

CYSP  
2022



نخستین  
کنفرانس  
فضای ساینس  
مجموعه مقالات



دانشدگان فارابی دانشگاه تهران، قم، ایران

University of Tehran, College of Farabi, Qom, Iran

۱۰ تا ۱۲ آبان ۱۴۰۱

1-3 November 2022

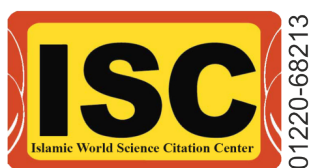


بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

CYSP  
2022



نخستین  
کنفرانس  
فضای سایبر  
مجموعه مقالات



دانشکدگان فراهی دانشگاه تهران، قم، ایران

۱۰ تا ۱۲ آبان ۱۴۰۱

---

### مجموعه مقالات

نخستین کنفرانس ملی فضای سایبر (CYSP 2022)  
برگزار کننده: دانشگاه تهران

تدوین: کاظم فولادی قلعه  
با همکاری: حسین عظیمی، علیرضا زینی، محمد جواد خدمتی، علی لکزایی، امیرمحمد خسروی، سید رضا مسلمی،  
مهدی حسومی، علیرضا میرزایی، محمدعلی شکوهیانزاد

ناشر: دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران  
چاپ و صحافی: ماتریس  
سال انتشار: ۱۴۰۱

---

نشانی دبیرخانه: قم، بلوار دانشگاه، دانشکدگان فارابی دانشگاه تهران، دانشکده مهندسی

کد پستی: ۳۷۱۸۱۱۷۴۶۹

تلفن: ۰۲۵-۳۶۱۶۶۶۵۱

فکس: ۰۲۵-۳۶۱۶۶۶۵۲

ایمیل: [cysp2022.conf@ut.ac.ir](mailto:cysp2022.conf@ut.ac.ir)

وبسایت: <http://cysp2022.ut.ac.ir>

پیامرسان و شبکه‌های اجتماعی: @cysp\_conf

همه‌ی پیوندها در یک جا: <http://conf.cysp.ir/links>

---



CYSP  
2022

THE FIRST CONFERENCE ON  
CYBERSPACE

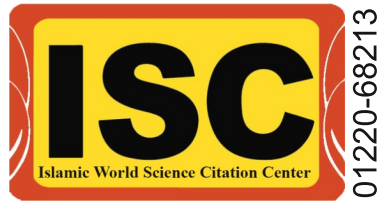
فضای سایبر  
نخستین  
کنفرانس



۱۴۰۱ آبان ۱۴ - دانشکده مهندسی دانشکدهان فارابی دانشگاه تهران

## Scientific Sponsors

## حامیان علمی



## Organizational Sponsors

## حامیان سازمانی



## Media & Publication Sponsors

## حامیان رسانه‌ای و نشر



پیام‌رسان  
گپ



صدای پیام‌رسان



سبک‌آستانه نور



پیام‌رسان  
آی‌گپ

## اعضای کمیته اجرایی

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. دکتر حسین آقابابا، استادیار، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: دبیر اجرایی
۴. دکتر امیرحسین کیهانی پور، استادیار، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول نشست‌ها و کارگاه‌ها
۵. دکتر احمد علی نژاد، استادیار، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور دانشجویی
۶. مهندس محمدعلی شکوهیان راد، پژوهشگر ارشد آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران و مدرس مدعو دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول ارتباطات

## همکاران کمیته اجرایی

۱. علی لک زائی، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور مقالات
۲. علیرضا زینی، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول چاپ و انتشارات
۳. محمدجواد خدمتی، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور رسانه و خبرگزاری
۴. میلاد محمدی، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور چندرسانه‌ای و بخش زنده اینترنتی
۵. حسین عظیمی، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور نمایشگاه جانبی
۶. امیرمحمد خسروی، دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران: مسئول امور پذیرش و تشریفات

## اعضای کمیته علمی

۱. دکتر سروناز تربتی، استادیار، دانشگاه آزاد اسلامی
۲. دکتر سید محمدباقر جعفری، دانشیار، دانشگاه تهران
۳. دکتر حامد جلالی بیدگلی، استادیار، دانشگاه صنعتی اصفهان
۴. دکتر سید محمد جولائی، پژوهشگر، دانشگاه تهران
۵. دکتر مهدی چمپور، استادیار، دانشگاه صنعتی قوچان
۶. دکتر سید احمد حبیب‌نژاد، دانشیار، دانشگاه تهران
۷. دکتر سید نصیب‌اله دوستی مطلق، استادیار، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی
۸. دکتر محمدجواد شایگان‌فرد، دانشیار، دانشگاه علم و فرهنگ
۹. دکتر محمدحسن شیرعلی شهرضا، استادیار، دانشگاه صنعتی امیرکبیر
۱۰. دکتر سید امید فاطمی، دانشیار، دانشگاه تهران
۱۱. دکتر کاظم فولادی قلعه، استادیار، دانشگاه تهران
۱۲. دکتر مسعود کوثری، دانشیار، دانشگاه تهران
۱۳. دکتر مهدی کارگهی، دانشیار، دانشگاه تهران
۱۴. دکتر علی اصغر کیا، استاد، دانشگاه علامه طباطبائی
۱۵. دکتر امیرحسین کیهانی‌پور، استادیار، دانشگاه تهران
۱۶. دکتر محمود مختاری، استادیار، دانشگاه شهید بهشتی
۱۷. دکتر زهرا موحدی، استادیار، دانشگاه تهران
۱۸. دکتر عبدالرضا نوروزی چاکلی، استاد، دانشگاه شاهد
۱۹. University of Basel, Professor, Dr. Christoph Stückelberger

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



دکتر محمدعلی زلفی گل

۹ آبان ۱۴۰۱

بسم الله الرحمن الرحيم

محضر همه‌ی مدعوین نخستین کنفرانس فضای سایبر، به ویژه میهمانان بین الملل این رویداد علمی سلام عرض می‌کنم و آرزو مندم 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 مناسبی ست تا استادان و پژوهشگران محترم حوزه‌های مختلف، مطالعات، دستاوردها و آخرین یافته‌های علمی خود را با یکدیگر به اشتراک گذارند.

