لوین و آدامز در آزمایشی جالب به اهمیت این میادین در ایجاد عدم تقارن راست - چپ اشاره کردند. آنها بیان داشتند که میادین درون‌زاد ناشی از جریان نامتقارن یون‌های هیدروژن در نتیجه‌ی فعالیت پمپ سدیم پتاسیم به‌عنوان نیروی پیش‌رونده برای جابه‌جایی مولکول‌های کوچک در جنین ابتدایی ظاهر می‌شوند. همان‌طور که درشکل یک نشان داده شده است، در نتیجه‌ی وجود میدان الکتریکی درون‌زاد، شیبی از غلظت مواد در سلول‌های مجاور مشاهده می‌شود؛ بدین صورت که حداکثر غلظت در قطب مثبت و حداقل آن در قطب منفی ایجاد می‌شود.

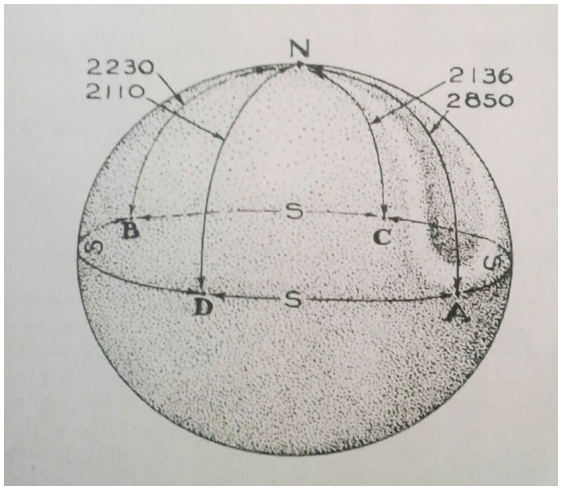
۲.۳ نقش میادین درون‌زاد در شکل‌گیری اندام

روبینسون و بورگن آزمایش‌های جالبی بر روی جنین دوزیستان انجام دادند تا به نقش میدان‌های الکتریکی درون‌زاد جنین در شکل‌گیری اندام پی ببرند. اندام‌زایی در جنین دوزیستان در منطقه‌ی جانبی جنین با سست شدن اپی‌تلیال آغاز می‌گردد و به دنبال آن مهاجرت سایر سلول‌ها به این ناحیه رخ می‌دهد. روبینسون و هوتاری برای آزمایش خود از لارو اکسولوت[۷] استفاده کردند. آنها دریافتند یک هفته پیش از تشکیل پای عقبی در قسمت جانبی جنین، جریان‌های رو به خارج در اپی‌تلیوم ظاهر می‌شود و به تدریج شدت آنها تا بروز جوانه‌ی اندام افزایش می‌یابد. حداکثر جریان در حدود ۲ تا ۳ میکرو آمپر در سانتی‌متر قبل از بروز جوانه‌ی اندام ظاهر شده است.

[7] axolot



شکل ۲: جریان‌های الکتریکی اندازه گیری شده در طرفین جنین اکسولوت طی تشکیل جوانه اندام حرکتی. در منطقه ۵ حداکثر جریان الکتریکی درون‌زاد ثبت شد.



شکل ۳: شیب ولتاژ بین قطب حیوانی و ۴ نقطه از ناحیه استوایی تخم قورباغه: بیشترین ولتاژ، محل آینده لوله عصبی را نشان می‌دهد.

بورگن و روبینسون بیان داشتند با اندازه‌گیری جریان‌های درون‌زاد در طرفین جنین می‌توان محل و زمان بروز جوانه‌ی حرکتی را پیش‌بینی کرد. با توجه به شکل ۲ در ناحیه ۵ طرفین جنین حداکثر جریان‌های الکتریکی اندازه‌گیری شد. این ناحیه دقیقاً محلی است که جوانه‌ی اندام ظهور خواهد کرد.

بورگن و روبینسون متوجه شدند که بعد از ظهور جوانه، اندام میدان‌های الکتریکی رو به کاهش می‌گذارند و حتی در مواردی معکوس می‌شوند. آنها در ادامه‌ی کار خود به تحلیل جالبی رسیدند، اینکه مهاجرت سایر سلول‌ها طی اندام‌زایی به منطقه‌ی جوانهی اندام به این دلیل است که جوانه‌ی اندام همانند کاتد عمل می‌کند که از نظر ولتاژ منفی‌تر است.

بور نیز توانست نشان دهد که میتوان با اندازه گیری ولتاژ در نقاط مختلف تخم قورباغه مکان تشکیل دستگاه عصبی را تعیین کرد (شکل ۳).

جدول ۱: تحقیقات انجام شده در بیومگنتیزم

آزمایش	جزئیات	منابع
میدان‌های الکترومغناطیسی درون‌زاد در موجودات در حال تکوین	– میدان‌های درون‌زاد سبب هدایت مواد به سمت تخمک می‌شود. – جنین جوجه و موش میدان‌هایی را در اطراف خود ایجاد می‌کنند. – لوله‌ی عصبی دوزیستان، میدان‌های بزرگی را ایجاد می‌کند.	Nuccitelli, R. (1983), Barish, M.E. (1983), Levin, M. (2003), D. Borgens, R. B. (1989), Burr, H.S. (1941a), Burr, H.S. (1947a)
میدان‌های درون‌زاد مرتبط با پدیده‌های تکوینی	– با سنجش میدان‌های درون‌زاد موجود در تخم، می‌توان مکان سر در جنین ابتدایی را پیش‌بینی کرد. – میدان‌های درون‌زاد جنین دوزیست بسیاری از فرایندهای ریخت‌زایی را هدایت می‌کند. – میدان‌های الکترومغناطیسی درون‌زاد قبل از ظهور اندام‌ها ایجاد شده. بنابراین می‌توان اندام‌زایی را پیش‌بینی کرد.	Burr, H.S. (1941a), D. Borgens, R. B. (1989), Borgens, R. B., Metcalf, M. E. (1994), Borgens, R. B. (1979), Levin, M. (2003), D. Borgens, R. B. (1989)

۴ نتیجه‌گیری

در این بازنگری، میدان‌های الکترومغناطیسی جنینی مورد بررسی قرار گرفتند. گورویچ[8] تقریباً صد سال پیش بیان داشت سلول‌ها، میدان‌هایی را به منظور تعیین سرنوشت نهایی خود طی تکوین ایجاد می‌کنند. آزمایش‌های بی‌نظیر بورگنز، روبینسون و هوتاری[9] مفهوم جدیدی از تکوین را ارائه کرد. بورگنز نشان داد میدان‌های الکتریکی، شیب‌های ولتاژ سه بعدی را درون جنین ایجاد می‌کنند که در مسیر تکوین جاندار نقش بسیار مهمی دارند. او حتی توانست توپوگرافی این میدان‌های درون‌زاد را ترسیم کند. جریان‌های الکتریکی اولیه‌ی جنین در راستای محورهای صلی جنین –سر – دم) و پشتی – شکمی شکل می‌گیرند. شیب‌های ولتاژ همانند آنچه در طول محور سر – دم ایجاد می‌گردد به سلول‌ها در شناسایی موقعیت‌شان کمک کرده و مهاجرت آنها را در مسیر صحیح ممکن می‌سازد.

میدان‌های ایجاد شـده درون جنین در نقاط مختلف و زمان‌های مختلف یکسان نیستند و همین امر سبب ایجاد الگوهای پیچیده‌ای از میدان در سراسر جنین می‌شود و به دنبال آن ساختارها و بافت‌های متفاوتی در قسمت‌های مختلف جنین شکل می‌گیرد. سلول‌های مختلف پاسخ‌های متفاوتی را به میدان‌های الکترو مغناطیسی موجود در جنین می‌دهند و حتی آستانه‌ی خاصی برای پاسخ خود به میدان دارند.

روبینسون ثابت کرد که جنین قادر است با تولید میدان‌های الکترو مغناطیسی، تشکیل ساختارهای خاص و تعیین قطبیت بخش‌های مختلف را هدایت کند. برای مثال شکل‌گیری لوله‌ی عصبی، روده و جوانه‌ی اندام

[8] Gorwitch
[9] Borgens, Robinson, Hotary

حرکتی در نتیجه‌ی ظهور وابسته به زمان و مکان این میادین است.

یافته‌های این محققان در طول سی سال اخیر تحولی عظیم در درک چگونگی تکوین و رشد موجود زنده ایجاد کرده است. امید آن می‌رود که بتوان در آینده‌ای نزدیک به درک بیشتری از مکانیسم‌های تکوین در سطح سلول، بافت و حتی ژن‌ها برسیم و بتوانیم در مراحل بالاتر در جهت ترمیم و درمان ضایعات با داشتن درک درستی از میادین الکترومغناطیسی درون‌زاد گام برداریم.

پیشنهادهایی جهت انجام تحقیقات گسترده در آینده:

- ارزیابی نقش میدان‌های الکترومغناطیسی بر عملکرد ، مهاجرت و سرنوشت سلولی
- ارزیابی نقش میدان‌های الکترومغناطیسی بر القای تمایز عصبی سلول‌های بنیادی
- انتقال هدفمند و کارامد ژن به سلول تحت میدان مغناطیسی و بکارگیری نانوذرات مغناطیسی
- تعیین روند تکوین جنین و سرنوشت سلولی با بکارگیری میادین و نانوذرات مغناطیسی
- تعیین مسیر سرنوشت سلولی با بکارگیری میادین و تابش‌های خاص

مراجع

[1] Altizer, A., Moriarty, L., Bell, S., Schreiner, C., Scott, W., Borgens, R. (2001). “Endogenous electric current is associated with normal development of the vertebrate limb”. Dev Dyn 221:391-401.

[2] Anderson, M., Bowdan, E., Kunkel, J.G. (1994). “Comparison of defolliculated oocytes and intact follicles of the cockroach using the vibrating probe to record steady currents”. Dev Biol 162: 111-122.

[3] Asashima, M., Shimada, K. Pfeiffer, C. J. (1991). “Magnetic shielding induces early developmental abnormalities in the newt”. Bioelectromagnetics 12:215-224.

[4] Barish, M. E. (1983). “Atransient calcium-dependent chloride current in the immature Xenopus oocyte”. J Physiol 342:309-325.

[5] Bohrmann, J., Dorn, A., Sander, K., Gutzeit, G. (1986a). “The extracellular electrical current pattern and its variability in vitellogenic Drosophila follicles”. J, Cell Sci 81:189-206.

[6] Borodin, Y.I., Letiagin, A.Y. (1990). “Reaction of circadian rhythms of the lymphoid system to deep screening from geomagnetic fields of the earth”. Biull Eksp Biol Med 109(2):191-193.

[7] Bohrmann, J., Huebner, E., Sander, K., Gutzeit, H. (1986b). “Intracellular electrical potential measurements in Drosophila follicles”. J, Cell Sci 81:207-221.

[8] Barnes, F.S. (1992). “Some engineering models for interactions of electric and magnetic fields with biological systems”. Bioelectromagnetics Suppl 1:67-85.

[9] Borgens, R. B. (1982). “What is therole of naturally produced electric current in vertebrate regeneration and healing’?” Int. Rev. Cytology, Vol. 76, pp. 245-298.

[10] D. Borgens, R. B. (1989). “Natural and Applied Currents in limb Regeneration and Development”. In Electric Field and Vertebrate Repair, pp.27-75.

[11] Borgens, R. B., Callahan, L., Rouleav, M. F. (1987). “Anatomy of axolotl flank integument during limb bud development with special reference to a transcutaneous current predicting limb formation”. J. Exp. Zool., Vol. 244, pp. 203-214.

[12] Borgens, R. B., Metcalf, M. E. (1994). “Weak applied voltage interfere with amphibian morphogenesis and pattern”. J. Exp. Zool., Vol. 268, pp. 322-338.

[13] Borgens, R. B., Rouleav, M.F., Delanney, L.E. (1983). “A steady efflux of ionic current predicts hind limb development in the axolotl”. J. Exp. Zool., Vol. 228, pp. 491-503.

[14] Borgens, R. B., Shi, R. (1995). “Three-dimentional gradiants of voltage during development of the nervous system as invisible coordinates for the establishment of embryonic pattern”. Dev Dyn, Vol. 202, pp. 101-114.

[15] Borgens, R. B. (1995). “Uncoupling histogenesis from morphogenesis in the vertebrate embryo by collapse of transneural tube potential”. Dev Dyn, Vol. 203, pp. 456-467.

[16] Borgens, R. B. (1979). “Small artificial currents enhance Xenopus limb regeneration”. J. Exp. Zool., Vol. 207, pp. 217-255.

[17] Burr, H.S. (1941a). “Field properties of the developing frog’s egg”. Proc, Natl Acad Sci USA 27:276-281.

[18] Burr, H.S. (1947a). “Field theory in biology”. Sci Mon 64:217-225.

[19] Burr, H.S., Musselman, L.K., Barton, D.S., Kelly, N.B. (1937). “A bioelectric record of human ovulation”. Science 86:312.

[20] Brown, F.A., Webb, H.M., Brett, W.J. (1955b). “Magnetic response of an organismand its lunar relationships”. Biol Bull 118:382-392.

[21] Brown, F.A., Scow, K.M. (1978). “Magnetic induction of a circadian cycle in hamsters”. J, Interdiscip Cycle Res 9:137-145.

[22] Becker, R.O. (1960). “Bioelectric field pattern in the salamander and its simulation by an electronic analog”. IRE Trans Med Electron ME-7:202-206.

[23] Barnothy, M.F. (1969). “Biological effects of magnetic fields”. Vol 2. NY: Plenum Press.

[24] Becker. G. (1976). “Reaction of termites to weak alternating magnetic fields”. Naturwissenschaften 63:201-202.

[25] Basset, C.A.L. (1993). “Beneficial effects of electromagnetic fields”. J, Cell Biochem 31:387-393.

[26] Chwirot, W.B., Dygdala, R.S. (1986). “Light transmission of scales overing male inflorescences and leaf buds in Larch during microsporogenesis”. J Plant Physiol 125:79-86.

[27] Cole, F.E., Graf, E.R. (1974). “Precambrian ELF and abiogenesis”. In: Persinger MA, editor. ELF and VLF electromagnetic field effects. New York: Plenum Press.

[28] Friedman, H., Becker, R.O., Bachman, C.H. (1963). "Geomagnetic parameters and psychiatric hospital admissions". Nature, 200:626-628.

[29] Funk, R.H., Monsees, T.K., et al. (2009). "electromagnetic Effects - from cell biology to medicine". Progress in Histochemistry and Cytochemistry 43 (2009) 177-264 .

[30] Gould, J. L. (1984). "Magnetic field sensitivity in animals". Annu Rev Physiol 46:585-598.

[31] Gurwitsch, A. A. (1988). "A historical review of the problem of mitogenetic radiation". Experientia 44:545- 550.

[32] Hotary, K.B., Robinson, K.R. (1991). "The neural-tube of the Xenopus embryo maintains a potential difference across itself". Dev Brain Res 59:65-73.

[33] Jaffe, L.F., Poo. M. M. (1979). "Neurites grow faster toward the cathode than the anode in a steady field". J. Exp, Zool., Vol. 209, pp. 115-128.

[34] Jaffe, L.F., Nuccitelli, R. (1974). "An ultrasensitive vibrating prob for measuring steady extra-cellular currents". J, Cell Biol., Vol,63, pp.115-128.

[35] Jaffe, L. (1981). "The role of ionic currents in establishing developmental pattern". Philos Trans R Soc Lond B 295:553-566.

[36] Levin, M., Thorlin, T., Robinson, K., Nogi, T., Mercola, M. (2002). "Asymmetries in Hp/Kp-ATPase and cell membrane potentials comprise a very early step in left-right patterning". Cell 111:77-89.

[37] Levin, M. (2001). "Isolation and community: The role of gap junctional communication in embryonic patterning". J, Membr Biol 185: 177-192.

[38] Levin, M. (2003). "Bioelectromagnetics in Morphogenesis". J, Bioelectromagnetics 24:295-315.

[39] Lund, E.J. (1921). "Experimental control of organic polarity by the electric current I". J Exp Zool 34:471-494.

[40] Lund, E.J. (1923). "Experimental control of organic polarity by the electric current III". J Exp Zool 37:69-87.

[41] Lund, E. (1947). "Bioelectric fields and growth". Austin: University of Texas Press.

[42] Malin, S.R.C., Srivastava, B.J. (1979). "Correlation between heart attacks and magnetic activity". Nature 277:646-648.

[43] McCaig, C.D. (1986a). "Dynamic aspects of amphibian neurite growth and the effects of an applied electri field". J Physiol 375:55-69.

[44] McCaig, C.D. (1986b). "Electric fields, contact guidance and the direction of nerve growth". J, Embryol Ex Morphol 94:245-255.

[45] McCaig, C.D. (1987). "Spinal neurite reabsorption and regrowth in vitro depend on the polarity of a applied electric field". Development Suppl 100:31-41.

[46] Nuccitelli, R. (1983). "Transcellular ion currents: Signals and effectors of cell polarity". Mod Cell Biol 2:451-481.

[47] Nuccitelli, R., Erickson, C.A. (1983). “Embryonic cell motility can be guided by physiological electric fields”. Exp Cell Res 147: 195-201.

بازتعریف مفهوم شناخت و کارکردهای آن با رویکرد سایبرنتیکی

محمدعلی شکوهیان‌راد[1]

[1]مدرس دانشگاه تهران و پژوهشگر ارشد آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
cm@shokoohian.ir

چکیده

مفهوم شناخت، مفهومی است که به‌واسطه‌ی فراگیری و همه‌گستری اطلاعات، در چند سال اخیر به یکی از پرکاربردترین مفاهیم در ادبیات علمی، نظامی، سیاسی، اقتصادی و حتی فرهنگی و اجتماعی تبدیل شده است؛ خصوصاً از منظر بسترسازی نوع جدیدی از منازعات که به منازعات شناختی (با تعبیر عامیانه‌ی جنگ شناختی) شهرت یافته است. در این بین، آسیب جدی و اثرگذاری که رخ داده است، پرداختن به حوزه‌ی منازعات شناختی بدون توجه به خودِ مفهوم شناخت، سپس دانش شناختی و نهایتاً قدرت برآمده از دانش شناختی است (قدرت شناختی). این خلأ مهم باعث شده است به دلیل عدم توجه به مبانی پایه‌ی مفهومی و نظری، از سویی در حوزه‌های مذکور به سمت تأثیرپذیری از جریان فکری غرب سوق یابیم و از سوی دیگر، دچار اختلافات متعدد در تعریف منازعات شناختی بشویم. همچنین خلأ مذکور باعث شده است تا نسبت‌شناسی میان دانش شناختی و دانش کنترل‌کننده‌ی جریان اطلاعات (دانش سایبرنتیک) که عملاً بسترساز و گسترانندهٔ مفهوم شناخت است، مغفول واقع شود. برای رفع خلأ مذکور، ابتدا مبناشناسی مفهوم شناخت بر اساس عنصر اطلاعات انجام شد و نسبت‌یابی آن با دانش سایبرنتیک به سرانجام رسید، به‌گونه‌ای که مشخص شد دانش شناختی در پاسخ به دو پرسش اساسی سایبرنتیک برای کنترل پدیده‌های مُدرک از طریق جریان اطلاعات کاربرد یافته است. سپس طی چهار گام، تعاریف کارکردی برای مفهوم شناخت، دانش شناختی، قدرت شناختی و نهایتاً منازعات شناختی ارائه گردید به‌طوری که جامع، راهبردی و قابل استفاده در اقدامات عملی باشند.

کلمات کلیدی: سایبرنتیک؛ شناخت، دانش شناختی، منازعات شناختی، جهان‌بینی، اطلاعات.

۱ مقدمه

در روند تولید دانش‌ها، یک زنجیره‌ی فرایندی بسیار مهم مطرح است؛ که با عنوان «سیر مفهوم تا محصول» شناخته می‌شود. منظور از سیر مفهوم تا محصول، این است؛ که برای تعیین کارکرد و کاربردهای عملیاتی هر دانش، ابتدا باید مفهوم‌شناسی آن به درستی انجام شود، سپس بر اساس مفهوم‌شناسی، دانش متناظر با مفاهیم تدوین گردد و در نهایت کارکرد و کاربردهای برگرفته از دانش، به‌عنوان محصولات آن مفهوم اولیه، تشریح شوند.

در چند سال گذشته ، حوزه‌ی شناخت از اهمیت ویژه‌ای برخوردار شده است ؛ که از فرایند فوق مستثنی نیست و برای آنکه کاربردهای مختلف شناخت نظیر منازعات شناختی قابل بحث و بررسی باشد، لازم است ؛ تعریفی جامع، منطبق با واقعیت، کارکردی و راهبردی برای مفهوم شناخت ارائه گردد تا بتوان بر اساس آن، گام‌های بعدی را نیز طی نمود.