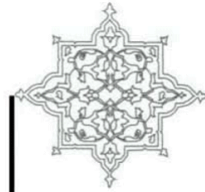
لازم می‌دانم مراتب سپاس و قدردانی خود را از همه‌ی استادان، پژوهشگران، دبیران علمی و اجرایی و عوامل برگزاری رویداد، اعلام دارم و امیدوارم دوره‌های بعدی این کنفرانس نیز با شکوه هر چه بیشتر برگزار شده و آثار آن سال به سال در نظام تصمیم‌سازی و حکمرانی کشور و سایر امور به‌طور فزاینده ملاحظه گردد.

بسمه تعالی

تاریخ: ۱۴۰۱/۰۸/۰۹

شماره: ۲۲۸۰۳۳/و

پوست: \_\_\_\_\_

جمهوری اسلامی ایران  
وزارت علوم، تحقیقات و فناوری

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

بسم الله الرحمن الرحيم

محضر همه‌ی مدعوین نخستین کنفرانس فضای سایبر، به ویژه میهمانان بین‌المللی 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 اتمام 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 به تعبیر 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 مناسبی است 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 تصمیم‌گیری و حکمرانی کشور و سایر امور به‌طور فزاینده ملاحظه گردد.

محمدعلی زلفی گل  
وزیر علوم، تحقیقات و فناوری

شماره پیگیری

۹۸۰۲۹۲۷



نشانی:

تهران شهرک قدس  
میدان صنعت، خیابان  
خوردین، خیابان هرمزان  
نبش خیابان پیروزان جنوبی  
کد پستی: ۱۴۶۶۶-۶۴۸۹۱  
شماره تلفن: ۸۲۲۳۱۰۰۰  
سندوق 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.

فضای سایبر، فضایی است که اطلاعات در آن به گردش در می‌آید؛ اما این گردش اطلاعات به صورت 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 فضا است 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.

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 بین‌رشته‌ای 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. 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، نخستین کنفرانس ملی فضای سایبر توسط دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران با محوریت «آزمایشگاه پژوهشی فضای سایبر» در تاریخ ۱۰ تا ۱۲ آبان ۱۴۰۱ 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. 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، ان شاء الله.

## 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
- جنگ سایبری، جنگ در فضای سایبر، جنگ به‌وسیله‌ی فضای سایبر
- قدرت سایبری، فضای سایبر و حاکمیت
- حکمرانی فضای سایبر، حکمرانی بر فضای سایبر، حکمرانی با فضای سایبر
- 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
- سیستم‌های سایبر-فیزیکی و اینترنت اشیا، 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
- واقعیت ویرچوآل و واقعیت افزوده، متاورس و زندگی دوم
- سایر موضوعات مرتبط



## نشست‌های تخصصی و کارگاه‌های آموزشی

کد نشست	زمان	نوع نشست	عنوان	سخنران / ارائه‌کننده	برگزار کننده
۱-الف 1A	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	نشست تخصصی	روان‌شناسی فضای مجازی از شناسایی تا درمان	دکتر فاطمه علوی اصیل	کنفرانس ملی فضای سایبر
۱-ب 1B	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	نشست تخصصی	پلتفرم مشترک دولت دیجیتال (دانش‌بنیان)	محسن شکوری مقدم، حمیدرضا حسینی، بریر خوشینی‌ها، سید احمد صوفیاف، محمدمامین شکوری مقدم	شرکت فناوری اطلاعات ایده گستر
۱-ج 1C	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	کارگاه آموزشی	امنیت وب (۱)	مهندس فرهاد علی محمدی	آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
۱-د 1D	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	نشست تخصصی	موج اتفاقات اخیر از دیدگاه تحلیل کلان‌داده‌های شبکه‌های اجتماعی (پیام و بروس)	دکتر حسین رحمانی فاضل	کنفرانس ملی فضای سایبر
۱-ه 1E	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	نشست تخصصی	بیانیه سایبری ستاد کل نیروی مسلح از منظر حقوق بین‌الملل	دکتر محسن نیک بین	دانشکده حقوق دانشکدگان فارابی دانشگاه تهران
۱-و 1F	سه‌شنبه ۱۳:۳۰ تا ۱۵:۱۵	نشست تخصصی	تبیین الزامات کلان فقهی حکمرانی فضای سایبر	آیت‌الله محسن اراکی	پژوهشگاه فقه نظام دانشکده اصول الدین

کد نشست	زمان	نوع نشست	عنوان	سخنران / ارائه‌کننده	برگزار کننده
۲-الف 2A	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	نشست تخصصی	روان‌شناسی سایبری و سلامت الکترونیکی	آقای حجت حاجی محمدی یزدی	کنفرانس ملی فضای سایبر
۲-ب 2B	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	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
۲-ج 2C	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	کارگاه آموزشی	امنیت وب (۲)	مهندس فرهاد علی محمدی	آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران
۲-د 2D	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	نشست تخصصی	گفتمان‌های مواجهه با فضای سایبر	حجت‌الاسلام محمد کرباسی	فمتا (فضای مجازی تراز انقلاب اسلامی)
۲-ه 2E	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	کارگاه آموزشی	چالش‌های حکمرانی فرهنگی در عصر سایبر: با تأکید بر ایران معاصر	دکتر امیررضا باقرپور شیرازی	مرکز ملی فضای مجازی
۲-و 2F	سه‌شنبه ۱۵:۳۰ تا ۱۷:۱۵	نشست تخصصی	هوش مصنوعی و علوم اسلامی	دکتر بهروز مینایی بیدگلی، حجت‌الاسلام دکتر مهدی جعفرزاده، دکتر محمدرضا قاسمی	ستاد راهبری فناوری‌های هوشمند حوزه‌های علمیه

کد نشست	زمان	نوع نشست	عنوان	سخنران / ارائه کننده	برگزار کننده
aA مجازی	چهارشنبه ۰۸:۰۰ تا ۰۹:۴۵	کارگاه آموزشی	<b>بکارگیری فضای مجازی برای دانشگاهیان: مشارکت عمومی و رسانه های اجتماعی</b>	دکتر علیرضا صالحی نژاد	مرکز پژوهشی سیاست های فضای مجازی دانشگاه تهران
aB مجازی	چهارشنبه ۰۸:۰۰ تا ۰۹:۴۵	نشست تخصصی	<b>الزامات حقوقی سایبری جنگ ترکیبی</b>	دکتر جواد جاویدنیا	کنفرانس ملی فضای سایبر
bA مجازی	چهارشنبه ۱۰:۰۰ تا ۱۱:۴۵	نشست تخصصی	<b>روند تکوین جنبش های اجتماعی در تطبیق محیط مجازی با محیط واقعی</b>	دکتر عباس چگینی	دانشگاه جامع امام حسین (ع)
bB مجازی	چهارشنبه ۱۰:۰۰ تا ۱۱:۴۵	نشست تخصصی	<b>ظرفیت های فضای سایبری برای حکمرانی تعالی گرا</b>	دکتر علی اصغر پورعزت	دانشکده حکمرانی دانشگاه تهران

## فهرست مقالات

- ۱۰۰۰] وجوب تأمین امنیت در فضای سایبر بر اساس بیانیه گام دوم انقلاب اسلامی  
- سعید حسنی ..... ۱
- ۱۰۰۵] استراتژی امنیت ملی تعاملی سازنده بر توسعه دانش سایبرنتیک در عصر جنگ سایبری  
- امین حسوند ..... ۱۹
- ۱۰۰۷] نظام حقوقی مطلوب و حق بر حریم خصوصی در آفند سایبری شبکه‌های مجازی  
- امین حسوند ..... ۳۵
- ۱۰۰۸] خلوت عالم‌ساز یا جلوت فرهیخته‌ساز (بررسی مؤلفه گمنامی یا هویت‌مندی در فرآیند عمومی‌سازی علم)  
- سید محمد مهدی شرف‌الدین ..... ۴۷
- ۱۰۰۹] پروتکل توافق کلید امن احراز اصالت شده برای کاربرد در گواهی (تصدیق) دیجیتال  
- امیر حسین رحیمی ..... ۵۷
- ۱۰۱۱] تصدیق دیجیتال کلید عمومی برای احراز اصالت کاربر و برقراری کلید جلسه برای ارتباطات شبکه‌ای امن  
- امیر حسین رحیمی ..... ۷۱
- ۱۰۱۲] ارائه تعریف فضای سایبری و فضای مجازی بر پایه مبانی علم سایبرنتیک  
- احسان خوشحال‌پور ..... ۹۱
- ۱۰۱۴] ارائه یک مکانیزم تشویقی برای شبکه‌های حسگر جمعی بر پایه ارتباطات گوشی به گوشی  
- رسول اسماعیلی فرد - ستاره قره چاهی ..... ۹۹
- ۱۰۱۷] تشخیص طنز در زبان فارسی با رویکرد یادگیری عمیق  
- فاطمه نجفی لیپوندانی - محمد حسن شیرعلی شهرضا ..... ۱۱۱
- ۱۰۱۸] اصول سیستم‌های سایبرنتیکی و انطباق آن با مراکز اطلاع‌رسانی  
- نعیمه ظریف قاسمیان - حسن بهزادی ..... ۱۲۳
- ۱۰۲۰] سازگاری یا ناسازگاری توصیه‌نامه‌ی اخلاق هوش مصنوعی یونسکو با نظریه اخلاقی اسلام  
- حمید محسنی - کاظم فولادی قلعه ..... ۱۳۳
- ۱۰۲۱] واکاوی بنیاد فکری نظام سایبرنتیک و راهکار مقابله با تهدیدات آن در نظام ولایت  
- رضوان هامانی - زهرا حبیبیان ..... ۱۴۱
- ۱۰۲۳] ارتقاء خبررسانی جمهوری اسلامی با استفاده از خبرگزاری جمع‌سپار مبتنی بر فناوری بلاک‌چین  
- سید محمد حسین موسوی - مرتضی انصاری ..... ۱۵۳
- ۱۰۲۴] بازجستی در چرایی جرائم رایانه‌ای و راهکارهای مقابله با آن  
- سهیل معیری ..... ۱۷۵
- ۱۰۲۵] شبکه‌های اجتماعی مجازی و کنش سیاسی  
- حمزه عالمی چراغعلی ..... ۱۸۵
- ۱۰۲۶] ترسیم نقشه‌ی هم‌واژگانی و تحلیل موضوعی مقالات حوزه داده‌کاوی در پایگاه اسکوپوس با استفاده از نرم‌افزار وی.او.اس. ویور  
- آرام مجیری - محسن حاجی زین العابدینی ..... ۱۹۹
- ۱۰۲۷] تحلیل راهبردی اقدامات مکررات حفاظت از داده‌های عمومی (ارائه چارچوب مفهومی اقدامات کلان حفاظت از داده در کشور)  
- رحیم خانی زاد - ابودر عرب سرخی ..... ۲۰۹