این در حالی مهم است ؛ که ادبیات حوزه‌ی شناخت در جمهوری اسلامی ایران، بدون توجه به مفاهیم و تعاریف پایه و بنیادین مورد بحث قرار گرفته است ؛ که در نتیجه‌ی این خلأ بزرگ، از سویی تعدد تعاریف به‌صورتی که بعضاً با یکدیگر متضاد هستند و از سوی دیگر عدم توانمندی اتصال حوزه‌ی نظر به عمل رخ داده است. از این رو برای رفع خلأ مذکور ؛ باید مفهوم شناخت بر اساس مبانی علمی و در راستای کارکردهای حاصل، بازتعریف شود.

۲ پیشینه‌ی پژوهش

در حوزه‌ی شناخت ،ادبیات تولید شده را می‌توان به دو گروه ادبیات خارجی و ادبیات داخلی تقسیم نمود ، بدین صورت که وجه تمایز این تقسیم‌بندی، مدخل مباحث شناختی است؛ به‌گونه‌ای که عموم منابع علمی خارجی (با تمرکز بر زبان انگلیسی) فهم شناخت را از تعریف دانش شناختی آغاز کرده‌اند اما ؛ منابع داخلی به‌صورت مستقیم و بدون پشتوانه‌ی مفهومی - نظری به حوزه‌ی منازعات شناختی و بررسی آن وارد شده‌اند.

۱.۲ اهم منابع خارجی

در بررسی ادبیات تولید شده پیرامون حوزه‌ی شناخت، می‌توان اذعان داشت ؛ که مهم‌ترین مجموعه‌ی علمی در حوزه‌ی دانش شناختی، «انجمن دانش شناختی آمریکا»[1] است، به‌گونه‌ای که خط‌دهی و مدیریت فضای علمی شناختی در سطح بین‌الملل را بر عهده دارد. به استناد وب‌سایت انجمن مذکور «انجمن دانش شناختی، پژوهشگران این حوزه را از سراسر جهان گرد هم می‌آورد که هدف مشترکی آن ها «درک ماهیت ذهن انسان» است (وب‌سایت انجمن دانش شناختی، صفحه‌ی About). از این رو، انجمن دانش شناختی آمریکا، تعریف و هدف دانش شناختی را درک ماهیت ذهن انسان معرفی می‌نماید.

شایان ذکر است که انجمن مذکور، رسالت خود را «ترویج دانش شناختی به عنوان یک رشته و تقویت تبادل علمی بین پژوهشگران ،در زمینه‌های مختلف مطالعاتی از جمله هوش مصنوعی، زبان‌شناسی، انسان‌شناسی، روانشناسی، علوم اعصاب، فلسفه و آموزش» (همان) بیان کرده است؛ که در این راستا، یک کنفرانس سالانه و انتشار مجلات Cognitive Science و TopiCS مورد بحث را ایجاد و پشتیبانی می‌نماید.

دومین مرجع مهم در حوزه‌ی دانش شناخت، دانشگاه استنفورد آمریکا است؛ که یکی از مهم‌ترین مراکز علمی آمریکا و اروپا در حوزه‌ی دانش‌های فلسفی و نظری به‌شمار می‌آید. تعریف دانش شناختی در دانشگاه استنفورد، بدین گونه است که؛ «دانش شناختی، مطالعه‌ی بین رشته‌ای ذهن و هوش است که شامل فلسفه، روانشناسی، هوش مصنوعی، علوم اعصاب، زبان‌شناسی و انسان‌شناسی می‌شود» (دایرةالمعارف

[1] US Cognitive Science Society

فلسفی استنفورد، ۲۰۲۳). همچنین شایان ذکر است ،که دانشنامه‌ی بریتانیکا نیز؛ از تعریف فوق برای هوش مصنوعی استفاده کرده است. (وب‌سایت دانشنامه‌ی بریتانیکا، دانش شناختی)

دپارتمان دانش شناختی دانشگاه جان هاپکینز ،که نقش ویژه‌ای در شبیه‌سازی الگوهای نظری دارد؛ دانش شناختی را چنین تعریف می‌نماید: «دانش شناختی، مطالعه‌ی ذهن و مغز انسان است که بر چگونگی بازنمایی و دستکاری ذهن، دانش و نحوه‌ی تحقق بازنمایی‌ها و فرآیندهای ذهنی در مغز تمرکز دارد. با تصور ذهن به عنوان یک دستگاه محاسباتی انتزاعی که در مغز ساخته شده است، دانشمندان دانش شناختی تلاش می‌کنند تا محاسبات ذهنی زیربنای عملکرد شناختی و نحوه‌ی اجرای این محاسبات توسط بافت عصبی را درک کنند.» (دانشگاه جان هاپکینز، دانش شناختی چیست؟).

دانشگاه پنسیلوانیا نیز ،دانش شناختی را «منعکس‌کننده‌ی پیشرفت طبیعی روش علمی که موفقیت فوق‌العاده‌ای در علوم طبیعی و کاربرد آن در ذهن پیدا کرده است» می‌داند. در ادامه‌ی تعریف فوق ذکر شده «دانش مدرن بر این تعهد بنا شده است که جهان دارای مبنایی مکانیکی است که می‌توان آن را چنین فهمید» (دانشگاه پنسیلوانیا، دانش شناختی چیست؟).

از بررسی آرا و نظرات پژوهشگران نیز تعاریف مشابهی به‌دست می‌آید،برای نمونه؛ دانش شناخت از منظر اوبِرلَندر –یکی از نویسندگان کتاب مروری بر دانش شناختی– اینچنین تعریف شده است: «دانش شناختی، مطالعه علمی بین رشته‌ای ذهن است. بنابراین بسیاری از سؤالات در محدوده‌ی آن قرار می‌گیرند. به عنوان مثال؛ مردم چگونه جهان را از طریق حواس خود درک می‌کنند؟ آن چگونه موفق می‌شوند در یک دنیای در حال تغییر به موقع عمل کنند؟ چگونه مشکلات جدید را حل می‌کنند؟ چگونه آنها موفق به یادگیری مهارت‌های جدید می‌شوند؟ و چگونه یکدیگر را درک می‌کنند؟» (اوبرلندر، ۲۰۰۶). چاتِر نیز اعتقاد دارد: «دانش شناختی، از جمله دانش شناختی پردازش زبان، بر توصیف بازنمایی‌ها و فرآیندهای دخیل در رفتار شناختی تمرکز کرده است» (چاتر، ۲۰۰۶).

دِرِک ریم و آیزاک تورگِمان نیز تعریف مشابهی را بیان کرده‌اند، چنانکه «دانش شناختی، یک حوزه‌ی میان رشته‌ای است که بر معماری انتزاعی ذهن و نحوه‌ی پردازش اطلاعات، به ویژه نحوه‌ی عملکرد مغز با توجه به احساسات، توجه و آگاهی، زبان، ادراک، یادگیری و حافظه و عملکرد اجرایی تمرکز دارد» (ریم و تورگمان، ۲۰۲۰).

۲.۲ اهم منابع داخلی

در آثار و تألیفات پژوهشگران داخلی، منابع متعددی وجود دارد ؛ که حوزه‌ی شناخت را به‌طور مستقیم از منازعات شناختی آغاز به بررسی کرده و کمتر به مبانی مفهومی و نظری توجه شده است. برای نمونه، در کتاب «جنگ شناختی، حمله به واقعیت و اندیشه» مبحث فوق چنین بیان شده است: «این جنگ، یک استراتژی است که بر تغییر نحوه‌ی تفکر مردمِ هدف و نحوه‌ی پیاده‌سازی آن تمرکز دارد. با وجود ابهامات ماهیتی در این تعریف، یک چهارچوب مناسب نسبت به گذشته برای بررسی بیشتر جنگ شناختی در آن دیده می‌شود؛ که می‌تواند اثرگذاری مفاهیم آن را نسبت به گذشته نشان دهد» (برنال، ترجمه‌ی قربانی زواره، ۱۴۰۱، ص ۲۳).

اثر مذکور پس از توضیحات فوق، در نهایت جنگ شناختی و کارکرد آن را این گونه توصیف می‌کند: «جنگ شناختی؛ سلاح‌سازی افکار عمومی توسط یک نهاد خارجی می باشد، که به منظور تأثیرگذاری بر سیاست عمومی، حاکمیت یا بی‌ثباتی در اقدامات و یا ساختار نهادهای دولتی به‌کار گرفته می‌شود» (برنال، ترجمه‌ی قربانی زواره، ۱۴۰۱، ص ۲۴).

محمد جوانی –از پژوهشگران حوزه‌ی جنگ شناختی– در ابتدای کتاب خود برای توصیف دانش شناختی بیان کرده است: «علوم شناختی، دانشی است میان‌رشته‌ای، نوین، پویا و معطوف به آینده که در آن، مغز و فرایندها و کارکردهای آن مورد مطالعه‌ی روشمند و منظم علمی قرار می‌گیرد» (جوانی، ۱۴۰۱، ص ۱۰).

همانطور که ملاحظه می‌شود، تعریف فوق از حیث قرابت و الگوبرداری نسبت به موضوع دانش شناختی، کاملاً منطبق با تعاریفی که از سوی چندین دانشگاه آمریکا ارائه شده می باشد. این تلاش هرچند برای ورود به لایه‌ی علمی مهم است ، اما در نهایت باعث می‌شود منازعات شناختی را نیز آنگونه برداشت کنیم که مدنظر و مورد تأیید غرب است. این در حالی است که احتمالاً با ارائه‌ی یک تعریف بومی بر اساس مبانی اسلامی - ایرانی، می‌توان نوع متفاوت و بومی شده‌ای از منازعات شناختی را تدوین نمود.

کتاب تألیفی سید حسین محمدی نجم، از معدود آثاری است؛ که در حوزه‌ی دانش شناختی، تلاش نموده ابتدا فضای علمی را ترسیم و تعریف نماید و سپس بر اساس آن، منازعات شناختی را تحلیل کند. وی در اثر خود بیان کرده است: «ایده‌ها و فناوری‌های نوظهور نظامی که منبعث از تغییر یا تکمیل پارادایم‌های علمی در هر مقطع مفروض زمانی به میدان جنگ پا گذاشته‌اند، ابعاد جدیدی به فضای رزم افزوده و در نتیجه شیوه‌های رزم آن روزگار را دگرگون کرده‌اند. بنابر این **نقش پارادایم علمی حاکم** بر هر روزگار بر شیوه‌ی جنگیدن آن بسیار تأثیرگذار است» (محمدی نجم، ۱۳۹۳، ص ۴۸).

همچنین وی، منازعات شناختی را بعد پنجم جنگ دانسته و در این خصوص گفته است «بعد پنجم جنگ، فضایی است مجازی، سیال، نرم‌افزاری و خارج از حواس انسان که به استعاره می‌توان آن را ذهن نامید» (محمدی نجم، ۱۳۹۳، ص ۴۹).

اما یکی از مهم‌ترین مطالب محمدی نجم در کتاب مذکور، اشاره به بستر فنی‌ای است؛ که بروز و ظهور منازعات شناختی بدون وجود آن امکان‌پذیر نیست. محمدی نجم اشاره می‌کند «شکوفایی فناوری اطلاعات و رایانه و برتری مطلق کشورهای توسعه یافته‌ی غربی در این حیطه، سبب ایجاد الگویی برای توسعه‌ی شناخت فنی گردیده است که جریان آزاد اطلاعات، سوخت و انرژی محرک این شناخت به‌حساب می‌آید» (محمدی نجم، ۱۳۹۳، ص ۴۹).

در آخر محمدی نجم به تعریف مفهوم شناخت نیز ورود کرده و بیان می‌دارد «شناخت، فعالیتی است که مستلزم خودزایی و خودجاودانه‌سازی شبکه‌های زنده است. به بیان دیگر، **شناخت همان فرایند حیات است**» (محمدی نجم، ۱۳۹۳، ص ۷۵).

۳ ادبیات پژوهش

۱.۳ آسیب‌شناسی ادبیات رایج کشور در حوزه‌ی شناخت

همواره هر منازعه بر اساس قدرت طرفین آن منازعه شکل می‌پذیرد؛ لذا منازعات شناختی ریشه در قدرت شناختی دارد. همچنین ابزار اصلی تولید قدرت، دانش‌های اقتدارآفرین هستند ؛ از این رو دانش شناختی باید تدوین گردد. در ضمن بدیهی است که هر دانش، ابتناء بر مفاهیمی دارد که قلب آن دانش را تشکیل میدهند؛ بنابراین برای آنکه بتوان در خصوص منازعات شناختی به‌درستی اظهار نظر علمی نمود، لازم است فرایند مفهوم تا محصول در چهار گام ذیل طی شود:

۱. **تبیین مفهوم شناخت:** هر مفهوم باید به دقت و به‌صورت جامع و کارکردی تبیین گردد.

۲. **تدوین دانش شناختی:** برای ایجاد یک متن مدوّن که ارتباط مفهوم شناخت را با سایر مفاهیم و همچنین با محیط بیرونی مشخص سازد، دانش شناختی باید تدوین شود.

۳. **تعریف قدرت شناختی:** قدرت شناختی که برگرفته از دانش شناختی است، بر اساس ساز و کار دانش بنیادین خود نیازمند تعریف دقیق است.

۴. **تنظیم منازعات شناختی:** در نهایت باید مشخص شود اگر بازیگران مجهز به قدرت شناختی با یکدیگر درگیر شوند، منازعات شناختی دقیقاً چه آثار و وضعیتی را در پی خواهند داشت و چگونه محیط را با خود هماهنگ و تنظیم خواهند نمود.

اما علی‌رغم وضوح و شفافیت روند فوق، از زمانی که مباحث مرتبط با حوزه‌ی شناخت در کشور مطرح گردیده است؛ بنیان و نقطه‌ی تمرکز عموم افراد بر حیطه‌ی منازعات شناختی –با تعبیر عمومی جنگ شناختی– قرار گرفت. لذا سه گام مهم ماقبل از منازعات شناختی، در عموم منابع جنگ شناختی اصلاً دیده نشده است و در برخی از منابع که اشاراتی به آن داشته‌اند، به‌صورت موجز بوده و تمامی چهار گام مذکور را در بر نگرفته است. بر این اساس مادامی که نقص و اشکال فوق مرتفع نگردد، نمی‌توان به‌هم‌ریختگی ادبیات حوزه‌ی شناخت را منظم و یکپارچه نمود.

۲.۳ فرایند شناخت، از مفهوم تا محصول

برای آنکه شناخت به‌درستی معرفی شود، لازم است مبانی شناخت و ایجاد آن در پدیده‌های مُدرک مشخص و استنباط گردد؛ به‌عبارت دیگر مادامی که شناختِ شناخت محقق نشود، برای سایر عرصه‌های وابسته به شناخت نمی‌توان نظر جامع و مدوّنی ارائه نمود.

زمانی که درباره‌ی اصل و ماهیت مفهوم شناخت صحبت می‌شود، باید در نظر داشت که شناخت چه کارکردی را در پدیده‌های مُدرک به‌دنبال دارد. شناخت در عمیق‌ترین سطح اثرگذاری خود، نگاه پدیده‌های مُدرک به جهان را تعیین می‌کند. از این رو در گام نخست، مفهوم شناخت به‌عنوان عامل شکل‌گیری جهان‌بینی پدیده‌های مُدرک تبیین می‌شود.

حال باید در نظر گرفت که خود شناخت از چه طریقی به پدیده‌های مُدرک القاء می‌شود؟ به‌عبارت دیگر برای آنکه بخواهیم جهان‌بینی یک موجود مُدرک را آنگونه که مدنظر است شکل دهیم، چه کاری باید انجام دهیم یا چه چیزی را باید به وی ارائه کنیم؟

شناخت بر مبنای اطلاعاتی که به پدیدهی مُدرک داده می‌شود، شکل می‌گیرد. از این رو **پایه‌ی شناخت و جوهره‌ی فهم، اطلاعات است**. به همین دلیل است که برای ایجاد انحراف در شناخت، از عملیات‌های اطلاعاتی سه‌گانه شامل «قطع جریان اطلاعات»[۲]، «تحریف اطلاعات»[۳] و «بمباران اطلاعاتی»[۴] استفاده می‌شود. لذا مادامی که شناخت صحیحی از مفهوم و کارکرد اطلاعات و جریان‌مندی اطلاعات حاصل نشود، شناخت صحیح و ساز و کار شناخت نیز به سرانجام نخواهد رسید. از سوی دیگر، دانشی که جریان اطلاعات را توصیف و کنترل می‌نماید، دانش سایبرنتیک است. به‌همین سبب باید بر دانش سایبرنتیک تسلط یافت تا بتوان بر اطلاعات نیز مسلط شد.

۳.۳ سایبرنتیک، دانش کنترل بر مبنای اطلاعات

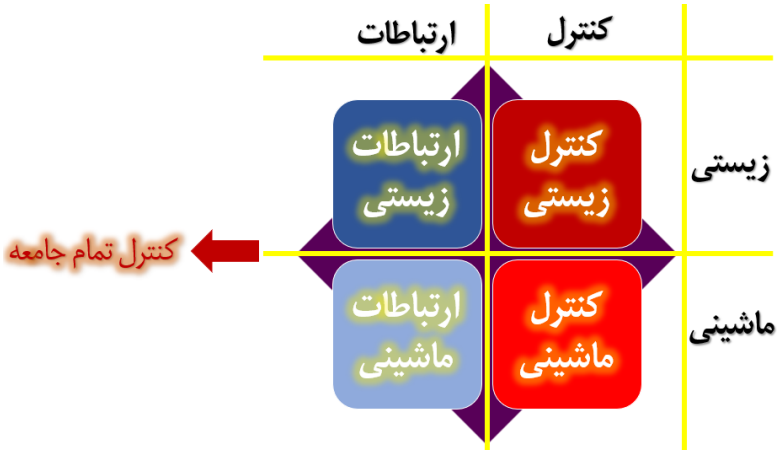
نوربرت وینر در سال ۱۹۴۸ میلادی برای اولین بار به زبان انگلیسی در کتابی با عنوان «سایبرنتیک: یا کنترل و ارتباط در حیوان و ماشین»[۵] واژه‌ی سایبرنتیک را به‌کار برد.

وینر در خصوص انتخاب واژه‌ی سایبرنتیک چنین بیان می‌دارد: «تا دوران اخیر، واژه‌ای که مبیّن این گروه از افکار [منظور، کنترل پدیده‌های مُدرک از طریق جریان اطلاعات و محتوای ارسالی به آنها] باشد، وجود نداشت و برای برگرفتن این حوزه‌ی افکار به تمامی در یک اصطلاح، مجبور به اختراع واژه‌ای مخصوص شدم. لذا سایبرنتیک را به‌معنای سکاندار و از منشأ انگلیسی Governor انتخاب کردم» (وینر، ۱۳۶۶، ص۱). وی در تعریف این واژه گفته است: «تصمیم ما بر این است که کلیات مطالعات نظری کنترل و ارتباطات در ماشین و موجودات زنده را سایبرنتیک بنامیم» (شکوهیان‌راد، ۱۳۹۷، ص ۵۹).

بنابر تعریف وینر –که پدر دانش سایبرنتیک است– دانش سایبرنتیک از سمتی هم بر کنترل هر پدیده در جای خود تمرکز دارد و از سمتی دیگر ارتباطات پدیده‌ها با یکدیگر را کنترل می‌نماید. این یعنی اعمال کنترل هم در سطح فردی است و هم در سطح اجتماعی. همچنین کنترل فردی و اجتماعی، هم نسبت به موجودات زیستی انجام می‌شود و هم پدیده‌های مُدرک غیرزیستی. از تلفیق و ضرب ماتریسی گزاره‌های فوق، چنان نتیجه می‌شود که سایبرنتیک، کنترل تمام جامعه را مدنظر قرار داده است (شکل ۱).

بر اساس ماتریس فوق، در یک جمله می‌توان سایبرنتیک را **دانش کنترل تمامی پدیده‌های مُدرک در سطوح فردی و اجتماعی از طریق کنترل جریان اطلاعات** تعریف نمود. نکته‌ی بسیار مهم آن است که دانش سایبرنتیک، هر مؤلفه‌ای را که بتواند از طریق جریان اطلاعات تحت تأثیر قرار دهد، به‌عنوان متغیر کنترل مصادره نموده و از طریق آن، سایر پدیده‌ها و اجزای وابسته را کنترل می‌نماید؛ که شناخت یکی از اهم

[2] Disinformation
[3] Misinformation
[4] Massinformation
[5] Cybernetics: Or Control and Communication in the Animal and the Machine



شکل ۱: کنترل تمام جامعه

متغیرهای کنترلی است. از این رو شناخت؛ در نسبت با دانش سایبرنتیک قابل استنباط است.