- ۱۰۲۸] کتابخانه‌ها در متاورس  
فاطمه محمدخانی - محسن حاجی زین العابدینی ..... ۲۳۷
- ۱۰۳۱] اثر مشاهده تصاویر خویش انداز زنان تاثیرگذار اینستاگرام بر گرایش خانم‌ها به انجام جراحی‌های زیبایی با میانجی‌گری نارضایتی چهره‌ای  
فاطمه تمنائی - پگاه نجات ..... ۲۴۷
- ۱۰۳۲] مدل مفهومی فضای سایبر از دیدگاه کاربرد علوم داده در امنیت سایبری  
سید نصیب اله دوستی مطلق - علی اصغر نوروزی ..... ۲۶۱
- ۱۰۳۳] الگوی تدوین نقشه‌ی راهبرد حکمرانی بر فضای سایبر جمهوری اسلامی ایران  
ساسان چمنی - محسن آقایی ..... ۲۷۱
- ۱۰۳۴] نقد گفتمان رایج تبلیغ دینی در فضای سایبر از منظر شاخصه انتظار  
زهره جمالی زواره - محسن خوش‌فر ..... ۲۹۱
- ۱۰۳۵] فرصت‌ها و چالش‌های تبلیغ دین در فضای مجازی از دیدگاه قرآن  
محمدرضا برزویی‌زاده - زهره جمالی زواره ..... ۳۰۹
- ۱۰۳۷] بررسی دلایل عدم موفقیت شبکه‌های اجتماعی داخلی  
سید جواد شریف‌الاسلامی ..... ۳۳۱
- ۱۰۳۸] هستی‌شناسی فضای سایبر: بازخوانی انگاره فلسفی «مراحل تکامل عقل انسان» و انگاره فلسفی «عالم عقول» از منظر فضای سایبری  
مصطفی ملکشاهی‌صفت ..... ۳۴۹
- ۱۰۳۹] تحلیلی اخلاقی از رابطه احساسی انسان و روبات  
سعیده بابایی - نرجس صابری - منیره بحرینی ..... ۳۶۷
- ۱۰۴۲] رویکردهای هوشمند در شناسایی وبگاه‌های دام‌چینی  
یگانه ستاری - غلامعلی منتظر ..... ۳۷۷
- ۱۰۴۴] واکاوی نظریه‌های قدرت سایبری و ارائه مدل مفهومی نوین برای قدرت سایبری  
خداداد هلیلی ..... ۳۸۷
- ۱۰۴۵] ابعاد شناختی-هیجانی تعامل انسان-روبات  
زهره نوروزی - فاطمه امیرخانی ..... ۳۹۷
- ۱۰۴۷] بنیاد و چارچوب دانش سایبری اسلام  
ابوالفضل امامی مبینی - مجتبی شیخی ده‌آبادی ..... ۴۰۹
- ۱۰۴۸] نفرت‌پراکنی در وب تاریک از منظر نظام بین‌المللی حقوق بشر  
یاسمن صفایی ..... ۴۱۹
- ۱۰۵۰] بررسی روش‌های اجماع بلاک‌چین‌های مورد استفاده در اینترنت اشیا  
حسین شعله‌رسا - محمدعلی آصف - کاظم فولادی قلعه ..... ۴۳۱
- ۱۰۵۳] ضرورت اصلاح قوانین و مقررات تبلیغاتی فضای سایبر در جهت حمایت از حقوق کودکان و نوجوانان  
محمد امینی - رسول مظاهری کوهانستانی ..... ۴۴۹
- ۱۰۵۴] ارزیابی ناامنی سایبری در منطقه خاورمیانه و پاسخ دولت‌ها  
سید حامد حسینی ..... ۴۶۳
- ۱۰۵۵] حریم شخصی در فضای سایبر  
محمد جعفری ..... ۴۷۵
- ۱۰۵۶] بررسی قابلیت‌های فناوری بلاک‌چین در مدیریت اسناد و آرشیوهای الکترونیکی  
فاطمه ترکاشوند - محمدرضا وصفی - مژگان رستگار - محمدهادی وصفی ..... ۴۸۳

- ۱۰۵۸] مشروعیت آورده‌های اقتصادی بازی‌های دیجیتال  
- مهدی اخلاصی - جهانگیر رخشدگان - علی رستمی ..... ۴۹۳
- ۱۰۵۹] سئوی سایت‌های فروش آنلاین کتاب و استفاده از فناوری واقعیت مجازی (مطالعه موردی)  
- مهشید التماسی ..... ۵۰۳
- ۱۰۶۰] هوش مصنوعی و کاربردهای نظامی در فضای سایبری  
- فریده محمدعلی‌پور - میرامیر پور موسوی ..... ۵۱۵
- ۱۰۶۵] امکان‌سنجی معامله در فضای سایبر بر اساس فقه امامیه  
- محمدرضا صفایی تخت فولادی ..... ۵۲۵
- ۱۰۶۶] تأثیر فناوری سایبر در معماری  
- سیده زرگس حسینی - محمد امین دباغیان ..... ۵۳۵
- ۱۰۶۷] درآمدی بر انقلاب صنعتی پنجم: کنترل کربن، راهبردی برای کنترل جهان  
- سیده زهرا موسوی - محمدعلی شکوهیان‌راد ..... ۵۴۳
- ۱۰۶۸] بررسی گلوگاه سایبری در ورود به گام دوم انقلاب  
- مجتبی شیخی ده‌آبادی - ابوالفضل امامی میبیدی ..... ۵۶۳
- ۱۰۶۹] سایبرنتیک و طراحی رفتارگرا  
- سید علی فارغ - مهدیه رمضان‌خواه ..... ۵۷۳
- ۱۰۷۰] تهدیدات اکوسایبرنتیکی، چهار چوب نوین تهدیدات علیه زیست‌بوم  
- عاطفه نصیری - محمدعلی شکوهیان‌راد ..... ۵۸۱
- ۱۰۷۳] بهینه‌سازی ماژول NTT در الگوریتم رمزنگاری پساکوانتوم Crystals-Kyber  
- محمد غفاری - حاتم عبدلی ..... ۵۹۷
- ۱۰۷۴] دیپلماسی سایبری؛ توثیق‌پلماسی ایالات متحده آمریکا  
- فریده محمدعلی‌پور - محمدرضا نوروزپور ..... ۶۰۷
- ۱۰۷۵] بایوسایبرنتیک، مبنای کنترل‌های نوین در حوزه‌ی زیستی  
- محمدعلی شکوهیان‌راد - امیرحسین منتظر ..... ۶۱۷
- ۱۰۷۷] امکان‌سنجی تقنین در فضای مجازی با تأکید بر اصول قانون اساسی  
- زهرا رثوفی فرد - فیروز اصلانی ..... ۶۳۳
- ۱۰۷۹] شناسایی جملات حاوی کلمات توهین‌آمیز با استفاده از الگوریتم‌های یادگیری ماشین در سرویس‌های ابری آمازون  
- امیرعلی خانه‌نقا - زهرا موحدی ..... ۶۵۱
- ۱۰۸۴] سیستم اعتبار اجتماعی: مروری بر دیدگاه‌ها  
- علیرضا زینی - حسین عظیمی - علی لکزائی - کاظم فولادی قلعه ..... ۶۶۱
- ۱۰۸۶] شبکه ملی اطلاعات و نبردهای سایبری - شناختی  
- علی قهرمانی ..... ۶۸۵
- ۱۰۸۸] آسیب‌شناسی فضای سایبر در حوزه همسرگزینی و خانواده  
- محبوبه موسیوند - فائزه ساکی ..... ۶۹۵
- ۱۰۸۹] مفهوم تغییر کارکرد تکنیک در مطالعات فضای سایبر  
- محمد محمدی نیا ..... ۷۰۵
- ۱۰۹۱] فلسفه اطلاعات از منظر پدیدارشناسی  
- محمد رضاپور ..... ۷۱۷

- [۱۰۹۴] بررسی رابطه حاکمیت شرکتی و حکمرانی فضای مجازی  
- محمود اعتصامی فر ..... ۷۲۳
- [۱۰۹۷] بررسی جرم‌شناختی بزهکاری سایبری با تأکید بر نظریه‌ی فعالیت روزمره  
- سید علی شریفی ..... ۷۳۳
- [۱۰۹۹] وب تاریک و چالش‌های فراروی حقوق کیفری  
- پریسا حاجی زاده ..... ۷۴۱
- [۱۱۰۱] حوزه علمیه و متاورس، فرصت‌ها و پیامدها  
- مهدی منصوری خواه ..... ۷۴۹
- [۱۱۰۳] پیوند نظام کیفری و جاسوسی صنعتی در فضای سایبر: رویارویی با هم‌کنشی؟  
- مرضیه جعفرخانی - حسن عالی پور ..... ۷۶۳
- [۱۱۰۴] مدل‌سازی دینامیکی هوشمند صادرات در کشورهای نفت‌خیز  
- ارشیا بادی - حبیب‌الله آراسته‌راد - محمد طالبی - اسماعیل ناظم شهرضا ..... ۷۷۳
- [۱۱۰۵] روند تکوین جنبش‌های اجتماعی در تطبیق محیط مجازی با محیط واقعی  
- عباس چگینی ..... ۷۸۵
- [۱۱۰۶] فضای سایبری به مثابه ذهن-جهان  
- احمد امامی ..... ۷۹۷

## فهرست نویسندگان

- ابوالفضل امامی میبدی (ص ۴۰۹)
- ابوالفضل امامی میبدی (ص ۵۶۳)
- ابوذر عرب سرخی (ص ۲۰۹)
- احسان خوشحال پور (ص ۹۱)
- احمد امامی (ص ۷۹۷)
- ارشیا بادی (ص ۷۷۳)
- اسماعیل ناظم شهرضا (ص ۷۷۳)
- امیرحسین رحیمی (ص ۵۷)
- امیرحسین رحیمی (ص ۷۱)
- امیرحسین منتظر (ص ۶۱۷)
- امیرعلی خانه عنقا (ص ۶۵۱)
- امین حسنونند (ص ۱۹)
- امین حسنونند (ص ۳۵)
- آرام مجیری (ص ۱۹۹)
- پریسا حاجی زاده (ص ۷۴۱)
- پگاه نجات (ص ۲۴۷)
- جهانگیر رخسندگان (ص ۴۹۳)
- حاتم عبدلی (ص ۵۹۷)
- حبیب‌اله آراسته راد (ص ۷۷۳)
- حسن بهزادی (ص ۱۲۳)
- حسن عالی‌پور (ص ۷۶۳)
- حسین شعله‌رسا (ص ۴۳۱)
- حسین عظیمی (ص ۶۶۱)
- حمزه عالمی چراغعلی (ص ۱۸۵)
- حمید محسنی (ص ۱۳۳)
- خداداد هلیلی (ص ۳۸۷)
- رحیم خانی زاد (ص ۲۰۹)
- رسول اسماعیلی فرد (ص ۹۹)
- رسول مظاهری کوهانستانی (ص ۴۴۹)
- رضوان هامانی (ص ۱۴۱)
- زهرا حبیبیان (ص ۱۴۱)
- زهرا رئوفی فرد (ص ۶۳۳)
- زهرا موحدی (ص ۶۵۱)
- زهرا نوروزی فرانی (ص ۳۹۷)
- زهره جمالی زواره (ص ۲۹۱)
- زهره جمالی زواره (ص ۳۰۹)
- ساسان چمنی (ص ۲۷۱)
- ستاره قره چاهی (ص ۹۹)
- سعید حسنی (ص ۱)
- سعیده بابایی (ص ۳۶۷)
- سهیل معیری (ص ۱۷۵)
- سید جواد شریف شیخ‌الاسلامی (ص ۳۳۱)
- سید حامد حسینی (ص ۴۶۳)
- سید محمد مهدی شرف‌الدین (ص ۴۷)
- سید محمدحسین موسوی (ص ۱۵۳)
- سید نصیب‌اله دوستی مطلق (ص ۲۶۱)
- سیدعلی شریفی (ص ۷۳۳)
- سیدعلی فارغ (ص ۵۷۳)
- سیده زهرا موسوی (ص ۵۴۳)
- سیده نرگس حسینی (ص ۵۳۵)
- عاطفه نصیری (ص ۵۸۱)
- عباس چگینی (ص ۷۸۵)
- علی اصغر نوروزی (ص ۲۶۱)
- علی رستمی (ص ۴۹۳)
- علی قهرمانی (ص ۶۸۵)
- علی لک‌زائی (ص ۶۶۱)
- علیرضا زینی (ص ۶۶۱)
- غلامعلی منتظر (ص ۳۷۷)
- فاطمه امیرخانی (ص ۳۹۷)
- فاطمه ترکاشوند (ص ۴۸۳)
- فاطمه تمنائی (ص ۲۴۷)
- فاطمه محمدخانی (ص ۲۳۷)
- فاطمه نجفی لیوندانی (ص ۱۱۱)
- فائزه ساکی (ص ۶۹۵)
- فریده محمدعلی‌پور (ص ۵۱۵)
- فریده محمدعلی‌پور (ص ۶۰۷)
- فیروز اصلانی (ص ۶۳۳)
- کاظم فولادی قلعه (ص ۱۳۳)
- کاظم فولادی قلعه (ص ۴۳۱)
- کاظم فولادی قلعه (ص ۶۶۱)
- مجتبی شیخی ده‌آبادی (ص ۴۰۹)
- مجتبی شیخی ده‌آبادی (ص ۵۶۳)
- محبوبه موسیوند (ص ۶۹۵)
- محسن آقایی (ص ۲۷۱)
- محسن حاجی زین‌العابدینی (ص ۱۹۹)
- محسن حاجی زین‌العابدینی (ص ۲۳۷)
- محسن خوش‌فر (ص ۲۹۱)
- محمد امینی (ص ۴۴۹)
- محمد جعفری (ص ۴۷۵)
- محمد رضاپور (ص ۷۱۷)