۴.۳ نسبت‌شناسی شناخت و سایبرنتیک

تعریفی که برای دانش سایبرنتیک بیان شد، کاملاً منطقی و پذیرفته است ودر دهه‌های گذشته به‌صورت عملیاتی در سراسر جهان مورد استفاده قرار گرفته است. اما باید توجه داشت ؛که وقتی صحبت از کنترل پدیده‌ی مُدرک از طریق جریان اطلاعات می‌شود تا در نهایت اقدام وی به‌سمتی سوق یابد که مدنظر کنترل‌کننده می باشد و در نهایت پاسخ به دو پرسش، حیاتی است:

- موجود مُدرک مفروض، دقیقاً به کدام منابع اطلاعاتی اعتماد و دسترسی دارد؟
- موجود مُدرک مفروض، در نسبت با اطلاعات چگونه تفکر و تحلیل می‌کند؟ به‌عبارت دیگر الگوریتم‌های محاسبات ذهنی وی چگونه است؟

پرسش نخست، از این جنبه مهم است؛ که اطلاعات را باید از طریقی به موجود مُدرک ارائه کرد که اولاً در دسترس‌اش باشد و ثانیاً مورد پذیرش قرار بگیرد.

اما اهمیت پرسش دوم از آنجا است؛ که برای آنکه در رابطه‌ی «ورودی، پردازش، خروجی» دریافت یک خروجی مطلوب میسّر شود، باید بدانیم پردازش چگونه انجام می‌شود تا در نسبت با آن، ورودی را به‌گونه‌ای ارائه کنیم که پس از انجام پردازش مشخص، به خروجی مطلوب بینجامد. برای مثال اگر دو تابع f و g بدین صورت در نظر گرفته شوند که تابع $f(x) = x + ۳$ و $g(x) = ۲x$، آنگاه برای آنکه از هر دو تابع، عدد ۱۰ را به‌عنوان خروجی دریافت کنیم، باید ورودی‌هایی ارائه کنیم که پس از پردازش در الگوریتم محاسباتی تابع به خروجی مطلوب تبدیل شود. بنابر این ورودی تابع f و g به ترتیب معادل ۷ و ۵ است. همانند همین مثال برای تمامی پدیده‌های مُدرک وجود دارد و باید در نظر داشت برای دریافت خروجی مطلوب از حیث شناختی،

شکل ۲: اطلاعات، شناخت، جهان‌بینی

ورودی‌ای باید به آن ارائه شود که پس از پردازش توسط دستگاه محاسبات ذهنی به خروجی مطلوب تبدیل گردد. از این رو باید الگوریتم محاسبات ذهنی هر پدیده‌ی مُدرک را به درستی شناخت.

دو پرسش فوق که در عملیاتی‌سازی دانش سایبرنتیک ، از سوی دانشمندان این حوزه مطرح می‌شود؛ توسط دانش شناختی به پاسخ می‌رسد. بر این اساس **دانش شناختی، مکمل اقدامات دانش سایبرنتیک نسبت به پدیده‌های مُدرک در بُعد شناخت آنها** است (شکل ۲). علت اصلی آشفتگی نظرات و برداشت‌ها نسبت به حوزه‌ی دانش شناختی در کشور نیز غفلت از دانش سایبرنتیک و جایگاه بنیادین آن برای دانش شناختی است.

اکنون که پایه و مبنای شناخت و دانش شناختی مشخص گردید، می‌توان چهار گام مفهوم تا محصول را طی نموده و برای هر کدام، تعریف مشخصی که جنبه‌ی کارکردی داشته باشد ارائه نمود.

۱.۴.۳ گام یکم: تبیین مفهوم شناخت

شناخت به معنای شکل‌گیری جهان‌بینی پدیده‌ی مُدرک است. از این رو صحبت از شناخت به‌طور عام، به معنای صحبت از کل جهان‌بینی پدیده‌ی مُدرک است.

بر اساس همین تعریف از شناخت، بخشی از اختلاف نظرات جاری در کشور رفع می‌گردد؛ برای نمونه یکی از حوزه‌هایی که تقاضای پژوهش برای آن چشمگیر است، شناسایی و معرفی تکنولوژی‌های شناختی است، زیرا تصور بر این است که تکنولوژی‌ها به دو گروه شناختی و غیرشناختی تقسیم می‌شوند. این در حالی است که شناخت، یک نگاه نوینی است که به تمام جهان صورت می‌گیرد و از منظر شناخت، هر تکنولوژی و ابزاری، یک وجه شناختی دارد که سابق بر این مورد توجه قرار نگرفته بود. به‌عبارت دیگر هر چیزی که توان اثرگذاری بر جهان‌بینی را داشته باشد، جنبه‌ی شناختی دارد؛ خواه یک شئ کوچک باستانی باشد، یا الگویی خاص از پوشش، بازی، آموزش و ... . لذا شناخت، به مثابه عینکی است؛ که نوع بینش به جهان را ارتقاء می‌دهد، نه اینکه بخشی از همین دیدگاه فعلی را به پدیده‌ها و تکنولوژی‌های شناختی متمایز سازد.

۲.۴.۳ گام دوم: تدوین دانش شناختی

بر اساس تعریفی که برای تبیین مفهوم شناخت ارائه شد ؛ در گام دوم **دانش شناختی «دانش شکل دادن به جهان‌بینی پدیده‌های مُدرک به‌صورت مدنظر»** تعریف می‌شود. بنابر این دانش شناختی، دانشی است که باید الگوها، روش‌ها، فرایندها، ملزومات، بایدها و نبایدها، قواعد و اصول و سایر هرآنچه که صورت‌دهی به جهان‌بینی پدیده‌های مُدرک به آن نیازمند است را ،در خود داشته باشد. دقیقاً به همین دلیل است که ذیل دانش شناخت، مطالعات میان‌رشته‌ای متشکل از دانش‌های عصب‌شناسی، انسان‌شناسی، روانشناسی، زبان‌شناسی، ریاضیات، فلسفه، هنر و ... تعریف می‌شود ؛زیرا بخشی از فهم چگونگی کارکرد ادراک در پدیده‌های مُدرک از طریق تسلط بر دانش‌های مذکور میسر می‌شود. اما بدین معنا نیست ؛که دانش شناختی متشکل از رشته‌های مذکور است، بلکه این دانش، یک دانش واحد با قواعد مشخص است که برای حصول اهداف خود با دیگر دانش‌ها در تعامل است.

لذا بر این اساس از میان تمامی تعاریف مطرح شده؛ تنها تعریف دقیق و صحیح متعلق به انجمن دانش شناختی آمریکا است، که تأکید دارد «دانش شناختی به‌عنوان یک رشته‌ی علمی ...» مورد مطالعه است.در حالی که دیگر تعاریف خارجی و داخلی، دانش شناخت را به‌طور مستقیم حاصل تلفیقی از مطالعات میان‌رشته‌ای معرفی کرده‌اند. بر اساس چنین دیدگاه هایی، دانش شناخت دارای هویت مستقل نبوده و صرفاً فضایی است ،که از همپوشانی دیگر رشته‌های مؤثر بر ادراک انسان شکل گرفته است؛ نگاهی که طبق تعریف ارائه شده برای دانش شناختی و نسبت‌شناسی آن با دانش سایبرنتیک، مردود است.

۳.۴.۳ گام سوم: قدرت شناختی

یکی از مهم‌ترین شاخص‌های تعیین قدرت‌آفرین بودن یک دانش، این است؛ که تسلط بر آن دانش بتواند امکان سلطه و کنترل را ارائه نماید. لذا از آنجا که دانش شناختی امکان کنترل جهان‌بینی پدیده‌های مُدرک را میسر می‌سازد، یک دانش قدرت‌آفرین است که قدرت شناختی را عرضه می‌کند. به‌طور کل، **قدرت شناختی به‌معنای توان تحمیل جهان‌بینی مدنظر خود بر دیگران** است.

باید در نظر داشت که قدرت شناختی، به‌معنای توانمندی کنترل پدیده‌های مُدرک در عمیق‌ترین لایه‌ی وجودی آنها است. از این رو بسیار مهم است که برای کنترل شناخت، از چه مبانی، روش‌ها و ساز و کارهایی استفاده می‌شود؛ زیرا بخش چشمگیری از مبانی و روش‌های شناختی که غرب برای سلطه بر شناخت انسان به‌کار گرفته است، از حیث انطباق با مبانی الگوی اسلامی - ایرانی مردود است، فارغ از اینکه امکان مصادره به مطلوب آنها وجود دارد یا به‌صورت مطلق نفی میشود.

۴.۴.۳ گام چهارم: منازعات شناخت

به‌تبع تعریفی که برای قدرت شناختی ارائه شد ، بدین شرح است که ؛ منازعات شناختی به‌معنای درگیری دو سویه یا چند سویه میان بازیگرانی است ، که اولاً همگی به قدرت شناختی مجهز هستند و ثانیاً منافع آن برضد یکدیگر تعریف شده است و هر یک از آنها در تلاش است تا از سویی جهان‌بینی خود را ، دیگر بازیگران میدان منازعات شناختی تحمیل کند و از سوی دیگر مراقبت نماید تا جهان‌بینی دیگر بازیگران بر خودش

اثرگذار نشود.

۴ نتیجه‌گیری

بر اساس تطابیق و تعاریف ارائه شده، مشخص می‌شود که حوزه‌ی شناخت؛ از آنجا که اساساً جهان‌بینی مدنظر را به دیگران القاء می‌کند، به طور کامل از ارزش‌گذاری بر مبنای ایدئولوژی برخوردار است و نباید به‌عنوان یک دانش خنثی تلقی شود. از این رو توجه به چهار نکته‌ی مهم، ضرورت بسیار دارد:

۱. شکل‌گیری منازعات در لایه‌ی شناختی ؛ به معنای درگیر شدن باطل با جبهه‌ی حق در عمیق‌ترین لایه‌ی وجودی انسان است. از این رو؛ پایان منازعات شناختی به‌معنای روشن شدن تمدن آینده و سرنوشت جهان است.

۲. در حیطه‌ی منازعات شناختی باید بر اساس اصول، مبانی و فقه دین مبین اسلام عمل کرده و از ابتلا به روش‌ها و ساز و کارهای غیر شرعی و غیر اخلاقی غرب حذر شود.

۳. نقطه‌ی اصلی جهان‌بینی در مطالعات شناختی برای جهان اسلام، تعمیق و گسترش امام‌شناسی است ،که هر چه بهتر انجام شود؛ پدافند قدرتمندتری در مقابل حملات شناختی جبهه‌ی باطل ایجاد می‌کند. در این خصوص، مطالعه‌ی دو کتاب «ولایت‌فقیه» امام خمینی(ره) و «طرح کلی اندیشه اسلامی در قرآن» امام خامنه‌ای بسیار راهگشا است.

۴. از آنجا که در میدان منازعات شناختی، سرنوشت هر بازیگر به تصمیم و اقدام دیگر بازیگران وابسته است، لذا منازعات شناختی از جنس منازعات استراتژیک است. لذا می‌توان از اصول، قواعد و روش‌های بازی‌های استراتژیک –مانند نظریه‌ی بازی– برای طراحی و پیش‌بینی بخشی از منازعات شناختی بهره جست.

در نهایت، توجه به اهمیت این مسئله از سوی پژوهشگران حوزه‌ی مطالعات شناختی ، بسیار ضروری است ؛که در هر مرحله از مطالعات، به تفکیک اصول، مبانی، روش‌ها و راهبردها بر اساس بنیان‌های دینی و شریعت متعالی اسلامی توجه داشته باشند تا اهداف منازعات شناختی جبهه‌ی باطل، حتی در حد موجز نیز به وقوع نپیوندد.

مراجع

[۱] نوربرت وینر، «استفاده‌ی انسانی از انسان‌ها»، ترجمه‌ی مهرداد ارجمند، تهران، سازمان انتشارات و آموزش انقلاب اسلامی، ۱۳۶۶، صفحه‌ی ۳۰.

[۲] آلونسو برنال، «جنگ شناختی، حمله به واقعیت و اندیشه»، مترجم: محمد حسین قربانی زواره، انتشارات شناخت‌پژوه، ۱۴۰۱، قم.

[۳] محمد جوانی، «علوم شناختی در جنگ شناختی»، نشر نواندیشان، ۱۴۰۱، تهران.

[۴] سید حسین محمدی نجم، «جنگ شناختی، بعد پنجم جنگ»، مؤسسه‌ی آموزشی و تحقیقاتی صنایع دفاعی، ۱۳۹۳، تهران.

[۵] محمد علی شکوهیان‌راد، «نظریه‌ی جنگ در عصر سیستم‌های فرماندهی و کنترل»، انتشارات مؤسسه‌ی آموزشی و پژوهشی شهید سپهبد صیاد شیرازی، ۱۳۹۷، تهران.

[6] Britannica, Science & Tech, Cognitive Science Definition, Link: https://www.britannica.com/science/cognitive-science

[7] Johns Hopkins, Department of Cognitive Science, “What Is Cognitive Science?”, Link: https://cogsci.jhu.edu/about/

[8] Cognitive Science at PENN, How minds work?, “What is Cognitive Science?”, Link: https://web.sas.upenn.edu/cogsci/what-is-cognitive-science/

[9] J. Oberlander, “Cognitive Science: Overview” Encyclopedia of Language & Linguistics, (Second Edition), 2006.

[10] N. Chater, “Rational Analysis and Language Processing”, Encyclopedia of Language & Linguistics, (Second Edition), 2006.

[11] Derek Ream & Isaac Tourgeman, “Encyclopedia of Evolutionary Psychological Science”, Springer, Year 2020, pp 1177–1183.

[12] US Cognitive Science Society, About Page, Link: https://cognitivesciencesociety.org/about/

[13] Stanford Encyclopedia of Philosophy, Cognitive Science, Jan 31, 2023, Link: https://plato.stanford.edu/entries/cognitive-science/

تغییرات اقلیمی، ابر پروژه‌ای برای کنترل جهان

عاطفه نصیری [۱]

[۱] کارشناس ارشد مهندسی منابع طبیعی، دانشگاه آزاد اسلامی، واحد تهران شمال
nasiry.atefeh@gmail.com

چکیده

سابقه‌ی طرح مفهوم تغییرات اقلیمی، به دو قرن پیش باز می‌گردد، هرچند که عبارت خاص «تغییرات اقلیمی» از ۱۹۷۵ وارد ادبیات علمی شد. علت تغییرات اقلیمی، به انباشت گازهای گلخانه‌ای و به خصوص CO2 و عنصر کربن نسبت داده می‌شود. مروری پیش‌بینی‌های اسبق درباره‌ی تغییرات اقلیمی و گرمایش زمین، حاکی از آن است که عمده‌ی آنها، هرگز محقق نشدند. آیا نظریه‌ها و پیش‌بینی‌های امروزی تغییرات اقلیمی و آینده‌ی آب و هوایی زمین هم به سرنوشت پیش‌بینی‌های پیشین، دچار خواهند شد؟ برای کنترل همه جا، باید از عاملی استفاده کرد که در همه جا حضور داشته باشد و جهان شمول باشد. همچنین باید در نظر داشت که اساس تغییرات آب و هوایی بر مواردی است که برای مردم، قابل اندازه‌گیری نیست. از سوی دیگر، برخورد درست با پدیده‌های اقلیمی و محیط زیستی، منوط به داشتن داده‌های درست است. هرگونه داده‌پردازی یا ارائه‌ی داده‌های نادرست، سبب واکنش‌های نادرست شده، که خود می‌تواند عامل بحران اقلیمی و زیست محیطی باشد، بدون آن‌که در اصل و در واقعیت، بحرانی وجود داشته باشد. به نظر می‌رسد که هدف تمامی این موارد –که نظریه‌های علمی پشتیبان‌شان، تاکنون به اثبات دقیق نرسیده‌اند– کنترل نمودن جریان اقتصاد و انرژی کشورها و ملت‌ها، به بهانه‌ی تغییرات اقلیمی است.

کلمات کلیدی: تغییرات اقلیمی، کنترل، جهان، گازهای گلخانه‌ای، کربن، سایبرنتیک، ۱کوسایبرنتیک، اطلاعات.

۱ مقدمه

تغییرات اقلیمی چیست؟ مطابق تعاریف مجامع علمی حال حاضر دنیا، تغییرات اقلیمی، عمدتاً حاصل گازهای گلخانه‌ای و به خصوص CO_2 است. تغییرات اقلیمی، به جنبه های عملی و نظری تغییرات آب‌وهوای جهانی در دوره‌های مختلف زمین شناسی می‌پردازد. بررسی تغییرات اقلیم، به مسائل کل‌نگر مربوط به تغییرات آب‌وهوا و سهم‌شان در افزایش دما، با تأثیرات متعدد بر فرآیندهای طبیعی می‌پردازد (سروشی سینگ و همکاران، ۲۰۲۱). تغییرات اقلیمی جهانی، به‌خاطر انباشت گازهای گلخانه‌ای (CO_2، متان، CFCها و غیره) رخ می‌دهد که منجر به افزایش اثر گلخانه‌ای طبیعی – که عامل حفظ دمای زمین است – می‌شود

(روبین مارجوری لوکاس و پیتر گیس، ۲۰۱۱).

در این مقاله، تلاش شده تا با بررسی حقیقت داشتن/ نداشتن مسئله‌ی تغییرات اقلیم، به هدف نهفته در پسِ مطرح شدن وسیع و گسترده‌ی این موضوع، پرداخته شود.

۲ پیشینه‌ی پژوهش

نخستین بار، اصطلاح خاص «تغییرات اقلیمی»، در مقاله‌ای که به قلم والاس اس بروکر [۱] در مجله‌ی ساینس [۲] منتشر شد، مورد استفاده قرار گرفت (۱۹۷۵). عنوان مقاله‌ی بروکر این بود: «تغییرات اقلیمی: آیا ما در آستانه‌ی یک گرمایش جهانی قرار داریم؟» وی در مقاله‌ی خود عنوان نموده که افزایش تصاعدی CO_2 سبب افزایش میانگین دمای زمین، در اوایل قرن آینده خواهد شد.

به نظر می‌رسد که سابقه‌ی مطرح شدن این موضوع، بیش از این‌ها باشد. پیش‌تر، جوزف فوریه [۳]، در مقاله‌ای که در ۱۸۱۸ منتشر نمود، حدس زد که در طی یک دوره‌ی زمانی طولانی، مقدار گرمای موجود در اتمسفر می‌تواند تغییر کند – هم به واسطه‌ی تکامل طبیعی زمین و هم فعالیت‌های انسانی– وی پیش‌بینی کرد: استقرار و پیشرفت جامعه‌ی بشری و عملکرد قدرت‌های طبیعت، می‌تواند سبب تغییرات قابل‌توجهی در وضعیت سطح، توزیع آب‌ها و حرکت‌های عظیم هوا در سطح وسیعی از مناطق شود. چنین اثراتی در طی چند قرن، باید تغییراتی را در دمای میانگین این نواحی ایجاد کند» (کلایو تامپسون، ۲۰۱۹).

در ۱۸۹۶، سوانته آرنیوس [۴]، فیزیکدان سوئدی، اولین مدل تغییر آب‌وهوا را ایجاد کرد. او پیش‌بینی کرد که اگر مقدار CO_2 موجود در جو دوبرابر شود، دمای جهان، به میزان ۵ تا ۶ درجه سانتی‌گراد افزایش می‌یابد (ایزابل هیلتون، ۲۰۰۸).

۳ مفهوم‌شناسی

در این قسمت مروری بر پیش‌بینی‌هایی صورت می‌گیرد که پیش‌تر درخصوص تغییرات اقلیمی و گرمایش زمین صورت گرفتند.

برخی دانشمندان، به مناسبت اولین اعلام روز زمین در ۱۹۷۰، پیش‌بینی‌هایی در خصوص آینده‌ی اقلیم، زمین، محیط زیست و جمعیت داشتند که در ذیل به برخی از آنها، اشاره می‌شود:

الف) پل ارلیش [۵] با اطمینان در آوریل ۱۹۷۰ اعلام کرد: «افزایش جمعیت قطعاً از افزایش ذخایر غذایی ما پیشی خواهد گرفت و نرخ مرگ و میر افزایش خواهد یافت، به نحوی که حداقل ۱۰۰ تا ۲۰۰ میلیون نفر در سال در طول ده سال آینده [تا سال ۱۹۸۰] از گرسنگی خواهند مرد». وی هشداردهنده‌ترین سناریوی

[1] Wallace S. Brocker
[2] Science
[3] Joseph Fourier
[4] Svante Arrhenius
[5] Paul Ehrlich

خود را برای شماره‌ی ویژه‌ی روز زمین مجله‌ی «پروگرسیو[۶]» (۱۹۷۰) ترسیم کرد و به خوانندگان اطمینان داد که بین سال‌های ۱۹۸۰ تا ۱۹۸۹، حدود ۴ میلیارد نفر، از جمله ۶۵ میلیون آمریکایی، در «مرگ بزرگ» از بین خواهند رفت.

ب) در ژانویه ۱۹۷۰، «لایف[۷]» گزارش داد: «دانشمندان، شواهد تجربی و نظری محکمی برای حمایت از پیش‌بینی‌های زیر دارند: اینکه ظرف یک دهه، ساکنان شهرها مجبور خواهند بود برای زنده ماندن از آلودگی هوا، از ماسک‌های گاز استفاده کنند ... تا سال ۱۹۸۵ آلودگی هوا آنقدر زیاد خواهد شد که تنها نیمی از نور خورشید به زمین خواهد رسید».

ج) کنت وات[۸]، بوم شناس (اکولوژیست)، در مصاحبه‌ای با تایمز[۹] گفت: «با ادامه‌ی روند کنونی، ما از نفت خام با چنان سرعتی استفاده خواهیم کرد که تا سال ۲۰۰۰، دیگر نفت خامی وجود نخواهد داشت».

د) هریسون براون[۱۰]، دانشمند آکادمی ملی علوم، نموداری را در مجله‌ی «ساینتیفیک آمریکن[۱۱]» منتشر کرد که در خصوص ذخایر فلزی بود و مطابق آن، تخمین زد که ظرف مدت کوتاهی پس از سال ۲۰۰۰، منابع مس به طور کامل تمام خواهد شد و این در حالی است که سرب، روی، قلع، طلا و نقره، پیش‌تر و تا قبل از سال ۱۹۹۰ تمام شده‌اند.

ه) کنت وات در یک سخنرانی در مورد عصر یخبندان پیش رو هشدار داد که: «جهان حدود بیست سال است که به شدت در حال سرد شدن است و اگر این روند ادامه یابد، میانگین دمای جهانی در ۱۹۹۰، حدود چهار درجه سردتر خواهد بود، اما در سال ۲۰۰۰ یازده درجه سردتر خواهد بود. این تقریباً دو برابر چیزی است که برای وارد شدن به عصر یخبندان نیاز است» (ام. جی پری، ۲۰۲۲).

و) در گزارشی که آلاسدایر ادواردز[۱۲] برای گروه متخصصان مشترک‌المنافع تغییرات آب‌وهوا و افزایش سطح دریاها[۱۳] تهیه کرد، عنوان شد که به علت آب شدن یخ‌ها، مالدیو ظرف ۳۰ سال آینده، به طور کامل، به زیر آب خواهد رفت. اتفاقی که البته هرگز رخ نداد (ادواردز، ۱۹۸۹).

---

[6] The Progressive
[7] Life
[8] Kenneth Watt
[9] Times
[10] Harrison Brown
[11] Scientific American
[12] Alasdair J. Edwards
[13] Commonwealths' expert groups on climate change and sea level rise

۴ بحث

برای کنترل همه جا، باید از عاملی استفاده کرد که در همه جا حضور داشته باشد و جهان شمول باشد. لذا، به نظر می‌رسد که تغییرات اقلیمی و موارد مرتبط با آن (مثل افزایش گازهای گلخانه‌ای و مصرف کربن)، گزینه‌ی خوبی برای کنترل جهان‌شمول است، چرا که اقلیم، پدیده‌ای جهان شمول است.

مطابق نظر بیل گیتس: «تا سال ۲۰۶۰، تغییرات آب‌وهوایی می‌تواند به اندازه‌ی کرونا کشنده باشد و تا سال ۲۱۰۰ می‌تواند پنج برابر مرگبارتر شود ... به عبارت دیگر، تأثیرات تغییرات آب‌وهوایی تقریباً به طور قطع شدیدتر از کرونا خواهد بود و برای آنهایی که کمترین اثر را در ایجاد این تغییرات داشته‌اند، اوضاع وخیم‌تر خواهد بود» (گیتس، ۲۰۲۰). پرسشی که در اینجا مطرح می‌شود آن است که این صحبت بیل گیتس، تا چه اندازه درست است؟

سپتامبر امسال و همزمان با نشست مجمع عمومی ملل متحد در نیویورک، بنیاد راکفلر اعلام کرد که برای پیشبرد اهداف اقلیمی جهانی و کمک به اطمینان از مشارکت همه در آن، در طول پنج سال آینده، بیش از یک میلیارد دلار سرمایه گذاری خواهد کرد. دریاسالار جیمز استاوریدیس[۱۴]، رئیس هیئت امنای بنیاد راکفلر، گفت: «بحران آب‌وهوا بزرگ‌ترین تهدید بشریت است – و برای بنیادی که مختص رفاه بشری است – اتخاذ این استراتژی هم منطقی و هم ضروری است (بنیاد راکفلر، ۲۰۲۳). در اینجا باید پرسید که در پس این هزینه هنگفت، چه سودی برای این قبیل بنیادها نهفته است؟ در واقع هدف از خرج این ارقام هنگفت چیست؟

چند سال پیش (۲۰۱۰)، بنیاد راکفلر و شبکه جهانی کسب‌وکار[۱۵]، در گزارش مشترک خود، با عنوان «سناریوهایی برای آینده‌ی تکنولوژی و توسعه بین‌الملل» به مبحث قرنطینه[۱۶] اشاره داشته است که نمونه‌ی آن در دوران کرونا، رخ داد. نکته‌ی بسیار جالب آن است که یکی از ابزارهای کنترلی تغییرات اقلیمی، همین قرنطینه کردن مجدد مردم است که ذیل قرنطینه‌های آب‌وهوایی و ... تعریف می‌شود. نشریه تلگراف انگلستان، با اشاره به پژوهشی از کوری و همکاران[۱۷] (۲۰۲۱) عنوان کرده که برای دستیابی به اهداف اقلیمی، باید هر دو سال یک‌بار، قرنطینه و لاکدان[۱۸] داشته باشیم تا انتشار گازهای گلخانه‌ای کاهش یابد اولویا رودگارد[۱۹]، (۲۰۲۱)؛ که اولین نمونه‌ی آن را هم در کشور خودمان، در تابستان امسال و با عنوان تعطیلی به دلیل گرمای بی‌رویه شاهد بودیم (خبرگزاری تسنیم، ۱۴۰۲). هرچند که به نظر نمی‌رسید که گرمای مردادماه امسال، تفاوت خاصی با سال‌های قبل داشته باشد.

در متن گزارش بنیاد راکفلر، ذیل عنوان مرحله‌ی قرنطینه، نوشته شده: «دنیایی با کنترل شدیدتر دولتی از بالا به پایین و راهبری مستبدانه‌تر، با نوآوری محدود و جلوگیری از رشد شهروندان»؛ نکته‌ی جالب آن است که در این گزارش که چند سال پیش از کرونا نوشته شده، دقیقاً حرف از پاندمی، ماسک زدن و کنترل مردم

[14] James Stavridis
[15] Rockefeller Foundation and Global Business Network
[16] Lock Step
[17] Corinne Le Quéré et al.
[18] Lockdown
[19] Olivia Rudgard

به بهانه‌ی پاندمی، آمده است.

در این گزارش، در خصوص اقلیم و اشارات مرتبط با آن، آمده: بدون شک، وضعیت اقلیمی زمین، به طور فزاینده‌ای ناپایدار شده است. تغییرات آب‌وهوایی هم، مشکل منحصر به کشورهای در حال توسعه نیست (بنیاد راکفلر، ۲۰۱۰).

اکنون، پاندمی پایان یافته است اما گویا اهداف کنترلی و سلطه‌جویانه‌ی امثال راکفلرها، پایان نیافته و مستند به گفته‌های خود ایشان، به نظر می‌رسد که برنامه‌ی بعدی برای کنترل دنیا، تغییرات اقلیمی باشد که با دخالت بشر در روندهای طبیعت (از قبیل سدسازی، بارورسازی ابرها و ...) در حال وقوع است. قرآن کریم در این خصوص می‌فرماید: «به سبب آنچه دست‌های مردم فراهم آورده، فساد در خشکی و دریا نمودار شده است» (سوره‌ی روم، آیه‌ی ۴۱).

یکی از مهم‌ترین دلایل نادرستی نظریه‌های مرتبط با گرم شدن زمین که البته در حال حاضر، بیشتر ذیل عبارت تغییرات اقلیمی تعریف می‌شود، اثبات نادرستی پیش‌بینی‌های قبلی انجام شده، با گذر زمان است.

به تازگی، جان کلاوزر[۲۰]، برنده‌ی نوبل فیزیک در سال ۲۰۲۲، اعلام کرد: «روایت تغییر آب‌وهوا به واسطه‌ی فعالیت بشر، فریبی است که توسط نخبگان و برای خالی کردن زمین از جمعیت ایجاد شده است» (عدل طباطبایی، ۲۰۲۳).

و حالا پرسش مهم آن است که اگر کل ماجرای تغییرات اقلیم، یک فریب است، به چه جهت، این دروغ بزرگ، مرتب تکرار می‌شود و در عهدنامه‌های مختلف بین‌المللی (مثلاً توافق‌نامه‌ی اقلیمی پاریس[۲۱])، از لزوم پرداختن به آن و اعمال روش‌های گوناگون برای کنترلش، سخن به میان آمده است؟

در متن سند توسعه پایدار ۲۰۳۰، ذیل هدف سیزدهم (اقدام فوری برای مبارزه با تغییرات اقلیمی و اثرات آن) زیر هدف ۲.۱۳ آمده است: توافق‌نامه‌ی پاریس که در سال ۲۰۱۵ به تصویب رسید، آخرین گام در تکامل رژیم تغییر اقلیم سازمان ملل است و بر اساس کارهای انجام شده تحت کنوانسیون است که هدف اصلی آن تقویت واکنش جهانی به تهدید تغییرات آب‌وهوایی، از طریق نگه داشتن افزایش دمای جهانی در این قرن به میزان بسیار کمتر از ۲ درجه سانتی‌گراد است. رقم دمایی که البته بالاتر از میزان طبیعی آن، از قبل از صنعتی شدن بشر است. اکنون، پیگیری تلاش‌ها برای محدود کردن افزایش دما تا ۵.۱ درجه سانتی‌گراد است. در خصوص گام‌های قبلی سازمان ملل در مورد تغییرات اقلیمی، می‌توان به چهارچوب سندای (مصوب ۲۰۱۵) و بیانیه‌ی ریو (مندرج در پایگاه اطلاعاتی جمهوری اسلامی ایران بر روی سایت سازمان ملل، ۱۹۹۲) و از این قبیل اشاره کرد. توافق اقلیمی پاریس، در کنار سند توسعه پایدار، جدیدترین اسناد تحمیلی سازمان ملل به کشورها، در راستای پروژه‌ی تغییرات اقلیم این سازمان است. هدف از این توافق، تقویت توانایی کشورها برای مقابله با اثرات تغییرات آب‌وهوایی است (metadata indicator, SDG, 2021).

اساساً چه سنجه و معیاری وجود دارد که ثابت کند این اعداد و ارقام پیش‌بینی شده (گرم شدن زمین

[20] John Clauser

[۲۱] توافق‌نامه اقلیمی پاریس، در سال ۲۰۱۵ و در کنفرانس بین‌المللی سازمان ملل برای تغییرات اقلیمی، و در جهت مقابله با تغییرات اقلیمی و اثرات منفی آن تصویب شد که یک معاهده‌ی الزام‌آور بین‌المللی است. این موافقت‌نامه مشتمل بر تعهدات اعضا برای کاهش انتشار گازهای گلخانه‌ای و همکاری برای تطبیق با تأثیرات تغییرات اقلیمی است (سازمان ملل متحد، ۲۰۲۳).

به میزان ۲ درجه و تلاش برای کم کردن آن، تا ۵.۱ درجه) درست هستند؟ آیا این امکان وجود ندارد که این اعداد و ارقام، همانند آنچه در ۵۰ و اندی سال پیش، برای اولین پاسداشت روز زمین، توسط دانشمندان آن زمان پیش‌بینی شده بود – پیش‌بینی‌هایی که غلط بودند – نادرست باشند؟

تغییرات آب‌وهوایی، بر پایه‌ی مواردی استوارند که نادیدنی هستند و برای افراد مختلف، قابل سنجش و ارزیابی نیستند (شبیه کرونا)؛ اساس تغییرات آب‌وهوایی بر مبنای چیزی است که قابل اندازه‌گیری نیست: CO_2 (همنت بروانی و همکاران،۲۰۲۲). لذا فریب دادن مردم، با آنچه که برای خودشان، ملموس نیست، کار چندان سختی نیست.

در ابتدای بحث حاضر گفته شد که: «برای کنترل همه جا، باید از عاملی استفاده کرد که در همه جا حضور داشته باشد و جهان شمول باشد». آب‌وهوا، عاملی است که در همه جا حضور دارد. به‌علاوه باید در نظر داشت که اِعمال کنترل، مستلزم داشتن اطلاعات است و مهم‌ترین مقوله در سایبرنتیک، توان اعمال کنترل است (نصیری و شکوهیان‌راد، ۱۴۰۱)؛ لذا بدیهی است که مقوله‌ی تغییرات اقلیمی، ارتباط تنگاتنگی با اطلاعات، جریان داده و همچنین سایبرنتیک دارد. ظاهر امر آن است که کنترل آب‌وهوا، در همه جا مقدور نیست، اما در خصوص کنترل جریان اطلاعات، این طور نیست. با کنترل جریان اطلاعات و در نتیجه‌ی آن، می‌توان بخش اعظم ماده و انرژی جهان را کنترل کرد. در واقع جریان اطلاعات، اهرم کنترل ماده و انرژی برای انسان است. به نظر می‌رسد یکی از دانش‌هایی که در خصوص تغییرات اقلیمی و اعمال کنترل جهان‌شمول، کاربرد دارد، اکوسایبرنتیک است که بحث اصلی آن، اعمال کنترل بر زیست‌بوم (و به تبع آن، تمامی اجزای وابسته به آن، خصوصاً انسان) از طریق کنترل جریان اطلاعات است (نصیری و شکوهیان‌راد، ۱۴۰۱). پترز و همکارانش (۲۰۲۱) معتقدند که ما اکنون در نقطه تاریخی خاصی قرار داریم که در آن، زیست‌شناسی و اطلاعات گرد هم می‌آیند تا با گسترش سیستم‌های اکوسایبرنتیک، مسیرهای تکاملی – فرهنگی را در رابطه با حکومت زمین تعیین کنند. جالب آن است که از نظر ایشان، اطلاعات و اکوسایبرنتیک، چیزهایی است که منجر به تعیین حکومت در زمین می‌شود! یعنی همان چیزی که گلوبالیست‌ها در تلاشند تا ذیل مقوله‌ی علم و تعابیر علمی، اما در عمل، برای اِعمال کنترل بر کشورهای مختلف و ابناء بشر بدان دست یابند و به همین دلیل است که به بحث تغییرات اقلیمی پر و بال داده‌اند و آن را به عنوان یک اصل مسلم مطرح نموده‌اند و وارد ادبیات بین‌المللی، سازمان ملل و توابع آن و نیز معاهدات بین‌المللی (نظیر توافق‌نامه‌ی اقلیمی پاریس) نموده‌اند.

برای روشن شدن این بحث و توضیح بیشتر، باید اشاراتی در خصوص جمع‌آوری اطلاعات، در سامانه‌های مختلف هوا و اقلیم‌شناسی، جنگل‌بانی، محیط‌بانی و ... داشت. امروزه، پیش‌بینی آب‌وهوا، تا حد زیادی به سیستم‌های سایبرنتیکی و بانک‌های اطلاعات و داده‌ها وابسته است. همچنین، کنترل بسیاری از پدیده‌های زیست‌محیطی، به سیستم‌های سایبری واگذار شده است (مثال ساده و ملموس این موضوع، کنترل خودکار دریچه‌ی سدهاست. هرگونه دستکاری، عملیات مخرب و ارائه‌ی داده‌ای غلط در سیستم‌های کنترلی این دریچه‌ها، می‌تواند منجر به باز شدن اشتباهی آنها و وقوع سیلاب شود). برای نمونه، در کشور کانادا، سیستم

مدیریت داده‌ها در رصد زمین[۲۲]، بخشی از طرح احیای منابع طبیعی کانادا برای بهبود ظرفیت ماهواره‌ای رصد زمین در کانادا و دسترسی به داده‌های آن است. اساساً حفظ و بایگانی داده‌ها و اطلاعات سایبرکارتوگرافی[۲۳]، بخشی از فرآیند حفاظت محیط زیست، در نظر گرفته می‌شود (تریسی پی. لوریو و فریزر تیلر، ۲۰۱۹). لذا آنچه که در اینجا، مثل بسیاری از پدیده‌های دیگر عصر کنونی زندگی بشر، پررنگ است، جمع‌آوری داده‌ها و اطلاعات و اعمال کنترل، بر مبنای همین داده‌ها، بر سیستم‌های طبیعی و زیستی است. در اینجا، هرگونه داده‌ی ورودی غلط، منجر به خروجی اشتباه در عملکرد سیستم‌ها می‌گردد که می‌تواند به یک فاجعه یا بحران زیست‌محیطی بینجامد. در اینجا نیز، کسی که دست برتر را در کنترل داده‌ها در اختیار دارد، می‌تواند در زمان لازم، برای القای فریب تغییرات اقلیمی، وارد عمل شده و مسیر واکنش‌های بشری را، بر مبنای شیطنت و دستکاری در اطلاعات ورودی، تغییر دهد و به این ترتیب، به دلیل ایجاد واکنش نادرست، سبب ایجاد بحران زیست‌محیطی شود، بحرانی که در اصل، وجود خارجی نداشته و به سبب واکنش غلط، ایجاد شده است (شبیه همان ماجرای باز شدن دریچه‌های سد).

۵ نتیجه‌گیری

به نظر می‌رسد با باور کردن هرچه بیشتر فریب تغییرات اقلیمی، در واقع به دست خود، محدودیت‌های گوناگونی برای صنعت، کشاورزی و حیات ایجاد کرده‌ایم، چرا که تغییرات اقلیمی، متصل به عنصر کربن است و تمام موارد مذکور، با کربن در ارتباطند. همچنان که مارک مورانو[۲۴]، دستیار سیاسی سابق جمهوری‌خواهان و مدیر ارتباطات کمیته‌ی محیط زیست و امور همگانی سنا در دولت جورج دبلیو بوش و نویسنده‌ی کتاب «بازتنظیم بزرگ: سردمداران گلوبال و قرنطینه‌ی همیشگی»، در یک مصاحبه گفته است: فروپاشی اقتصادی برنامه‌ریزی شده و قرنطینه‌ها، همگی بخشی از دستور کار اقلیمی هستند. وی معتقد است که تمام نشست‌های مرتبط با آب‌وهوا، خواستار «جنبش رشد زدایی» یا «رکودهای برنامه ریزی شده» برای مبارزه با گرمایش جهانی‌اند. و این بدان معناست که دولت‌ها، رشد اقتصادی کندتری را تحمیل می‌کنند و یا برای کاهش انتشار گازهای گلخانه‌ای، رکود اقتصادی را اجباری می‌کنند (گریت گیم ایندیا، ۲۰۲۲).

با استفاده از بالا و پایین کردن محدودیت‌های کربنی، به سادگی می‌توان در صنعت و کشاورزی، ایجاد محدودیت و کنترل نمود؛ لذا منطقاً پذیرش این موارد، به مثابه ترمزی برای صنایع و کشاورزی خواهد بود. از آنجایی که هیچ یک از نظریه‌هایی که برای گرم شدن زمین و تغییرات اقلیم، مطرح می‌شوند، تاکنون به اثبات کامل نرسیده‌اند، و نادرستی اغلب نظریات سابق نیز، در گذر زمان، اثبات شده است، لذا هیچ لزومی به پذیرش این فریب بزرگ که در واقع، برای محدودسازی بیشتر و اعمال کنترل همه‌جانبه بر تمام جنبه‌های حیات بشری (به واسطه‌ی عنصر کربن) می‌باشد، وجود ندارد.

نکته‌ی دیگری که باید مدنظر داشت، آن است که واکنش‌های درست به پدیده‌های مرتبط با آب‌وهوا و

[22] EODMS: The Earth Observation Data Management System

[۲۳] Cybercartography: کارتوگرافی، به معنای نقشه‌برداری است که در کنار سایبر، به مفهوم نقشه‌برداری مبتنی بر سایبر است.

[24] Marc Morano

محیط زیست، منوط به داشتن داده‌های درست است. هرگونه داده‌پردازی یا ارائه‌ی داده‌های نادرست (شبیه همان چیزی که در پیش‌بینی‌های اقلیمی سال ۱۹۷۰ صورت گرفت که عمدتاً اشتباه بودند) منجر به ایجاد واکنش‌های نادرست شده که می‌تواند، مسبب ایجاد بحران اقلیمی و زیست‌محیطی باشد، بدون آنکه در اصل و در واقعیت، بحرانی وجود داشته باشد!

آنچه در فوق، به صورت خلاصه و مختصر ارائه شد، می‌تواند ابزاری باشد که ذیل عنوان تغییرات اقلیمی، کشورها و دولت‌ها را وادار به انجام واکنش‌ها و عملکردهایی کند که مد نظر دست‌های پنهان حاکم بر دنیا و گلوبالیست‌هاست.