- محمد طالبی (ص ۷۷۳)
- محمد غفاری (ص ۵۹۷)
- محمد محمدی نیا (ص ۷۰۵)
- محمد امین دباغیان (ص ۵۳۵)
- محمد حسن شیرعلی شهرضا (ص ۱۱۱)
- محمدرضا برزویی زاده (ص ۳۰۹)
- محمدرضا صفایی تخت فولادی (ص ۵۲۵)
- محمدرضا نوروزپور (ص ۶۰۷)
- محمدرضا وصفی (ص ۴۸۳)
- محمدعلی آصف (ص ۴۳۱)
- محمدعلی شکوهیان راد (ص ۵۴۳)
- محمدعلی شکوهیان راد (ص ۵۸۱)
- محمدعلی شکوهیان راد (ص ۶۱۷)
- محمود اعتصامی فر (ص ۷۲۳)
- مرتضی انصاری (ص ۱۵۳)
- مرضیه جعفرخانی (ص ۷۶۳)
- مژگان رستگار (ص ۴۸۳)
- مصطفی ملکشاهی صفت (ص ۳۴۹)
- منیره بحرینی (ص ۳۶۷)
- مهدی اخلاصی (ص ۴۹۳)
- مهدی منصوری خواه (ص ۷۴۹)
- مهدیه رمضان خواه (ص ۵۷۳)
- مهشید التماسی (ص ۵۰۳)
- میر امیر پور موسوی (ص ۵۱۵)
- نرجس صابری (ص ۳۶۷)
- نعیمه ظریف قاسمیان (ص ۱۲۳)
- یاسمن صفایی (ص ۴۱۹)
- یگانه ستاری (ص ۳۷۷)



**CYSP  
2022**

THE FIRST CONFERENCE ON  
**CYBERSPACE**

نخستین  
کنفرانس  
**فضای سایبر**



۱۰ تا ۱۲ آبان ۱۴۰۱ - دانشکده مهندسی دانشکدهگان فارابی دانشگاه تهران

## متن کامل مقالات فارسی

## وجوب تأمین امنیت در فضای سایبر بر اساس بیانیه گام دوم انقلاب اسلامی

سعید حسنی<sup>۱</sup>

<sup>۱</sup> استادیار دانشگاه فرهنگیان اراک، گروه معارف و تربیت اسلامی  
shahidmohammad.4101365@gmail.com

### چکیده

«بیانیه گام دوم انقلاب اسلامی» بر وظیفه سنگین دستگاه‌های حکومتی نسبت به «ابزارهای رسانه‌ای پیشرفته و فراگیر» تأکید دارد؛ و با توجه به اینکه بسیاری از این رسانه‌ها در فضای سایبر فعالیت می‌کنند، واکاوی وظیفه یادشده با تأکید بر رسانه‌های سایبری، دارای نوآوری است. هدف پژوهش، پاسخ به این پرسش است که از منظر فقه سیاسی، وظیفه حکومت اسلامی نسبت به تأمین امنیت در فضای سایبر کدام است و جایگاه این وظیفه در بیانیه گام دوم چیست. بنابراین با جستجو در منابع کتابخانه‌ای؛ مستندات حکم به وجوب تأمین امنیت همه جانبه در فضای سایبر توصیف و با رویکرد فقه حکومتی تحلیل شده و دیدگاه مقام معظم رهبری پیرامون امنیت فضای سایبر، در منظومه فکری ایشان بررسی شده تا جایگاه این وظیفه در بیانیه مشخص گردد. در نتیجه، ایجاد امنیت همه جانبه در فضای سایبر بر حکومت اسلامی واجب دانسته شده که مشمول مطالبه جدی بیانیه گام دوم انقلاب اسلامی نیز می‌باشد.

**کلمات کلیدی:** بیانیه گام دوم انقلاب، امنیت فضای سایبر، ابعاد امنیت، وجوب ایجاد امنیت، مقام معظم رهبری.

### ۱ مقدمه

در چهلمین سالگرد انقلاب اسلامی، بیانیه‌ی مهمی از سوی رهبر انقلاب اسلامی، آیه الله خامنه‌ای (مد ظله العالی) صادر گردید، که همانند سایر سیاست‌های کلی ابلاغ شده از سوی ایشان، بر اساس وجوب اطاعت از ولی امر، لازم الاجرا می‌باشد. در توصیه دوم این بیانیه که پیرامون اخلاق و معنویت است، بر وظیفه سنگین دستگاه حاکمیت نسبت به برنامه‌ریزی برای مدیریت ابزارهای رسانه‌ای پیشرفته و فراگیر، تأکید شده است. ایشان در دومین توصیه بیانیه گام دوم انقلاب اسلامی می‌فرماید: «ابزارهای رسانه‌ای پیشرفته و فراگیر، امکان بسیار خطرناکی در اختیار کانون‌های ضد معنویت و ضد اخلاق نهاده است و هم‌اکنون تهاجم روزافزون دشمنان به دل‌های پاک جوانان و نوجوانان و حتی نونهالان با بهره‌گیری از این ابزارها را به چشم

خود می‌بینیم. دستگاه‌های مسئول حکومتی در این باره وظایفی سنگین بر عهده دارند که باید هوشمندانه و کاملاً مسئولانه صورت گیرد و این البته به معنی رفع مسئولیت از اشخاص و نهادهای غیرحکومتی نیست. در دوره‌ی پیش‌رو باید در این باره‌ها برنامه‌های کوتاه‌مدت و میان‌مدت جامعی تنظیم و اجرا شود» (خامنه‌ای، بیانیه گام دوم انقلاب اسلامی: ۷).