مراجع

[۱] پایگاه اطلاعاتی جمهوری اسلامی ایران بر روی سازمان ملل متحد، «بیانه‌ی ریو، پیرامون محیط زیست و توسعه»، آگوست ۱۹۹۲.
https://tinyurl.com/26bfhknb

[۲] خبرگزاری تسنیم، «چهارشنبه و پنج‌شنبه، سراسر کشور تعطیل شد»، مرداد ۱۴۰۲.
https://tinyurl.com/44xr8x9e

[۳] ع. نصیری و م.ع. شکوهیان‌راد، «تهدیدات اکوسایبرنتیکی، چهارچوب نوین تهدیدات علیه زیست‌بوم»، از مجموعه مقالات نخستین کنفرانس ملی فضای سایبر، ۱۴۰۱، ۱۵ ص.

[4] H. Bherwani, D. Balachandran, A. Das, R. Kumar, “Monetary quantification of COVID-19 impacts on sustainable development goals: Focus on air pollution and climate change”, in: “COVID-19 and the Sustainable Development Goals”, Elsevier Publication, 2022, pp. 159-175.

[5] W. S. Brocker, “Climatic Change: Are We on the Brink of a Pronounced Global Warming?”, Science, Vol 189, Issue 4201, 1975, pp. 460-463.

[6] A. J. Edwards, “The implication of sea level rise for the republic of Maldives”, Center for tropical coastal management studies, University of Newcastle, 1989, 109 p.

[7] B. Gates, “COVID-19 is awful. Climate change could be worse.”, Auguste 2020: https://www.gatesnotes.com/Climate-and-COVID-19

[8] Great Game India, “World Economic Forum Cites Compliance with COVID Mandates to Promote ‘Climate Change’ Lockdowns”: September 2022: https://greatgameindia.com/climate-change-lockdowns/

[9] I. Hilton, “The Reality of Global Warming: Catastrophies Dimly Seen”, World Policy Journal, Vol. 25, No. 1, 2008, pp. 1-8.

[10] T. P. Lauriault, D. R. F. Taylor, “The preservation and archiving of geospatial data and Cybercartography as a proactive preservation process” in Further Developments in the Theory and Practice of Cybercartography, Modern Cartography Series, Volume 7, 2019, pp. 179-196.

[11] R.M. Lucas, P. Gies, “Stratospheric Ozone”, Encyclopedia of Environmental Health, ScienceDirect Publication, 2011, pp. 249-263.

[12] "The Paris Agreement" on The United Nations' website, last update: 2023: https://www.un.org/en/climatechange/paris-agreement

[13] M. J. Perry, "18 Spectacularly Wrong Predictions Were Made Around the Time of the First Earth Day in 1970", Expect More This Year", 2022, American Enterprise Institute: https://www.aei.org/carpe-diem/18-spectacularly-wrong-predictions-were-made-around-the-time-of-the-first-earth-day-in-1970-expect-more-this-year/

[14] M.A. Peters, P. Jandric, S. Hayes, "Biodigital Philosophy", Technological Convergence, and Postdigital Knowledge Ecologies, Postdigital Science and Education, vol. 3, 2021, Pages 370-388.

[15] Rockefeller Foundation, "The Rockefeller Foundation Commits Over USD 1 Billion To Advance Climate Solutions", 2023: https://www.rockefellerfoundation.org/news/the-rockefeller-foundation-commits-over-usd-1-billion-to-advance-climate-solutions/

[16] Rockefeller Foundation and Global Business Network, "Scenarios for the Future of Technology and International Development", 2010, 54 p. https://www.docdroid.net/YMLwGat/2010-scenarios-for-the-future-of-technology-and-international-development-rockefeller-gbn-pdf

[17] O. Rudgard, "Lockdown-level emissions cuts needed every two years to meet climate goals", The Telegraph, March 2021: https://www.telegraph.co.uk/environment/2021/03/03/lockdown-level-emissions-cuts-needed-every-two-years-meet-climate/

[18] SDG indicator metadata, "Target 13.2: Integrate climate change measures into national policies, strategies and planning", last update: 2021, 5 p: https://unstats.un.org/sdgs/metadata/files/Metadata-13-02-02.pdf

[19] S. Singh, P. Singh, R. Selvasembian, K.K. Srivastava, "Global Climate Change", ScienceDirect Publication, 2021, 425 p.

[20] S. A. Tabatabai, "Nobel Prize-Winning Scientist: 'Climate Crisis Is a Hoax To Depopulate the Planet'", July 2023: https://thepeoplesvoice.tv/nobel-prize-winning-scientist-climate-crisis-is-a-hoax-to-depopulate-the-planet/

[21] C. Thompson, "How 19th Century Scientists Predicted Global Warming", December 2019: https://daily.jstor.org/how-19th-century-scientists-predicted-global-warming/

Optics and Photonics, 2008.

[2] C.-S. Chan, "An image authentication method by applying hamming code on rearranged bits," Pattern Recognition Letters, vol. 32, no. 14, pp. 1679 – 1690, 2011.

[3] C.-S. Chan and C.-C. Chang, "An efficient image authentication method based on hamming code," Pattern Recogn., vol. 40, pp. 681–690, Feb. 2007.

[4] A. Haouzia and R. Noumeir, "Methods for image authentication: a survey," Multimedia Tools and Applications, vol. 39, no. 1, pp. 1–46, 2008.

[5] Ling Du, Anthony T.S. Ho, Runmin Cong, Perceptual hashing for image authentication: A survey, Signal Processing: Image Communication, Volume 81, 2020, pp. 115713.

[6] M. Sajjad, I. U. Haq, J. Lloret, W. Ding and K. Muhammad, "Robust Image Hashing Based Efficient Authentication for Smart Industrial Environment," in IEEE Transactions on Industrial Informatics, vol. 15, no. 12, pp. 6541-6550, Dec. 2019, doi: 10.1109/TII.2019.2921652.

[7] Karsh, R.K. LWT-DCT based image hashing for image authentication via blind geometric correction. Multimed Tools Appl 82, pp. 22083–22101, 2023.

[8] Thabit, R. Review of medical image authentication techniques and their recent trends. Multimed Tools Appl 80, 13439–13473, 2021.

[9] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," Information Forensics and Security, IEEE Transactions on, vol. 1, pp. 215 – 230, 2006/06// 2006

[10] G. Zhu, J. Huang, S. Kwong, and J. Yang, "A study on the randomness measure of image hashing," IEEE Transactions on Information Forensics and Security, vol. 4, pp. 928–932, Dec 2009.

[11] Y. Mao and M. Wu, "Unicity distance of robust image hashing," IEEE Transactions on Information Forensics and Security, vol. 2, pp. 462–467, Sept 2007.

[12] O. Koval, S. Voloshynovskiy, P. Bas, and F. Cayre, "On security threats for robust perceptual hashing," in Media Forensics and Security, vol. 7254, p. 72540H, feb 2009.

[13] T. Uehara and R. Safavi-Naini, "On (In)security of A Robust Image Authentication Method", pp. 1025–1032. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002.

[14] M. Heidari, S. Samavi, S. M. R. Soroushmehr, S. Shirani, N. Karimi, and K. Najarian, "Framework for robust blind image watermarking based on classification of attacks," Multimedia Tools and Applications, Nov 2016.

[15] D. Hu, B. Su, S. Zheng, and Z. Zhang, "Secure architecture and protocols for robust perceptual hashing," in Computational Intelligence and Security (CIS), 2013 9th International Conference on, pp. 550–554, Dec 2013.

instead of one in the original scheme will increase the diffusion. However, it is worth to mention that the robustness of the scheme is not influenced in the proposed modification due to using the same coding and embedding building blocks. Here it is shown that the proposed modification strengthens the security of the original scheme significantly against the mentioned key recovery attack. Let the image be of size $N \times N$. To recover the first secret key corresponding to Torus automorphism uniquely, the attacker does not have difficulties due to Equation 1 and negligible image size in this sense. However the cost of finding the positions is of order $O(N^6)$. Also the cost of recovering the secret random permutation is approximately 12!. So the whole computational complexity required for recovery of secret components excluding the generated random numbers would be $C = O(N^6) + 16 \times 12!$. The generated random numbers must be disclosed via exhaustive search as well which increases the complexity.

The complexity would be higher for the extended version as well. In fact, the cost of recovering secret random permutation used in the parity check part is 16! which simply affects the second term of the equation. Concerning the commonly used values for N and pixel depth, the attack complexity C has increased significantly however some low thresholds on N and pixel depth can be set to satisfy desired security strength according to the existing computational power. To enhance the security more, a keyed pseudo-random function whose label is dependent to the image can be used instead to embed the generated random output into the MSBs. In this case the labeled function provides the intrinsic security strength of a cryptographic authentication function. Further improvement in the accuracy of the tamper localization is possible as well by using another code structure with higher detection and correction capability. The latter suggestions are considered as future work since there is not enough room left in this paper.

7 Conclusion

An image authentication scheme based on Hamming code and rearrange MSBs of pixel intensity values has been analyzed. Some modifications in preprocessing step and computation of authentication data have been proposed to enhance the security and accuracy of the scheme. The proposed modifications strengthen the scheme against the aforementioned flaw and generalize the scheme to be used on grayscale images with 16 bits pixel intensity values. However there is still some room left for further enhancement to elaborate the design more. Using different types of systematic error-correcting schemes which increases the detection and correction capability and engaging a keyed labeled cryptographic pseudorandom function would be a potential track for the improvement and further secure designs.

References

[1] O. Koval, S. Voloshynovskiy, F. Beekhof, and T. Pun, “Security analysis of robust perceptual hashing,” in Electronic Imaging 2008, pp. 681906–681906–10, International Society for

be corrected using the correction capability of the error-correcting code. Whenever the occurred errors are beyond the capability of Hamming code (more than one bits) the correction attempt is further continued using adjacent pixels. If the latter trial fails, the erroneous pixels are marked as tampered or manipulated area of the image.

5.2 Extension to 16-bit Grayscale Images

The scheme has been so far set for the cases wherein images are grayscale and the pixel depth is an 8-bit value. However, there are many applications specially in medical images in which the pixel depth is 16 bits. The proposed scheme with the existing coding structure is not applicable in such cases due to the code word length. To extend the scheme, the Hamming error correcting code with parameters $n = 15$, $k = 11$ ($[15, 11, 3]_2$) with higher coding rate can be used. In the latter code, four parity check bits for eleven MSBs of each pixel are generated and embedded into the four LSBs of other pixels values corresponding to the revised algorithm described in Section V. However the embedding procedure is modified slightly and eleven pixels are selected in each step to generate four parity check words for embedding in the eleven target pixels determined by Torus transformation (the value of k is set to 4). When the image size number is not a multiple of 11 which is in the most of the cases, the last pixels to be processed are processed naively one by one which does not significant impact on the security. Similar to the initially proposed scheme, each selected pixel will contribute in generating each parity check word. However to avoid further computational cost and size adjustment problem one can update four pixels in each step like the latter enhanced scenario as follows.

$$
\begin{aligned}
W_1 &= p_{11}p_{22}p_{33}p_{44}p_{15}p_{16}p_{17}p_{18}p_{19}p_{110}p_{111} \\
W_2 &= p_{21}p_{12}p_{43}p_{34}p_{25}p_{26}p_{27}p_{28}p_{29}p_{210}p_{211} \\
W_3 &= p_{31}p_{42}p_{13}p_{24}p_{35}p_{36}p_{37}p_{38}p_{39}p_{310}p_{311} \\
W_4 &= p_{41}p_{32}p_{23}p_{14}p_{45}p_{46}p_{47}p_{48}p_{49}p_{410}p_{411}
\end{aligned}
$$

Further processing is the same as the enhanced scheme in the latter subsection in which the 11-bit words are added via XOR operation with random words of the same size before encoding. The generated parity check bits are permuted and then embedded into the LSBs accordingly. Like the original scheme, erroneous bits can be detected or one can be corrected without detection of other erroneous bits. However the security of the scheme will be strengthened due to longer parity check values. This point is addressed in the following section.

6 Revisiting the Analysis of the Modified Scheme

The main security aspect of the modified scheme is that any significant changes in a pixel (MSBs) will be reflected to up four host pixels which was one pixel at max in the original Chan's scheme. Also expanding the pixels processing to four branches simultaneously

5 Improving and Enhancing the Authentication Model

5.1 Enhancing the Scheme

To enhance the Chan's scheme and increase the security against the aforementioned attack while keeping its original elaborated robustness, the following modifications will be suggested on two steps of the scheme.

1) At first as a preprocessing step, the image undergoes some preprocessing steps including a bilinear interpolation and mapping to a fixed-size square image. An optional low-pass filtering can be applied on the image to provide minor robustness.

2) To start processing the image pixels, four pixels are chosen at random. The main modification applies in calculating the parity check parts of the pixels in the processing step. Similar to the original scheme a Hamming code with parameters $n = 7$ and $k = 4$ is used for encoding purpose. However all four pixels contribute in generating each parity check value in the proposed scheme. The details are as follows: let the four selected pixels are denoted by P_1, P_2, P_3, and P_4 whose first four MSBs are indicated by $p_{i1}p_{i2}p_{i3}p_{i4}$ for $i = 1, 2, 3, 4$.

$$W_1 = p_{11}p_{22}p_{33}p_{44}, W_2 = p_{21}p_{12}p_{43}p_{34}, W_3 = p_{31}p_{42}p_{13}p_{24}, W_4 = p_{41}p_{32}p_{23}p_{14} \quad (3)$$

By this arrangement of the MSBs, each generated authentication bit would be a function of all processed pixels. Also each new nibble W_1, W_2, W_3, W_4 contains all significant values. In the proposed modified scheme four pixels are used in each step for extracting the authentication data. To increase the entropy of the intermediate bits, the nibbles are added via XOR operation with random words (R_1, R_2, R_3, R_4) generated from a key-based pseudo random number generator PRNGk as follows.

$$W'_i = W_i \oplus R_i \quad , i = 1, 2, 3, 4 \quad (4)$$

Some proper Boolean functions can be used instead to introduce some nonlinearity into the scheme.

3) Four 3-bit parity check values as authentication data of four pixels are computed by applying the Hamming code on W'_1, W'_2, W'_3, W'_4 respectively. The authentication bits are firstly concatenated and then permuted using a key-based random permutation before embedding. Finally the next four pixels to be processed are determined by Torus transformation wherein the permuted parity check bits are embedded.

The recovery procedure in the modified image authentication is almost the same as recovery procedure in the original Chan's scheme. In the recovery phase, the original pixel values (MSBs) are recovered by applying reverse permutation and decoding operation followed by XORing with the random nibble words. However in the modified scheme, four pixels are recovered at the same time. Hamming codes are able to detect up to two erroneous bits whereas are able to correct one bit without detection. The possible tampered or manipulated areas of the image are localized further and tried to

$(00000011)_2$, $(00000110)_2$ receptively. It is observed trivially that as the four MSBs of P'_j are left unchanged, its authentication data will not be affected as well. This indicates the termination of the diffusion in the embedding process. Now, with the knowledge on the position of modified pixel (j), Equation (1) and aforementioned weakness property the value of the second key can be extracted. This attack in a chosen plaintext model can be easily generalized. It is supposed that the attacker has a black-box oracle access to the image authentication scheme indicating that she can request the watermarked image on any chosen input image. The attack is described in the following steps:

- Step One (offline step): The attacker chooses an image I whose pixels have the same intensity value $P_i = p$. To skip the impact of the first secret key (to ease the attack scenario as mentioned before), p can be selected from the set $[0; 15] \cup [112; 143] \cup [240; 255]$.
- Step Two: The watermark image I' is calculated using the image authentication scheme. It is easy to verify analytically that for some values like $p = 0, 8, 112$, $I = I'$.
- Step Three: The attacker modifies a pixel value P_i as $P'_i = p + d_i$. The choice of d is of great importance and plays a crucial role. d_i is selected such that $d > 0$ and the MSBs of the host pixel will not be influenced however LSBs will be modified.
- Step Four: The attacker calculates the watermarked image I'' using the image authentication scheme.
- Step Five: A binary difference matrix indicating the difference between I' and I'' is calculated as $[Dij] = 1 - d_{(I'ij - I''ij)}$.

The elements corresponding to '1' in the above difference matrix is used to solve the system of linear equations 1 to recover the unknown value k_2. The secret permutation generated by the first secret key using a sequence of random numbers is extracted by an exhaustive search using some chosen MSBs which generate the required parity check values. To launch the attack, the attacker just requires two calls to the image authentication scheme for recovering the second key. Also, secret permutation used before embedding can be extracted with $2N^2$ calls resulting in maximum $2N^2 + 2$ total calls with chosen images. Considering the typical image sizes corresponding to N = 512, 1024, the complexity is of order 219 or 221 which is negligible in cryptanalysis.

This attack can be extended to the earlier version of the Chan's image authentication scheme presented in [3] trivially. In the initial scheme, the LSB replacement is used instead of the Modulus function and the pixels are being processed one by one from left to right according to the Torus automorphism. Also the bit reversion on the MSBs are not applied. The attack conditions are met much easier in this case. In fact the choice of difference value di in the third step is less restricted: all of the values of d which keep the encoded value of $(p + d) >> 4$ unchanged (while changing the LSBs of $p + d$) would be valid for this attack. However the complexity of the attack remains unchanged.

cycle is completed by reaching the first pixel P_i. Then the process is repeated to process the whole pixels set. At the end of this procedure the authentication data of each pixel is embedded into another pixel. The detecting procedure localizes and marks the tamper area for the sake of recovery in the recovery procedure. In this phase the authentication data of each pixel is extracted firstly and compared with the regenerated value. The details of this procedure are given in [2].

4 Analysis of Chan's Scheme

The presented image authentication scheme uses two main secret keys in the embedding phase. This first key is used as a seed to generate a sequence of random numbers for the rotation operation and the second key is used in the Torus automorphism to provide ambiguity in locating the host pixel. According to [2, 3], the purpose of employing two secret keys is to provide the security against cases when one key is recovered by the attacker. In fact, if the keys are disclosed, the attacker can design different attack scenarios like impersonation or substitution attack. In this section, we show that when the Chan's image authentication scheme is applied on the chosen images with specified pattern (chosen plaintext attack model) then the second secret key can be recovered trivially followed by an exhaustive search to recover the first key. The second key can be recovered by inquiring two authenticated images I, I' differing in one pixel $(x_i; y_i)$, by solving the Equation (1) for k_2. However, it might happen that more than one pixel in the row $i+j$ in I' will be modified. In this case the key k_2 cannot be determined uniquely. The main security issue of the discussed image authentication scheme is the lack of enough diffusion which is required for a robust image authentication scheme. In fact, the required diffusion in image authentication schemes is not evaluated as in classical cryptographic primitives. It should not hinder the robustness without compromising the security. This issue is used to recover the value of the second key uniquely. To explain this property, let the image I consisting of the pixels all with the same intensity value and its authentication embedded version J are given. The attacker manipulates a pixel value P_i at a chosen position $(x_i; y_i)$ such that $P'_i = P_i + d_i$. The choice of d_i and the constant pixel intensities will be explained later. To bypass the influence of the first key, it is supposed that the parity check (and therefore the authentication data) of the pixel p_i is $(000)_2$ or $(111)_2$. With this assumption reordering the bit positions does not influence on the recovered value. To satisfy the latter assumption, the four MSB values of P_i must be one of the possible values $(0000)_2$, $(0111)_2$, $(1000)_2$ and $(1111)_2$ based on the Hamming code generator matrix. The strategy of the attack is to manipulate one-pixel intensity value such that its authentication data just modifies the host pixel while embedding. To observe how the attack works, the simplest case is considered. Let $P_i = 0$ and $d_i = 96 = (01100000)_2$. Then the authentication data of P'_i is calculated as $s'_i = (101)_2$ or $s'_i = (011)_2$ or $s'_i = (110)_2$ depending on the corresponding random number R_i. Let the host pixel wherein s_i is embedded be denoted by P_j. According to Equation (2), the updated value of P_j indicated by P'_j would be one of the intensity values $(00000101)_2$,

proach does not justify due to existing scale variant property [10]. In another approach unicity distance was used to determine the maximum number identical used keys for an image authentication scheme [11]. The fundamental works which consider the generic security of perceptual hashing in information theory viewpoint emerge in [1, 12]. Some works also analyze the security problems of the existing schemes individually [13, 14]. A secure framework for general perceptual image hashing also has been proposed in [15].

3 Image Authentication Method based on Applying Hamming Code on Mixed Bits

The proposed method by Chan consists of three procedures including the embedding, the detecting and recovery procedure [2]. It is based on the initial scheme firstly introduced in 2007 [3] where some improvements have been applied. In this section just the recent scheme [2] is recalled and described. The embedding procedure generates the parity check from each pixel intensity value and embed it into another pixel intensity value. In this procedure a Hamming code scheme (Hamming(7, 4)) is used to generate three parity check bits from four most-significant bits of a pixel. To generate the parity check bits, at first the order of the first four most-significant bits of each pixel indicating the data bits is reversed and then a three-bit parity check value is produced. The three-bit parity check value is rotated and embedded into another pixel specified by a transformation. The rotation operation is performed by the use of a sequence of random numbers extracted from a random number generator based on a secret key k_1. Let the image size be $N \times N$, the aforementioned parity check of the pixel P_i with the original bit order J and new bit order J' goes as $J' = (J + R_i) \bmod 3$. For the sake of simplicity the rotated parity check of each pixel is called authentication data. The authentication data bits are embedded into another pixel using the Torus automorphism and Modulus function as follows [2]. Let $P_i = (x_i; y_i)$ be the first pixel to be processed. The next pixel to be processed is specified by Torus automorphism:

$$\begin{bmatrix} x'_i \\ y'_i \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k_2 & k_2 + 1 \end{bmatrix} \times \begin{bmatrix} x_i \\ y_i \end{bmatrix} \tag{1}$$

In the above equation k_2 is the second secret key. The authentication data of pixel P_i is modified using the Modulus function before embedding into the new pixel position $P'_i = (x'_i; y_i)$. In the Modulus function a secret value s of k bits length is embedded in a pixel value y. Let $d = s - (y \bmod 2^k)$, the new value of y denoted by y_0 is computed according to $y_0 = d_0 + y$ where d_0 is defined as follows.

$$d_0 = \begin{cases} d & , \text{ if } -\lfloor (2^k - 1)/2 \rfloor \le d \le \lfloor (2^k - 1)/2 \rfloor \\ d + 2^k & , \text{ if } -2^k + 1 \le d \le -\lfloor (2^k - 1)/2 \rfloor \\ d - 2^k & , \text{ if } \lceil (2^k - 1)/2 \rceil \le d \le 2^k \end{cases} \tag{2}$$

This procedure is continuing by embedding the authentication data of pixel P'_i into another pixel specified by the Torus automorphism and the Modulus function until the

corresponding to the images with semantically identical content are equal or very close to each other. This property addresses the robustness of perceptual image hashing. However, the independence of the hash output for perceptually different images must be ensured [1]. The concept of security in a hash-based image authentication is a challenging issue. It refers to the ability of the attacker to find perceptually different images with almost equal hashes after observing sufficient number of image-hash pairs. Also, it ensures that the secret key can not be compromised and no image hash or watermark can be generated without knowledge about the secret key.

In this paper, the analysis of an interesting proposed code-based image authentication scheme [2] is presented. The proposed scheme is based on the initial work given in [3] whose perceptual hashing algorithm uses Hamming code technique to generate and embed parity bits in the pixels. To provide the security two secret keys are involved in the embedding process. The main contribution of this paper is the analysis of the security aspects of the authentication scheme for further enhancement. In fact it is shown that the engaged keys do not strengthen sufficiently the security to be met by an image authentication mechanism. Furthermore a solution will be proposed and discussed in details. The rest of this paper is organized as follows. A short description on the related works is given in Section II. Section III describes the subjected coding-based image authentication scheme. The analysis of the scheme is given in Section IV followed by the proposed solution in Section V and security discussion in Section VI. Section VII concludes the paper.

2 Related Works

There is a large body of research works in the literature in the field of image authentication. They are categorized according to their construction technique and application. Classification based on the robustness of the scheme is mostly used in the taxonomy of image authentication methods. According to this classification they are categorized into two major groups performing hard authentication and soft authentication respectively [4]. The main techniques in the first group where the robustness and the number of acceptable modifications is limited are based on standard cryptography and fragile watermarking. In the second group of image authentication schemes, the level of robustness is higher than the first group and a wider range of authorized modifications is accepted while the malicious manipulations are supposed to be detected. The main technique in this group is based on the semi-fragile watermarking and content-based signature wherein the semantic content of an image is extracted as a feature in order to generate a digital signature [4, 5, 6, 7, 8]. Despite of a fast progress in extracting and analyzing the image data used in the image authentication scheme, there are relatively less attention to the corresponding security analysis as one of the main pillars in this design. As one of the leading works regarding to this matter, Swaminathan, et.al., [9] proposed to use differential entropy to evaluate the security of some existing image hashing schemes in the literature. Although it was shown later that the proposed ap-

Image Hashing Algorithm: An Analysis and Improvement

Seyed Amirhossein Tabatabaei[1]

[1]*Department of Computer Science, Faculty of Mathematical Sciences, University of Guilan, Rasht, Iran*
amirhossein.tabatabaei@guilan.ac.ir

Abstract

Image authentication code algorithms are schemes wherein the authenticity of an image is considered in a robust war. As the images are mainly subjected to some authorized modifications, such schemes must be able to accept the authorized changes while rejecting the malicious ones. This article analyzes an image authentication algorithm based on error detection code. The image authentication scheme utilizes a type of error detection code in order to encode the mixed most significant bits (MSB) intensity value of each image pixel. The secrecy of system is based on two secret keys. The algorithm provides an acceptable robustness and elaborate design however, it suffers from some security features that leave a gap for improvement. These features are analyzed and will be employed to show the vulnerabilities of the scheme. Also, some solutions are proposed to elaborate the algorithm more. The solutions will increase the strength of the scheme while keeping the robustness.

Keywords: *Image Authentication, Robustness, Image Hashing, Error detection and correction.*

1 Introduction

Appearance of the advanced technologies in multimedia processing techniques like image processing softwares facilitates performing the illegal actions on the digital multimedia object. Violation of image ownership, unauthorized duplication and redistribution and malicious copying and manipulating acts are examples which indicate high demand for image authentication. Image authentication aims to verify the authenticity of images which are subjected to some modification and/or unauthorized manipulation. Image authentication schemes are mainly based on the perceptual image hashing or watermarking techniques. A shared secret key is used in hash generation or watermark embedding process and verification to provide security of the scheme. A perceptual image hashing algorithm differs basically from a cryptographic hash function: the generated hash

Appendix

sample questionnaire: Below is a sample questionnaire used in this article.

1. Do you use a strong password (including uppercase and lowercase letters, numbers, and symbols) for your social media accounts?
A.Yes, always
B.Yes, but not always
C.No, I don't use one at all

2. Is your password for social media accounts up to date and changed periodically?
A.Yes, I regularly change my password
B.Yes, but not regularly
C.No, I never change the password

3. Do you share sensitive information (such as personal information, phone number, home address, etc.) in your social media posts and profile?
Yes, always
Yes, but with caution
No, I don't share sensitive information

4. Do you review attachments you receive on social media (such as files, links, etc.) before opening them?
A.Yes, always
B.Yes, but with caution
C.No, they are ignored

5. Do you use security-related apps and extensions to protect your social media accounts?
A.Yes, always
B.Yes, but with caution
C.No, I don't use them at all

6. Have you ever experienced phishing or attempts to infiltrate your social media accounts?
A.Yes, I have experienced it
B.No, I have never experienced it
C.I don't know what phishing is

7. If you have experienced phishing or intrusion attempts, have you reported it and taken necessary actions to protect your account?
A.Yes
B.No

8. Do you have sufficient knowledge of security measures related to social media account protection?
A.Yes
B.No

9. Do you use public social networks or public accounts for communication and sharing personal information?
A.Yes
B.No

10. Are you knowledgeable about cyber threats and ways to combat them?
A.Yes
B.No

References

[1] S. Y. A. A. M. subhi R. M. Zeebaree, "Social Media Networks Security Threats, Risks and Recommendation: A Case", in International Journal of Innovation, Creativity and Change. www.ijicc.net, 2020.

[2] A. Power, "What is social media?", British Journal of Midwifery, vol. 22, pp. 896-897, 2014.

[3] J. C. Bertot, P. T. Jaeger, and D. Hansen, "The impact of polices on government social media usage: Issues, challenges, and recommendations", Government information quarterly, vol. 29, pp. 30-40, 2012.

[4] S. Norden, "How the internet has changed the face of crime", 1554411 M.S., Florida Gulf Coast University, Ann Arbor, 2013.

[5] C. Konradt, A. Schilling, and B. Werners, "Phishing: An economic analysis of cybercrime perpetrators", Computers & Security, vol. 58, pp. 39-46, 5, 2016.

[6] K. J. Mitchell, D. Finkelhor, L. M. Jones, and J. Wolak, "Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization", Journal of Adolescent Health, vol. 47, pp. 183-190, 2010.

[7] M. Omar Saeed Al, "Threats and Anti-threats Strategies for Social Networking Websites", International Journal of Computer Networks & Communications, vol. 5, pp. 53-61, 2013

[8] Jan Vykopal. A Flow-Level Taxonomy and Prevalence of Brute Force Attacks. In Advances in Computing and Communications, pages 666–675, Kochi, India, 2011. Springer.

[9] A. P. a. M. T. Enrico Franchi, "Information and Password Attacks on Social Networks", in JITR, Italy, 2015.

[10] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios", Computers & Security, vol. 59, pp. 186- 209, 6, 2016.

[11] E. U. Osuagwu, G. A. Chukwudebe, T. Salihu, and V. N. Chukwudebe, "Mitigating social engineering for improved cybersecurity", in Cyberspace (CYBERAbuja), 2015 International Conference on, 2015, pp. 91-100.

type of password, but not always. Additionally, 80% of users update their passwords regularly, but not consistently, while 13.3% never change their passwords.

Regarding sharing sensitive information, 20% of users always share sensitive information, and 40% do so cautiously, while 40% do not share sensitive information at all.

The results indicate that 40% of users always check attachments before opening them, 26.7% do so cautiously, and 33.3% ignore this step.

Regarding the use of security apps and extensions, 13.3% of users always use them, 26.7% use them cautiously, and 60% do not use these tools at all.

Results show that 47.6% of users have experienced phishing or attempted unauthorized access to their social media accounts, while 26.7% of users have not experienced such attacks. Additionally, 26.7% of users are not familiar with phishing and lack sufficient awareness.

Regarding actions taken after experiencing phishing, the results indicate that 53.3% of users reported the incidents and took necessary measures to protect their accounts, while 46.7% of users did not take any actions.

Regarding awareness of security measures related to social media accounts, 53.3% of users have sufficient awareness, while 46.7% lack sufficient awareness.

Regarding the use of public social networks or public accounts for communication and sharing personal information, 46.7% of users use these networks, while 53.3% do not use them.

Regarding awareness of cyber threats and ways to counter them, 20% of users have sufficient awareness, while 80% lack sufficient awareness. These results indicate the need for promoting cybersecurity awareness and increasing users' knowledge about cyber threats.

5 Conclusion

In conclusion, the results indicate that a significant portion of users still lack sufficient awareness regarding cyber threats and ways to counter them. Therefore, increasing user awareness about cyber threats and protective measures on social media platforms requires further efforts from organizations and security-related entities.

By implementing necessary changes in user behavior and attitudes and promoting the importance of security for social media accounts, a considerable improvement in the security of these platforms and a reduction in security breaches and abuses can be achieved. As an initial study, these findings can serve as a motivational factor for conducting further research and taking more practical actions to enhance the security of user accounts on social media platforms.

2.5 Social Engineering

Social engineering is one of the most complex and popular methods of attacking the security of social networks. In this method, the attacker utilizes psychological tricks and social knowledge to prompt users to provide sensitive information and their credentials. With the increasing use of social networks and the importance of personal information in these environments, social engineering has become one of the biggest security threats in these networks [10].

As a deception-based attack, social engineering seeks to persuade individuals to perform inappropriate actions and disclose their sensitive information by exploiting their motivations, needs, and fears. Common social engineering techniques include phishing emails, enticing messages, and unknown phone calls, with the aim of extracting personal information and gaining access to user accounts [11].

To prevent social engineering attacks, users should consider the following:

- Do not trust unfamiliar and suspiciously sent information.
- Avoid sharing sensitive information and personal credentials with unknown individuals.
- Enable two-factor authentication and other security features in user accounts.
- Ensure the validity and reliability of received website sources and messages.

3 Methods

In this study, a questionnaire was used as a tool for data collection. This questionnaire consists of ten main questions presented with options A, B, and C for participants to respond to. The responses to this questionnaire were completed by individuals from the Persian-speaking community in various countries, including Australia, Iran, Afghanistan, and some European countries. The participants in this questionnaire include individuals with different educational levels, including Ph.D., Master's, Bachelor's, and lower levels. Furthermore, the design and collection of responses were conducted online.

In this research, responses from 80 participants were obtained. The questionnaire was distributed randomly among users of social networks such as Facebook, Instagram, and Telegram. After data collection, statistical analysis was performed, and the results were interpreted statistically. The questionnaire used in this paper is available in appendix 1 .

4 Results

The results showed that 53.3% of users always use strong passwords (including uppercase and lowercase letters, numbers, and symbols) for their accounts, and 46.7% do use this

2.2 Combation Phishing

1. Awareness and Education:

   Raising awareness among users about different phishing attacks and educating them on methods to detect deceptive messages and pages can significantly improve the security of their accounts.

2. Detection of Suspicious Links:

   Using tools and software that detect suspicious links and inform users to refrain from accessing suspicious pages [5].

3. Verifying Website Identities:

   Users should carefully verify the identity of websites and only enter sensitive information on official and reputable pages.

4. Software Updates:

   Regularly updating software and operating systems to patch vulnerabilities and potential security weaknesses [7].

2.3 Brute Force

In a brute force attack, the attacker attempts to gain access to the target user's account by using automated methods and extensive trial and error. The attacker tries all possible combinations to discover the user's password. If the account's password is weak and easily predictable, the attacker can easily penetrate the desired account and access the user's personal information, images, and content. Brute force attack is one of the most commonly used methods to infiltrate systems and user accounts and has been employed extensively in the past. From a technical perspective, this attack takes two main forms: brute force attack, which involves trying different combinations word by word, and dictionary-based brute force attack, which uses a list of words to guess the password [8].

2.4 Combatting Brute Force

To prevent brute force attacks, users should use strong and complex passwords that include a combination of uppercase and lowercase letters, numbers, and symbols. Additionally, enabling security features such as two-factor authentication can significantly enhance the security of user accounts. Given the increasing importance of social networks and the information stored in user accounts, it is essential for users and administrators of these networks to be aware of the vulnerabilities and threats posed by brute force attacks and take necessary actions to strengthen the security of these platforms [9].

objective of this scientific article is to examine the vulnerability of social media accounts against cyber-attacks. To achieve this goal, we delve into the analysis of phishing and brute force attacks as two important penetration methods on user accounts, evaluating the security weaknesses of these networks against such attacks. Additionally, we investigate and analyze social engineering as an attack based on deception and psychological manipulation of individuals. Through a comprehensive and reliable questionnaire, we assess users' attitudes and behaviors regarding security measures on social networks. This article emphasizes that users' awareness of cyber threats and countermeasures is key to strengthening the security of social media accounts and safeguarding their personal and confidential information. Given the increasing significance of social networks in modern society and their prominent role in human interactions, we hope that this article contributes to enhancing users' and administrators' awareness of information security and their accounts, ultimately leading to an overall improvement in the security of these platforms.

2 Hack

Hacking is a computer crime that involves using social media websites to gain unauthorized access to computers or digital devices. Cybercriminals can employ various attack methods to gain access to the targeted users' digital devices [2]. They send emails or messages to users of social media sites, and when the user clicks on a suspicious link, the hackers gain unauthorized access to information through hacking [3]. Two types of attacks are commonly used by cybercriminals: targeted attacks and opportunistic attacks. In targeted attacks, hackers use specific tools to attack a particular target, while opportunistic attacks utilize viruses and worms. This type of attack is especially carried out by hackers, spammers, and cybercriminals [4].

2.1 Phishing

Phishing refers to a type of cyber attack where the goal is to gain access to sensitive and important user information through deception and forgery and exploit it for malicious purposes. In this type of attack, attackers encourage users to provide sensitive information such as usernames, passwords, banking details, and similar information by sending deceptive messages or fake websites [4]. Social networks as the primary target of phishing attacks: Given the large number of users and the various personal information shared on social networks, these platforms are considered the primary target of phishing attacks. Attackers typically attempt to persuade users to enter their sensitive information on various pages by sending deceptive links or pages [5]. Consequences of phishing attacks on social networks: Phishing attacks result in the misuse of users' sensitive information. Attackers may use the obtained information for targeting, fraud, identity theft, and other malicious activities [6].

Vulnerability Analysis of Social Media Accounts Against Cyber Attacks

Ahamd Farid Aseel[1], Yashar Abri[1]

[1]*M.Sc. Student, Information Technology Engineering, Faculty of Engineering, College of Farabi, University of Tehran*
faridaseel.4all@gmail.com, yasharabri@ut.ac.ir

Abstract

This article examines the vulnerability of social media accounts against cyber attacks. With the increasing number of users on these platforms and the accumulation of sensitive information in user accounts, the security of these networks is facing cyber threats. The article analyzes phishing attacks and brute-force attacks as penetration methods and investigates the weaknesses of social media networks against these attacks. Additionally, social engineering, as a deception-based and psychological attack on individuals within social networks, is analyzed. Through a questionnaire, users' attitudes and behaviors regarding security measures are evaluated. The results indicate that some users use strong passwords but do not change them regularly, and users' awareness of security practices is inadequate. The security of social media accounts is of utmost importance, and this article emphasizes that increasing users' and administrators' awareness of cyber threats and countermeasures is crucial to strengthening the security of these platforms. The information presented in this article can contribute to enhancing the security of accounts and protecting users' personal information against cyber attacks.

Keywords: *Cyber Attacks, Social Networks, Phishing, Brute Force, Penetration.*

1 Introduction

In the world of digital communications and the widespread adoption of social networks, individuals increasingly utilize these platforms for communication, information sharing, and social interactions. However, with the continuous expansion of user numbers on these networks and the accumulation of sensitive information and user credentials in their accounts, the issue of security and vulnerabilities has become one of the most critical and prevalent concerns. Furthermore, as technology advances and cyber threats escalate, social networks are constantly facing various types of attacks. Attacks such as phishing, brute force, and social engineering are among the methods exploited by malicious actors to infiltrate user accounts and misuse sensitive information [1]. The main

https://www.extrahop.com/company/blog/2019/network-detection-response-vs-intrusion-prevention-systems/ (accessed Apr. 15, 2023).

[25] "NDR and the SOC Visibility Triad | ExtraHop | ExtraHop," www.extrahop.com, 2021. https://tinyurl.com/5n8ejpek (accessed Apr. 15, 2023).

[26] "Point of View." Available: https://www.crowdstrike.com/wp-content/uploads/2021/05/soc-triad-solution-brief.pdf

[27] Nettitude, "The SOC Visibility Triad – SIEM, EDR & NDR | Nettitude," blog.nettitude.com, 2020. https://tinyurl.com/mvuy4mme (accessed Apr. 15, 2023).

[28] I. Cybersecurity Inc., "Dynamic detection for dynamic threats," www.ironnet.com, 2020. https://tinyurl.com/5n89rews (accessed Apr. 15, 2023).

[29] "What is Network Detection and Response?," www.ironnet.com, 2021. https://tinyurl.com/37cct6mh (accessed Apr. 15, 2023).

[30] K. Bissinger, "Darktrace Immune System. Self-learning Detection & Response,"2020. https://tinyurl.com/yzr7u6z4 (accessed Apr. 15, 2023).

[31] K. Bissinger, "Fighting Ransomware with AI," www.n3t.com, 2022. https://www.n3t.com/about-us/blog/fighting-ransomware-with-ai (accessed Apr. 15, 2023).

[32] TechTerms, "SMB (Server Message Block) Definition," techterms.com, 2021. https://tinyurl.com/3mnsa2ft (accessed Apr. 15, 2023).

[33] "About Vectra - AI Driven Cybersecurity Company | Vectra AI," www.vectra.ai. https://tinyurl.com/bhxe967t (accessed Apr. 15, 2023).

[34] FireEye, "What Is SOAR? | Definition & Benefits | Trellix," www.trellix.com, 2019. https://tinyurl.com/muzap5zh (accessed Apr. 15, 2023).

[35] Y. Bari, "Infosys Knowledge Institute | The Future of Tomorrow: Automation for Cybersecurity," www.infosys.com, 2019. https://www.infosys.com/iki/perspectives/future-tomorrow.html (accessed Apr. 15, 2023).

[36] E. Segal, "The Impact of AI on Cybersecurity | IEEE Computer Society," Computer.org, 2020 https://www.computer.org/publications/tech-news/trends/the-impact-of-ai-on-cybersecurity.

[37] P. Donegan, "'Trusted Research, Analysis and Insight in IT & Telecom Security' AI in Cyber Security: Filtering out the Noise," 2019. Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/ycx5nvwj.

[38] Vectra AI, "E-book Prevention Phase Active Phase Clean-up Phase Initial Infection Minding the cybersecurity gap," 2017. Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/nbjrremc.

[9] E. Fossey, C. Harvey, F. Mcdermott, and L. Davidson, "Understanding and Evaluating Qualitative Research," Australian and New Zealand Journal of Psychiatry, vol. 36, no. 6, pp. 717–732, Dec. 2002, doi: https://doi.org/10.1046/j.1440-1614.2002.01100.x.

[10] Rev, "How to Analyze Interview Transcripts in Qualitative Research," Rev, Mar. 30, 2022. https://www.rev.com/blog/transcription-blog/analyze-interview-transcripts-in-qualitative-research.

[11] G. Fernandez, Deep learning approaches for network intrusion detection, M.S. thesis, Dept. Comput. Sci., Univ. Texas at San Antonio, San Antonio, TX, USA, 2019. https://tinyurl.com/3p32m3xt.