بخش مهمی از رسانه‌های فراگیر در بستر فضای سایبر فعالیت می‌کنند و لذا بخشی از مطالبات ایشان در این توصیه، به مدیریت فضای سایبر مربوط می‌شود. در این پژوهش تنها در مورد رسانه‌های سایبری بحث می‌گردد.

آنچه ضرورت این پژوهش در مورد تفسیر بیانیه گام دوم را روشن‌تر می‌کند، این سوء برداشت احتمالی است که تأمین امنیت فضای سایبر، مشمول وظایف حکومت اسلامی و مسئولیت سنگین مذکور در بیانیه محسوب نشود و در تأیید این سلب وظیفه از حاکمیت نیز، احترام گذاشتن به آزادی مردم ذکر گردد؛ چرا که تأمین امنیت همه جانبه، ممکن است قدرت انتخاب و نحوه فعالیت مردم در فضای سایبر را محدود کند. بر اساس این مبنا، دیدگاه فوق، مطالبه بیانیه گام دوم در مورد مدیریت فضای سایبر را، به افزایش سرعت و امکانات اینترنت و همچنین تولید محتوای ارزشی در مقابل تولیدات ناهنجار و کانون‌های ضد معنویت، تفسیر می‌کند؛ و به فضای سایبری رها شده فعلی افتخار می‌کند (خامنه‌ای، بیانات در دیدار نوروزی، ۱۴۰۰/۱/۱)؛ تا مردم بتوانند از مطالب مفید علمی، فرهنگی و اخلاقی استفاده کنند و به آسانی تجارت نمایند. البته اگر کسی از چاقوی دولبه استفاده ممنوع می‌کند مرتکب خطا شده و اگر آن کار ممنوع جرم‌انگاری شده باشد، تعقیب قانونی می‌شود، هرچند ارتقاء سواد رسانه‌ای مطلوب است و آحاد جامعه به آن توصیه می‌شوند و به نظر می‌رسد، بررسی اندیشه سیاسی مقام معظم رهبری در این موضوع و مستندات فقهی پیرامون آن نقش مهمی در تفسیر این بخش از بیانیه دارد.

در تفسیر مطالبه جدی ایشان در بیانیه گام دوم، فرضیه‌ی تحقیق عبارت است از: «وجوب ایجاد امنیت همه جانبه فضای سایبر بر حکومت اسلامی که بخشی از مطالبه مقام معظم رهبری در توصیه دوم از بیانیه گام دوم انقلاب اسلامی می‌باشد» و روش پژوهش حاضر این گونه است که دیدگاه ایشان در مقوله ابعاد امنیت و امنیت فضای سایبر در بیانات و سیاست‌های ابلاغی از سوی ایشان مرور می‌شود و متناسب با ابعاد امنیت فضای سایبر، به جستجوی مستندات فقهی به جهت حکم تکلیفی به وجوب ایجاد امنیت فضای سایبر توسط حکومت اسلامی پرداخته می‌شود تا بر اساس گزاره‌های فقه سیاسی، یک بخش از مطالبات ولی فقیه در بیانیه گام دوم، بر مطالبه ایجاد امنیت کامل و جامع در فضای سایبر تفسیر گردد. با این توضیحات، سؤال اصلی تحقیق عبارت است از: «از منظر فقه سیاسی وظیفه حکومت اسلامی نسبت به تأمین امنیت در فضای سایبر چیست و این وظیفه در بیانیه گام دوم انقلاب اسلامی چه جایگاهی دارد؟» سؤالات فرعی تحقیق عبارتند از: «مستندات فقهی وظیفه حکومت اسلامی در مورد تأمین امنیت در فضای سایبر کدام است؟»، «در سیاست‌های ابلاغی از سوی مقام معظم رهبری در مورد فضای سایبر، امنیت چه جایگاهی دارد و شامل چه اقسامی می‌شود؟»، «تأمین امنیت در فضای سایبر در بیانیه گام دوم انقلاب چه جایگاهی دارد؟»، «چه راهکارهایی جهت تأمین امنیت فضای سایبر پیشنهاد می‌شود و این راهکارها چه نوعی دارند؟».