[12] P. Uppamma and S. Bhattacharya, "Deep Learning and Medical Image Processing Techniques for Diabetic Retinopathy: A Survey of Applications, Challenges, and Future Trends," Journal of Healthcare Engineering, vol. 2023, pp. 1–18, Feb. 2023, doi: https://doi.org/10.1155/2023/2728719.

[13] J. Li, "Cyber security meets artificial intelligence: a survey," Frontiers of Information Technology & Electronic Engineering, vol. 19, no. 12, pp. 1462–1474, Dec. 2018, doi: https://doi.org/10.1631/fitee.1800573.

[14] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 19–31, Jan. 2016, doi: https://doi.org/10.1016/j.jnca.2015.11.016.

[15] "Gmail," accounts.google.com, 2019. https://tinyurl.com/4prmaw9c (accessed Apr. 15, 2023).

[16] K. Corrie, "Building a Large Scale Machine Learning Based Anomaly Detection System Part 2 Normal Behavior of Time Series Data," www.academia.edu, 2019, Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/yc34t6ac.

[17] K. Corrie, "ULTIMATE GUIDE TO BUILDING A MACHINE LEARNING ANOMALY DETECTION SYSTEM PART 1: DESIGN PRINCIPLES," www.academia.edu, 2019, Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/mswk4br8.

[18] J. Huang, Z. Kalbarczyk, and D. M. Nicol, "Knowledge Discovery from Big Data for Intrusion Detection Using LDA," IEEE Xplore, Jun. 01, 2014. https://ieeexplore.ieee.org/document/6906855 (accessed Apr. 15, 2023).

[19] M. Amrollahi, S. Hadayeghparast, H. Karimipour, F. Derakhshan, and G. Srivastava, "Enhancing Network Security Via Machine Learning: Opportunities and Challenges," Springer Link, 2020. https://tinyurl.com/bddar2tx (accessed Apr. 15, 2023).

[20] I. Humied, Cybersecurity Amazon, 2023. Accessed: Apr. 15, 2023. [Online]. Available: https://a.co/d/44cfZbK.

[21] R. Bhardwaj, "IDS vs IPS vs Firewall - Know the Difference - IP With Ease," ipwithease.com, Sep. 10, 2020. https://tinyurl.com/24pxy4jx (accessed Apr. 15, 2023).

[22] N-able, "Intrusion Detection System (IDS): Signature vs. Anomaly-Based," N-able, Mar. 15, 2021. https://tinyurl.com/37de7vn9 (accessed Apr. 15, 2023).

[23] C. Snyder, "NDR vs. IDS for Intrusion Detection - ExtraHop | ExtraHop," www.extrahop.com, Jan. 23, 2019. https://www.extrahop.com/company/blog/2019/network-detection-response-vs-intrusion-detection-systems/..

[24] C. Snyder, "NDR vs. IPS for Intrusion Prevention, Detection, and Response - ExtraHop | ExtraHop," www.extrahop.com, Feb. 07, 2019.

7 Conclusion

The concept of using AI techniques to defend against future cyberattacks has its pros and cons. As attackers and malicious actors continue to improve their attack methods, there is an urgent need for action. IDS, IPS, SOC, and SOAR systems in use today still rely heavily on human intervention. But with the number of attacks outstripping the effectiveness of traditional reactive rule-based defense techniques, the use of AI technology is the ideal way. AI, especially machine learning (ML), gives detection and response systems the opportunity to be more proactive and form real-time actions. It also improves the collection and analysis of network traffic data to improve the effectiveness of security operations and security teams. Today's AI tools are only useful for a limited number of network and cybersecurity related activities. Future research should focus on ways to facilitate automation of AI solutions while reducing the need for human interaction. Achieving this goal requires more accurate assessments, training datasets, and industry standards. ML and DL techniques also need to better understand the context within datasets in order to make decisions similar to humans and have a low rate of false outcomes.

References

[1] K. Thakur and A.-S. K. Pathan, Cybersecurity Fundamentals: A Real-World Perspective. CRC Press is an imprint of Taylor & Francis, 2020. Available: https://tinyurl.com/3kc6v6f8.

[2] "Cyber Security Education: Principles and Policies," Routledge & CRC Press, 2020. https://tinyurl.com/3dy44cua (accessed Apr. 15, 2023).

[3] D. Edeh, "Network Intrusion Detection System using Deep Learning Technique," www.utupub.fi, Aug. 2021, Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/ywhvx2sy.

[4] "Computer Security Fundamentals, 3rd Edition | Pearson IT Certification," www.pearsonitcertification.com, 2016. https://tinyurl.com/4sx2xsdd (accessed Apr. 15, 2023).

[5] D. Franke, "Amazon.com: Cyber Security Basics: Protect your organization by applying the fundamentals: 9781522952190: Franke, Don: Books," Amazon.com, 2023. https://www.amazon.com/Cyber-Security-Basics-organization-fundamentals/dp/1522952195.

[6] C. Sjöblom, "Artificial Intelligence in Cybersecurity and Network security," 2021. Available: https://www.doria.fi/bitstream/handle/10024/181168/sjoblom_christoffer.pdf

[7] R. Mark and R.-O. Bsc, 2022. Accessed: Apr. 15, 2023. [Online]. Available: https://tinyurl.com/mr2a9myf

[8] S. A. Salloum, M. Alshurideh, A. Elnagar, and K. Shaalan, "Machine Learning and Deep Learning Techniques for Cybersecurity: A Review," Advances in Intelligent Systems and Computing, pp. 50–57, 2020, doi: https://doi.org/10.1007/978-3-030-44289-7_5.

these systems are not intelligent in the sense that they have human-like awareness and knowledge in addressing problems.

Most ML techniques still rely heavily on manual oversight and human interaction. The unsupervised learning techniques have the potential to learn on their own, whereas supervised techniques are limited to certain tasks in the security architecture. The aspirations for a self-learning and decision-making computer have been partially satisfied by unsupervised methods and deep learning techniques, and as previously said, DL techniques have elevated the field of AI to a whole new level.

Future work on AI in cybersecurity should allocate more resources to testing unsupervised methods. It's important to remember that artificial intelligence is still a tool for security teams, not a replacement for human reasoning and problem-solving skills. This can improve the Preventive and automated aspects of security systems, so it is important to further develop AI techniques that understand context.

The AI techniques used in attacks may be more sophisticated than defense, so the challenge going forward will be keeping up with the latest techniques from attackers. Most datasets used to train and test AI systems are not up to date and do not contain enough malicious data points. In order for the chosen AI system to be able to learn what a typical activity actually looks like, and vice versa, the dataset needs to be updated [36]. AI techniques can also be compromised, so it is important to protect the integrity of AI techniques. Compromised data collection combined with compromised AI techniques can lead to erroneous results and prevent security systems from functioning properly [37].

Advances in cybersecurity are driven by knowledge and expertise in the field. These talented workers are in great demand and there is a skill gap in cybersecurity. More people need cybersecurity education and training to create identification systems, improve AI techniques, and develop security measures [38]. This is related to the interpretability of AI features, as the analyst needs to understand how the AI component of the system reaches its conclusions. Developing improved AI also requires a basic understanding of current AI techniques, but progress is hampered by widespread ability deficits. By making AI security solutions intuitive to use and visually compelling for companies and enterprises will adopt AI security solutions on a larger scale. The term "AI" is so widely used that there can be confusion about what a particular AI feature actually does. AI-controlled machines are different from AI-enabled machines.

Fully automated AI-driven solutions are still a concept of the future. The primary goal of most AI solutions is to help analysts make better decisions. Industry standards can be established to measure system autonomy and evaluate AI systems to prevent blind reliance on vendor solutions [37]. Product testing transparency is another issue when implementing AI. There may be human resistance to the paradigm shift towards AI, as there are not many industry norms and standards to rely on.

after business hours. The enterprise immune system detected this within 9 seconds, and after 24 seconds the engine stopped cryptographic operations, fixing the problem without human intervention. Due to the fast response time of the system, only a small portion of the network was slightly damaged. Detection of these threats is easier using unsupervised learning techniques, as demonstrated by the Darktrace case.

5.5.2 Vectra Cognito

Vectra AI company develops an NDR cybersecurity platform with AI-driven attack behavior detection [33]. Vectra Cognito is the name of the proposed system, and it claims that, similar to the enterprise immune system, Vectra AI can learn the system's behavior and capabilities in detecting threats. Instead of using all available network data, Vectra Cognito collects useful enriched metadata to give you a clearer picture of your system. This feature also reduces noise in the data using SIEM and EDR systems.

5.5.3 Security operations, automation, and response technology

A relatively new tool and implementation idea in network and cyber security is Security operations, automation, and response (SOAR) technology. SOAR technology aims to tackle three key aspects of modern cybersecurity. These three aspects include threat and vulnerability management (orchestration), automation of security operations (automation), and incident response (response) [34]. Input from internal and external sources can be accepted into the SOAR system, also improving visibility of network events and traffic flows. The system can automatically respond to situations using SOAR and AI, as well as recommending actions to security operations teams. The task of the orchestration function is to combine and coordinate the automated and manual processes of the information system [35].

6 Results and Discussion

Cybersecurity has made incredible progress over the past few decades, and there are solid examples of how AI has been applied to it. The results of this study show that AI techniques are suitable for cybersecurity. Integrating AI into security and surveillance systems can increase the effectiveness of anomalies and threat detection. It also reduces the number of daily repetitive tasks that work security teams have to perform.

Before adopt an AI technique, companies should assess their current systems to see what problems they face. There were recurring themes in this research that emerged from multiple sources, and most of these issues could be resolved or mitigated using AI techniques. But the term "AI" is used both as a commercial ploy and as a promising hypothesis of a panacea for any problem. Certain artificial intelligence techniques such as NDR have shown promising results in security tasks, but these are mostly machine learning techniques that are not as complex as could be possible. For example,

NDR system uses AI technology to provide businesses with enhanced detection capabilities. Furthermore, ML has given the NDR system the ability to more accurately assess threat levels [29]. It is important to emphasize the complementary nature of triads. Endpoint detection systems require continuous monitoring and maintenance, reducing internal network visibility. NDR uses behavioral analytics supported by ML and AI-based techniques to detect threats propagating and communicating between intranet devices. A more reliable security architecture is created by NDR's real-time monitoring capabilities and EDR's signature-based technology. Additionally, the NRD system uses a cloud-based ML technique to reduce tedious modeling work and reduce system load. In addition, NDR introduces the ability to automatically update its signature database and detection models using machine learning techniques. Real-time network information provided by the NDR component can improve the EDR system's ability to isolate specific endpoints from the network [25].

SIEM systems are a popular method used by companies for security operations because they are effective at recording data. With well-defined parameters for malicious behavior, SIEMs are typically able to detect threats early. Data analysis by SIEM systems leads to a large number of false alarms. This is an undesirable result when using security systems. Due to the large amount of data generated in large organizations, network traffic logging is disabled at certain times of the day or week. As a result, there is a window for attackers to launch attacks and delete or modify previous logs, making attacks difficult to detect. Wire data (network packets) is used in the NDR system to show network communication and paths through the network. Wire data, unlike log data, is immutable, providing SIEM systems with complete and reliable metadata to perform their functions [25].

5.5 Unsupervised learning techniques

In this subsection, we shall present three patented unsupervised learning security techniques.

5.5.1 Enterprise Immune System

The system uses unsupervised learning techniques to detect and block known and unconfirmed malicious network traffic. This method addresses the problem of rule-based systems by learning from data to create models of both normal and deviant behavior [30]. An example shows how the AI component of Darktrace's company solution can detect ransomware attacks in real time and react to them [31]. In one case, an employee accessed a malicious word document via a work email, allowing ransomware to enter the network. The employee's computer started connecting to suspicious external sites and searching for SMB shares. SMB or Server Message Block is a network protocol that allows files to be shared between devices connected to the same network [32]. Additionally, the ransomware can start encrypting SMB shares and have a detrimental effect on the entire corporate network. There were no employees on site as the incident occurred

and cannot be replaced, there are techniques that can address the above issues. Gartner's security operations center visibility triad represents a new development in network security. In the next section, we'll take a look at it.

5.4 Gartner's security operations center Visibility Triad

The SOC Visibility Triad was first mentioned by Augusto Barros, Anton Chuvakin, and Anna Belak in their March 18, 2019 Gartner research paper titled "Applying Network-Centric Approaches for Threat Detection and Response." The rising sophistication of threats necessitates companies to leverage many sources of data for threat detection and response, Gartner says in this note. Composed of three components called SIEM, EDR, and NDR, this idea enhances visibility of network traffic, reduces attack response time, and helps to detect various types of East-West attacks [25, 26].

5.4.1 Security information and event management

A software program called Security Information and Event Management (SIEM) is used to log and collect network data. SIEM brings this data gathered from applications, endpoints, cloud services, and security devices, and collects them in an integrated manner. Threats and events can be classified based on this aggregated data and alerts can be generated based on defined criteria. AI-based UEBA technology is incorporated into SIEM methodology. The process of creating network baselines is more automated using UEBA [27].

5.4.2 Endpoint detection and response

The second component of the visibility triad is endpoint detection and response (EDR) technology. The role of this technology is to detect malicious data and traffic on endpoints such as servers and laptops. EDR uses behavioral analysis on top of traditional antivirus software to detect risky activity [27]. EDR is a complementary technology to SIEM, and the two parts have long served as the foundation of security operations. An endpoint system can detect this behavior and flag it as an anomaly, but the log could be corrupted by an attacker, resulting in the threat not being reported by her SIEM [27]. Security operations personnel can use EDR technology to isolate infected endpoints from the network and prevent lateral spread of threats.

5.4.3 Network Detection & Response systems

The Network Detection and Response systems (NDR) represent a new development in network security and it is the latest addition to the Triad. NDR technology complements here, EDR, and SIEM methods by enabling detection without the use of rules or signatures that govern system operation [28]. By using carefully placed sensors, NDR can monitor east-west communications in addition to monitoring north-south traffic at the network perimeter. Advanced NDR systems can detect novel unknown attacks. The

detect malicious network traffic. Security information and event management systems often combine the output of network resources into hostile activity reports, Security information, and event management (SIEMs). An IDS is one part of a system that includes firewalls and intrusion prevention systems (IPS). However, there are significant differences in the functionality of these components. IPS is similar to IDS, except that the system has the ability to disconnect the network. An IPS is an active, inline threat protection system, often placed right behind a firewall. In contrast to IPS, IDS is a passive system that observes network packets and identifies potentially malicious behavior by comparing signature patterns to predefined typical patterns [20, 21].

There are two types of intrusion detection systems [20, 19]. Both host-based intrusion detection systems (HIDS) and network intrusion detection systems (NIDS) monitor operating system files and network traffic, respectively. NIDS works by distributing sensors throughout the network to monitor network activity. HIDS is a host or device-specific implementation and only tracks traffic on that host or device. Both NIDS and HIDS use two techniques to detect malicious network traffic: signature-based attack detection and Anomaly-based attack identifying.

The basis of signature-based intrusion detection is the identification of identified threats. This technique requires a predefined set of indicators of compromise to scan the traffic for. Byte sequences, file hashes, and email subjects are examples of indicators. When the system identifies a suspicious network activity, it observes the packet, compares it to a database of threat indicators, and flags the packet [22].

The second technique, known as anomaly-based intrusion identifying, uses machine learning techniques. Here, the system uses ML techniques to train the detection engine to detect typical behaviors and create a baseline. This strategy compares network behavior to the norm rather than looking for threats. This means that the system will sound an alarm if the behavior deviates from the norm. This method has advantages over signature-based strategies in that it can detect unknown threats [22]. The majority of surveillance infrastructure and systems use IDS and IPS. Nonetheless, there are some issues that hinder some components of the monitoring task. The primary purpose of IDS is to track north-south network traffic. Client/server traffic entering or exiting a network or data center is referred to as north-south traffic. In other words, IDS can detect risks and anomalies originating from networks outside the organization network. IDS cannot detect attacks inside the network [23].

Lack of visibility into internal network traffic such as Server-to-server or called east-west transmissions are problematic. Moreover, the IDS technique relies on a signing library, so it cannot detect new attack types. Moreover, automated analysis and investigations require human involvement or cooperation with IPS [23]. Like IDS products, intrusion prevention systems have some disadvantages. A large data set generates many meaningless alarms and IPS cannot separate the relevant signal from the noise. To effectively detect threats and anomalies, IPS solutions use signature models that need to be updated frequently [24].

While IDS and IPS technologies are essential components of any security operation

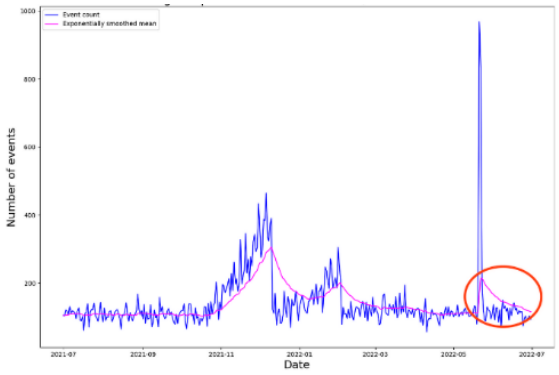


Figure 3: The data points outside of the shaded region are anomaly [15]

Score-based detection assigns a score to the amount by which an identified anomaly deviates from a specified normal norm. Anomalies are ranked according to their scores and can be further investigated. The second method, binary classifies instances as either normal or abnormal [14]. In other words, the system should be able to assess the relevance of anomalies to intruders and react only when necessary. The result is fewer pointless alerts and less manual work for network analysts.

Understanding how metrics are related and how they could stem from the same root cause is a challenge related to the problem of many alarms being active at the same time. Therefore, learning behavioral topology is of great importance in the development of automated systems. Investigating the occurrence of anomalies and determining whether there is a causal relationship between them is one way to detect commonalities in anomalies. The use of clustering techniques is a machine learning technique for determining causality [17]. Clusters can then be represented using the two techniques described earlier (scoring and binary labeling). The Latent Dirichlet Assignment (LDA) technique is a popular candidate for clustering big data. To find the underlying patterns in the data and understand how different sections of the data are related, thematic modeling uses his LDA, a machine learning technique [18]. Often data points are classified as belonging to only one class using clustering techniques. LDA has the advantage that measurements can belong to more than one class and commonalities can be found between them [17]. A strategy for intruder detection using the LDA technique was proposed by Huang et al. [18].

5.3 Intrusion Detection System

Intrusion detection systems (IDS) are one of the best known areas of cybersecurity using ML techniques. This section describes how IDS works and how to create an IDS taxonomy. IDS is a security software that automatically notifies network administrators when hostile activity, system compromises, and security policy violations occur [19]. IDS uses hardware solutions or software embedded in firewalls to monitor networks and

This gives better results when conducting root cause analysis.

Definition of incident is the final design principle to consider. A fully automated system for detection of intruders and anomalies is not yet feasible, so it remains necessary to determine what defines an event. A complete description of the event requires detection of all, or at least most, causes of the anomaly. This works for systems with a limited set of parameters and metrics, which is usually not the case. At this stage of system design, the ML and DL concepts of supervised, unsupervised, and semisupervised learning should be considered. Supervised methods are appropriate when some measures are clearly specified and the goal of the system is to provide classification or regression. For these techniques, to establish a baseline of typical behavior, the training data needs to be tagged. This technique is not very effective at detection new intruders or anomalies due to supervised learning-based anomaly detection training models.

Unsupervised learning is a valid strategy in most cases because it can be difficult to predict all possible situations. An unsupervised procedure identifies anomalies whenever the investigated data deviates from the trained model, and the system gradually learns typical system behavior. The training dataset is unlabeled, so the system can detect new incidents, whether known or unknown. The success of unsupervised learning depends on how accurately and completely the behavior of a typical system is described. This makes the training phase essential as it sets the thresholds and the framework within which the technique operates. Combining these two techniques creates a better methodology.

This is achieved through semisupervised learning. Here, the technique trains on a sparse set of labeled data to understand the input structure. Combining supervised and unsupervised techniques often gives the best results for anomaly and intruder identifying. Intrusion and anomaly automation fundamentally relies on the notion of normal or abnormal behavior. Any approach for detecting anomalies generally works by gathering data, determining what is normal, and then using a statistical test to determine if any subsequent data point in the same time series is normal or abnormal. Such as the shaded region in Figure 3. Below was created as a result of such statistical analysis. So, we might use statistical tests to identify any data point outside of the shaded region as abnormal and any data point of it as normal.

The input data for the network is often very large, but it can also be unpredictable and nonlinear. Combining several different models is a more reliable option to create a correct baseline, as it is impossible to simulate typical behavior. Seasonality is an important factor to consider when creating baselines, and failure to do so can result in contextual anomalies. Second, because ML and DL techniques periodically update new normal values based on incoming data, anomalous data points are subject to the fact that they change the baseline and to prevent or produce erroneous results in the future, it should be given less weight [16].

Output rendering in anomaly and intrusion detection is often problematic. The significance of an anomaly should be expressed in some way when designing an detection system to determine how far an anomaly deviates from the normal and how the system should respond. Scoring and binary metrics can usually be used to label anomalies.

significantly slows the incident response time. Manually setting thresholds on selected metrics is another way to detect anomalies. This technique relies on alerts being sent when metric measurements deviate from thresholds. Setting the thresholds correctly is essential for this strategy to work, but it can be difficult even for small networks as there are hundreds of measurements and functions to consider. Setting the threshold too high or too low will increase the number of false positives. Anomalies can also go unnoticed if the limit constraints are not specified correctly [15].

Several participants pointed out problems with real-time information and expressed a desire to further automate the anomaly detection process in the future. There are five key design elements that must be considered throughout the planning phase of an ML-based automated anomaly detection system [15]: Event timeliness, scale, rate of change, conciseness, and definition of incident.

The Event timeliness deals with the question of how quickly anomalies must be discovered. Alerts for attacks, threats, and identified dangerous network activity are part of real-time anomaly identifying. Enterprises should be aware of this factor as it influences the choice of which type of ML technique to apply and the tasks and goals for which it is used.

The infrastructure and execution of detection systems are highly dependent on scale and data amount. Different monitoring activities use different record sizes. In this case, it is important to examine whether the system works with large amounts of data or small amounts of information. ML and DL techniques react differently to data volume and labeling, or lack thereof, so the planning of the system is affected.

Rate of change is the rate of change of the measured data. Change rate affects the ML or DL technique used for a task, depending on the metric being monitored. Systems may experience frequent changes in measurements during network monitoring, so to work effectively, techniques must include adaptive properties.

Conciseness is the idea that a large number of measurements and factors should be considered when detection anomalies. This concept helps provide users and systems with a comprehensive view of the root cause of anomalies. Often, looking at just one measure doesn't tell the whole picture. For example, a system upgrade in one region may cause delays in another region. The conciseness of ML anomaly detection system can be a technique in three different ways. Each system metric is used by Univariate Anomaly Detection to create a map of typical behavior.

This technique scales easily because each instance is handled independently. Root cause analysis is not possible with this technique, and many anomalies are generated by one unexpected event affecting multiple metrics simultaneously. Multivariate anomaly detection takes multiple inputs and analyzes them together. We combine these metrics to create a virtual event model. This has the disadvantage that the anomaly output does not indicate the parameter that caused the anomaly. In order for the system to have the required computing power, the input signal types must be identical. The hybrid technique of these two methods takes a univariate single metric technique, but explores the relationships between anomalies rather than grouping many of them in a black box.

Staff College - Higher Military Academy discussed the administration of the system. Clear management and well-defined goals are necessary for the continued growth of the monitoring and security system in order to enhance the system.

5.2 Solutions and current techniques

As a part of my task at the workshop, I had to find and present AI-based solutions and techniques. The purpose of this section is to propose solutions and current techniques to the problems brought up by the participants. This section describes the design principles needed to create an ML-based recognition system and the factors that need to be considered. One of the main themes of the workshop was how to move from reactive to proactive action, so planning for systems should be emphasized. Moreover, the role of intrusion detection systems (IDS) and intrusion prevention systems (IPS) in network security and monitoring is discussed. Some typical surveillance systems use AI. IPS and IDS concepts and technologies are moving towards so-called Network Detection and Response NDR systems. Therefore, in the next subsections, we will discuss how to develop detection, response systems and AI-based strategies to address many of the issues raised at the talks. Together with AI-enhanced security operations, this section also discusses unsupervised learning techniques.

5.2.1 Machine Learning Anomaly Detection Systems

Today, any agency must regularly analyze its network data for trends. A large part of network monitoring is finding anomalies. A data analysis process called anomaly detection looks for unusual and irregular patterns in data. Deviations from standard network behavior and their identification are essential so that network administrators can take action and respond to attacks and hacking attempts. AI can be used in this process. Anomalies can be classified in different ways, depending on the type of anomaly and the context in which it is examined. A particular data point or instance that appears to deviate from the typical metric value of the dataset is called a point anomaly. Contextual anomalies are anomalies caused by the specific context and facts of a situation. For example, some periods or seasons are expected to deviate from typical data behavior. However, if this occurs outside the expected time frame, it is considered an anomaly of context. Groups of data instances that collectively deviate from normal network behavior are collectively referred to as collective anomalies. A single anomalous result is not considered an anomaly in this scenario [14].

Manual techniques are still commonly used to detect anomalies. A weekly reviewed dashboard is a popular way to monitor a network. Personnel monitoring the network watch for spikes and dips in traffic, her activities and see if they are abnormal. This method is limited to the original collection of measurements and is difficult to scale. This method can detect large anomalies, but may not easily detect small anomalies. Many attacks today are more scattered and short-lived, so the system may not even know what to look for. Reviewing the dashboard after an anomaly has already occurred

endpoint data and more real-time network traffic statistics. Participants made these suggestions to increase the effectiveness of their Workshop outcomes.

The first four participants brought up the visibility of network data. The data relevance and relevance of pertinent information about network traffic and networked devices are closely tied to the visibility issue. Directors of Information Systems bring up these kinds of problems. The collecting and analysis of data traveling inside the network as well as into and out of the network constitutes visibility in terms of network monitoring. East-west traffic is a term used to describe traffic that travels from one server to another inside a network.

Director of Information Systems and his two employees and Assistant Undersecretary for Technical Affairs at the Ministry of Communications and Information Technology raised concerns about lateral or east-west traffic monitoring. Around half of the participants brought up visibility-related issues. The fact that participants from other teams or agencies also mentioned this issue demonstrates the broad impact the visibility issue has. This makes it quite evident that in order to address this in the future, suitable solutions and action must be taken. An organizational network's visibility is essential in many ways. Visibility of network data is essential in a setting where the frequency of cyberattacks is rising.

Real-time network data and information were the second most common issue of the workshop. Real-time data is crucial because it enables monitoring and security teams to respond to threats and anomalies more quickly. Director of Information Security - General Post Authority and Assistant Undersecretary for Technical Affairs at the Ministry of Communications and Information Technology raised this issue. This problem is especially worth detection and recognizing because they have diverse job descriptions and duties.

Other top priorities are problems with alert processing and alert accuracy. The importance of alert accuracy makes issues with it a typical occurrence in network monitoring. More automated detection techniques have a byproduct of false positives and false negatives. This topic was only mentioned by one person (Director of Monitoring and Control - Public Telecommunications Corporation). Yet, this does not imply that the problem is unimportant, and the accuracy of the alerts is a crucial component of any security monitoring system. User and Entity Behavior (UEBA) can offer solutions to improve alert, confidence, and accuracy.

The monitoring procedure, including feature selection, still involves several manual chores, according to Director General of Cisco Academy. The application and use of DL to this problem is possible.

A few more themes that cannot be resolved by AI were also raised by the attendees. Finding solutions that are carried out internally was a prevalent subject that came up in the workshop. This gives the business more control over the design and system infrastructure. Regarding monitoring, this helps the agency to find solutions to issues more quickly without having to wait for input from providers. Director of the College of Postgraduate Studies - Police Academy and director of the Command and

raised by the participants. Respondents said that additional monitoring and carefully selected tools designed for the specific problem would be the answer. The idea behind the recommended technique was to streamline surveillance activities and increase their effectiveness.

Director of Information Security - General Post Authority: a key point for the participant in this conversation, also related to data visibility. According to the person, data about anomalies under investigation may lack relevant information, so one remedy is to learn more about the causes and underlying problems of anomalies. Custom development is another key component of network monitoring that the participant pointed out. According to the participant, this makes it easier to match the infrastructure with the authority's needs.

Director of Monitoring and Control - Public Telecommunications Corporation: this participant raised the possibility of improved alarm handling and alarm accuracy. Participants hope that in the future, incident managers will take a more active role in building and improving surveillance systems, resulting in more reliable system output and more accurate warnings. This participant suggested intelligent monitoring and creating easy-to-understand dashboards that monitoring teams could use as tools.

Director of the College of Postgraduate Studies - Police Academy and director of the Command and Staff College - Higher Military Academy: These two participants emphasized the management aspect. They noted the importance of clearly assigning and delegating responsibilities for various aspects of the monitoring and security process. In-house skills were also a factor, they said, and felt that this strategy should be promoted in the future. It was determined that some planned software improvements would require major hardware refreshes, which is neither feasible nor beneficial from a cost-effectiveness standpoint. Another technical issue was the difficulty or impossibility of linking the colleges' specific software to other system security colleges.

Director General of Cisco Academy - General Institute of Communications: this participant pointed out that some monitoring tasks and root cause analysis are still done manually. According to this participant, more automated techniques for detection of anomalies would be the solution to this problem. Participants specifically recommended that automatic feature selection can reduce some human effort. Participants also expressed a desire for staff to receive additional training on surveillance-related responsibilities in the future. According to the participant, one of the possible remedies, he said is skill certification, which will enhance the overall oversight process.

Director of Information Systems - TeleYemen Company: according to this participant, the existing system is too passive. This individual was interested in how AI could increase the aggressiveness of network monitoring systems and how AI-based systems could provide more real-time data and information. Attendees were also interested in AI-based products on the market and how they can be used to help companies.

Information Systems Consultant - General Post Authority: this participant found that some devices connected to the internal network did not have enough information during their daily work. Future solutions this participant hopes will include richer

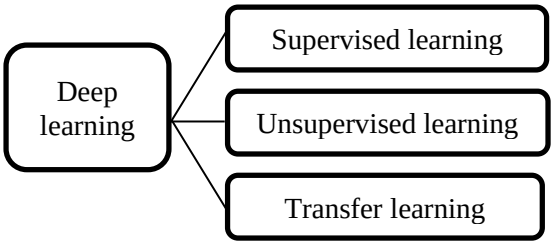


Figure 2: a taxonomy diagram of the deep learning algorithms [8]

5 Analysis, solutions and current techniques

This section presents analysis of workshop discussions, and possible solutions and current techniques which we can used.

5.1 Analysis of workshop discussions

In this subsection, a description of the discussion and notes taken during the workshop and the individual meetings of participants after that.

Director of Information Security - Yemen Mobile Company: this participant claimed that lack of visibility of network data was the biggest problem with network monitoring. Although no specific solutions were presented in this workshop, participants were intrigued by the potential application of AI to detect anomalies. We also explored what changes and adjustments should be made to existing networks to facilitate automation of anomaly detection anomalies.

Director of Information Systems and his two employees - Ministry of Communications and Information Technology: also, these respondents raised the concern of data visibility. Latitudinal mobility and methods for spotting potential assaults and threats inside the network were the specific types of network visibility that were covered. After they have gained access to the network, attackers exploit lateral movement to penetrate farther. One respondent mentioned a number of technologies, including security operations, automation and response technology, and Network Detection and response systems. According to the three respondents, these kinds of technologies were important for the ministry 's upcoming network security and monitoring goals. Moreover, skill certification was listed as a potential upgrade for the future.

Assistant Undersecretary for Technical Affairs at the Ministry of Communications and Information Technology: the topic of data visibility was also brought up by this participant. He claimed that the technology used does not provide real-time insight and alerts on network anomalies and risks. Endpoint detection technology and the potential to improve the monitoring process were mentioned by the respondent. Interesting topic he is one. He said researching techniques to increase the visibility of lateral movement and the hazards it poses will be another important feature in the future. Members of the Teaching Staff - Higher Military Academy: the issue of network visibility was also

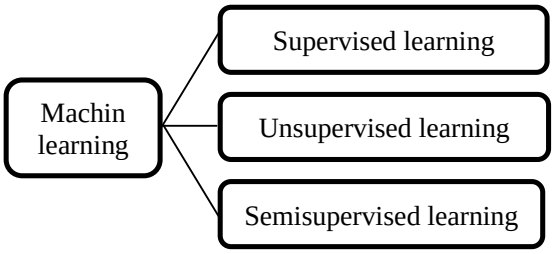


Figure 1: a taxonomy diagram of the machine learning algorithms [8]

cussion about AI due to the lack of specific AI expertise among most of participants. In hindsight, this was not ideal, as a more complete explanation of AI technology and how to use it would have been very helpful. I had no access to or training in network monitoring tools, this was another limitation for the study.

3 Machine learning techniques

The question whether a general-purpose computer should look at data and generate rules rather than relying on humans to generate them was raised by Alan Turing's assertion that computers can learn and determine their uniqueness. Techniques that can learn from data and adapt are called machine learning techniques. Machine learning techniques are created to generate results based on what is learned from the data and examples. For example, such techniques will allow a computer to select and perform certain innovative traffic detection tasks without explicit instructions [11].

Machine learning can be effectively used to perform automated evaluation of attacks and security events such as spam emails, user identification, social media analysis, and attack detection [3]. Supervised, unsupervised, semi-supervised, and reinforcement learning are the three primary methods used in machine learning. Supervised learning is based on labeled data, unsupervised learning is based on unlabelled data, and semisupervised learning is based on both [12], as shown in Figure 1.

4 Deep learning techniques

The main difference between these two methods is feature selection. Unlike ML, where selection must be done manually, feature selection in DL is automated. The goal of DL techniques is to better understand the input data and extract data qualities that are difficult for humans to perceive [13]. Machine learning methodologies are also utilized in deep learning. owever, other ways are employed in deep learning, such as Transfer Learning [8], as shown in Figure 2.

in place and how they can be used for network security. Intrusion detection systems are getting better at detection and remediating anomalous activities and potential threats as more AI techniques are integrated into computer security. Finally, the study seeks to shed light on the obstacles hindering the continued growth of the use of AI tools in cybersecurity and the prospects for AI in this area.

This research starts by descript machine learning techniques and deep learning techniques. In the next section, the presents analysis, possible solutions and current techniques from the workshop conducted and the individual meetings of participants after that are presented. Finally presents the discussion and conclusion.

2 Methodology

Literature research and workshop results were used as research methods in this research. A general literature review was conducted to learn more about the field of AI and cybersecurity. The literature survey first aims to provide an overview of artificial intelligence and various cybersecurity practices. Then, in the background, we discuss the theory of machine learning and deep learning; and how these techniques can be used to detect intruders and attacks. On November 3, 2020, in the meeting room of the Ministry of Communications and Information Technology, a workshop was held with the participation of thirteen responsible and specialists from several government and private agencies, which its results were used as a second technique in this research. During this workshop and the individual meetings of the participants after that, a discussion occurred to detecting concerns about network security and monitoring; and suggestions for improvement. Thus, this research includes potential AI-based remedies for identifying issues.

This study used qualitative research as a methodology. The focus is on individual and group actions and perspectives. Subjective opinions and observations often form the basis of qualitative research, there may not be many participants at the workshop, but a lot of information flows and enough data are collected to answer the questions. It is important that participants are suitable for the study and are carefully selected [9].

In qualitative research, a deductive technique involves a thoughtful, predefined rationales with clear connections between research and meetings. Thematic content analysis and narrative analysis are her two subsets of the inductive technique. looking for recurring themes and patterns in the material collected from participants. Participant comments are analyzed and the most important findings are highlighted [10]. A thematic content analysis technique was chosen for this study.

The first part of the workshop focused on the current network and security monitoring tasks and the types of activities each participant performs on a regular basis. Participants were then asked about the types of problems they encountered in performing their duties and how those problems affected the monitoring and security elements. Suggestions for improvement were also considered. I wrote down the problems and suggestions for improvement, then typed it up. It is difficult to have a general dis-

or connections. It is sometimes called computer security or information technology security. In addition to preventing harmful attacks, unauthorized access, and other harm, the objectives are to guarantee the data's integrity, availability, and confidentiality [1, 2].

Most of our computer systems and network infrastructure are connected via the Internet. Virtually all businesses, governments, and even individuals today rely on cybersecurity to protect their data, grow their businesses, and protect their personal information. People send and receive data over the network infrastructure. Routers are vulnerable to external hacking and tampering. Big data has emerged as a result of increased data volume and complexity due to increased internet usage. Due to the constant growth of the Internet and the amount of data it contains, it has become necessary to develop a reliable intrusion detection system. The network security subset of cybersecurity protects networked systems from unwanted activity. Networked computers become available to ensure data confidentiality, integrity, and accessibility. Current cybersecurity research focuses on developing reliable intrusion detection systems that can detect both known and new attacks and threats with high accuracy and minimal false alarm rates [3].

The most commonly used rule-based systems today are used to implement cybersecurity. The method used to teach a system rule to understand how to process, store, and sort data is called a rule-based system. The system manufacturer or vendor implements the rules. Rules can often be changed by updates. In the event of an attack, the system searches through a set of rules to find the correct answer. If no action is taken to counter a particular attack, the system should be shut down. The designer then has to detect the problem and manually fix the system with a patch or software upgrade [4, 5].

Rule-based systems are not amenable to modification and customization, resulting in a very high rate of new attacks and variants of the same attack. The tedious remediation process of these stubborn attacks takes a lot of time and effort, reducing production and efficiency. Addressing these issues requires designing systems that can adapt to their environment, learn from experience, and change rules to counter future adversarial attempts. This means that the system can patch itself and figure out how to fix vulnerabilities on its own. Additionally, the system can track past attacks and rebuild the system based on newly created rules [6].

To solve the above problems, cybersecurity can use artificial intelligence (AI). Cybersecurity products based on artificial intelligence have become more popular and have evolved rapidly over the past decade. The expansion of these technologies will improve the effectiveness of cybersecurity-related tasks and reduce the frequency and risk of security breaches [7, 8].

The purpose of this research is to show how cybersecurity can be advanced by systems and techniques based on artificial intelligence. There are many facets to AI, and this study does not explore them all. Moreover, there are so many types of attacks that it's impossible to cover them all here. The main purpose is to see real systems already

Improving Cybersecurity Systems Using Artificial Intelligence Techniques

Ismail A. Humied[1]

[1]*Associate Professor, Faculty of Police, Policy Academic, Ministry of Interior, Sana'a, Yemen*
dr.ismail_humied@yahoo.com

Abstract

Cyberattacks and threats are in complexity every day. With the number of attacks growing every day around the world, there are a variety of methods and strategies for penetrating business systems and individual devices. Individual attackers, organizations, and whole nations are responsible for these attacks. Attack resources are growing and cyberattacks can have severe global impact and consequences. These variables make it difficult for security teams to keep pace, so smarter solutions are needed. This research provides an overview of how two areas of artificial intelligence (AI), machine learning and deep learning, can be used to meet cybersecurity challenges. The research can also show how existing AI technologies can improve cybersecurity. Security systems can use AI to automate time-consuming manual security operations and make detection and response more proactive and predictive. As part of this research, a workshop was held with official from government and private agencies, who are responsible for network monitoring and security. During this workshop, a discussion occurred what problems individuals had at work. Thus, this research includes potential AI-based remedies for identifying issues.

Keywords: *Artificial Intelligence, Machine Learning, Deep Learning, Cybersecurity, Cyber-attacks, Cybercrime, Detect.*

1 Introduction

Computers are indispensable in today's workplace and daily life. The development and spread of modern technology have increased the need for information security. The amount of data collected is enormous and is constantly being driven by commercial, military, financial, medical, and government applications. This highlights the importance of cyber security. The term "cybersecurity" is widely used and is an issue that we must constantly address and move forward. Cybersecurity is the process of protecting data and information on networks, mobile devices, computers, and other electronic devices

.

English Full Papers

.

Table of Authors

Table of Papers

.

Proceedings of
The First Conference on Cyberspace (CYSP 2023)
Organizer: University of Tehran

Preparation: *Kazim Fouladi-Ghaleh*
with: *Hussein Azimi, Alireza Zeini*

Publisher: Faculty of Engineering, College of Farabi, University of Tehran
Printing: Matris Publishing Co.
Publishing Year: 2023

Secretariat Address: Faculty of Engineering, College of Farabi, University of Tehran, Old Qom-Tehran Road, Qom, Iran, Postal Code: 3718117469.
Telephone: 025-36166651
Fax: 025-36166652
E-mail: `cysp.conf@ut.ac.ir`
Web: `http://cysp2023.ut.ac.ir`
Messengers: `@cysp_conf`
All links in one: `http://conf.cysp.ir/links`

بسم الله الرحمن الرحیم

IN THE NAME OF ALLAH

CYSP 2023

The Second Conference on Cyberspace

Proceedings

ISC Islamic World Science Citation Center 02230-21686

University of Tehran

31 Oct., 1-2 Nov. 2023

CYSP 2023

THE SECOND CONFERENCE ON

CYBERSPACE

Proceedings

دهمین سال

تأسیس دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران

قم، ابتدای جاده قدیم تهران، دانشکدگان فارابی دانشگاه تهران، دانشکده مهندسی

تلفن: ۰۲۵-۳۶۱۶۶۶۵۱

Faculty of Engineering, College of Farabi, University of Tehran, Old Qom-Tehran Road, Qom, Iran

Phone Number:(+98-25)36166651

Website: http://cysp2023.ut.ac.ir

E-mail: cysp.conf@ut.ac.ir

Instant Messengers: @cysp_conf