## ۲ پیشینه تحقیق

از نیمه دوم قرن بیستم و با انحطاط ابعاد مختلف امنیت در سطح بین الملل، مطالعات پیرامون امنیت رو به گسترش است (لک زایی، ۱۳۹۴: ۸)؛ و از آن جا که انواع درهم تنیده‌ی امنیت در حکومت اسلامی مطلوب است (سیدباقری، ۱۳۹۷: ۲۷)؛ پژوهشگران فقه سیاسی، پیرامون وظایف حکومت اسلامی در تأمین تمام ابعاد امنیت در فضای فیزیکی، مطالعات گسترده‌ای انجام داده‌اند که در مجلات علمی علوم سیاسی و فقه سیاسی به رشته تحریر درآمده و منتشر شده اند (ر.ک: لک زایی و فاضلی، ۱۳۹۷: ۱۱۲؛ ورعی، ۱۳۹۷: ۱۲۶؛ حاج زاده و دیگران، ۱۳۹۵: ۵۷؛ شریعتمدار جزایری، ۱۳۷۹: ۷)؛ اما در حوزه‌ی مدیریت رسانه مخصوصاً در فضای سایبری، تحصیلات در مقطع دکتری در دانشگاه‌های ایران به تازگی و در دهه اخیر شروع شده است. البته پژوهش‌هایی در زمینه اخلاق زیستن در فضای سایبری و مبانی حقوقی و فقهی حریم خصوصی افراد و پالایش توسط حکومت، در مراکز هم‌چون مرکز مطالعات راهبردی فضای مجازی دانشگاه جامع امام حسین (علیه السلام) انجام گرفته و برخی پژوهش‌ها در مجلات علمی به چاپ رسیده است (ورعی، ۱۳۹۷: ۱۱۸؛ حسینی و برزویی، ۱۳۹۶؛ طباطبایی و لیالی، ۱۳۹۷: ۸۷؛ اسماعیلی و نصر اللهی، ۱۳۹۵: ۱۰). همچنین در فصل سی‌ام قانون مجازات اسلامی به جرایم رایانه‌ای پرداخته شده و مجازات‌هایی مرتبط با جرائم در فضای سایبر بیان گردیده که می‌توان این جرم انگاری‌ها را زیرمجموعه‌ی اخلاق به ابعادی از امنیت دانست. مانند: امنیت اطلاعات سرب‌ ملی و شخصی (مواد ۷۲۹ و ۷۴۰)، امنیت روانی و امنیت و آسایش عمومی (مواد ۷۴۶ و ۷۳۹)، امنیت اخلاقی (مواد ۷۴۲ و ۷۴۳)، امنیت جانی نسبت به تهدید، و ترغیب به خودکشی و اعمال خشونت‌آمیز (ماده ۷۴۳)، و امنیت حیثیت و آبرویی افراد (مواد ۷۴۴-۷۴۶)؛ (قانون مجازات اسلامی مصوب ۱/۲/۱۳۹۲، فصل سی‌ام: ۳۱۹-۳۳۶). اما بدیهی است که اکتفا به جرم‌انگاری و مجازات تنها یک بخش از وظایف حکومت اسلامی در بخش قضائی است که به وسیله تقنین و اجرای قوانین کیفری، تلاش می‌کند نسبت به اخلاق‌گری برخی آحاد جامعه به امنیت برخی دیگر، بازدارندگی ایجاد کند و آنچه مهم است، پیشگیری حکومت اسلامی از وقوع جرائمی است که اخلاق به امنیت محسوب می‌شوند؛ امری که در «رهنمود پیشگیری از جرم» سازمان ملل متحد نیز بر آن تأکید شده است (محسنی، صوفی زمرد، ۱۳۹۶: ۱۷۳). از این روی در بیانیه‌ی گام دوم انقلاب اسلامی، تنظیم برنامه‌های جامع کوتاه‌مدت و میان‌مدت برای مدیریت رسانه‌های پیشرفته و فراگیر که مصداق بارز آن‌ها، رسانه‌های سایبری است؛ ضروری دانسته شده است. نوآوری این پژوهش را می‌توان در این نکته دانست که به تفسیر برخی ابعاد بیانیه مهم گام دوم انقلاب اسلامی می‌پردازد و تفسیر خود را بر اساس دیدگاه‌های مقام معظم رهبری در مورد وظایف حکومت اسلامی در تأمین امنیت فضای سایبر، و همچنین از منظر فقه حکومتی انجام می‌دهد، چراکه اولاً ایشان دارای منظومه فکری است و لذا می‌توان انتظارات مطرح شده در بیانیه را بر اساس دیگر فرمایش‌های ایشان معنا کرد؛ و ثانیاً، اندیشه‌های ولی فقیه، متأثر از فقه و مبانی اسلامی است.

## ۳ مفاهیم تحقیق

### ۱.۳ رسانه‌های سایبری

رسانه به معنای هر آن چیزی است که برای رساندن پیامی مورد استفاده قرار می‌گیرد و رسانه‌های سایبری، ابزارهایی می‌باشند که با فناوری‌های جدید ساخته می‌شوند و در بستری موسوم به فضای سایبری به کار گرفته می‌شوند. فضای سایبر (cyberspace) معادل دنیای مجازی (virtual world) قرار داده شده است. این واژه در کاربرد رایج آن در ایران بیانگر محیطی است که در بستر اینترنت ایجاد شده و دارای دو ویژگی اصلی اشتراک‌گذاری و تعامل اطلاعاتی است. به همین منظور، به گستره‌ی فضای مجازی به اختصار «فاوا» (فناوری اطلاعات و ارتباطات) گفته می‌شود (شریفی دوست و واحد جوان، ۱۳۹۸: ۴). به عبارت دیگر، محیطی غیرفیزیکی از ارتباطات تعاملی و فکری از طریق شبکه‌ی رایانه‌ای و بر بستر دیجیتال را فضای سایبر می‌خوانند (اسماعیلی و نصراللهی، ۱۳۹۵: ۸). در این بحث باید توجه نمود که استفاده از لفظ مجازی به معنای غیر واقعی نیست و مجاز در این استعمال به معنای غیرفیزیکی است و لذا می‌بایست گفت: واقعیت مجازی و واقعیت فیزیکی (عاملی، ۱۳۹۰: ۲۴)؛ و نکته دیگر این که ایجاد و اداره مسیرهای این ارتباطات سایبری یا همان فضای سایبر در اختیار حاکمیت هر کشوری است، هرچند تصمیم یک کشور بر این باشد که امکان استفاده مردم آن کشور، از بستر شبکه اینترنت جهانی که با اشراف آژانس امنیت ملی ایالات متحده آمریکا (NSA) اداره می‌شود را فراهم کند (دفانس، ۱۳۸۲: ۴۳).

### ۲.۳ فقه سیاسی

مرگب‌واژه «فقه سیاسی» به معنای بخشی از ابواب و مسائل دانش فقه است که به موضوعات سیاسی عنایت دارند؛ و در واقع یک گرایش تخصصی در مطالعات فقهی است. دانشی که هدفش تدبیر فضای سیاسی و اجتماعی جامعه است و گزاره‌های خود را به نصوص و منابع شرعی مستند می‌کند (ایزدهی، ۱۳۹۴: ۱۵۵ و ۱۷۴). مرگب‌واژه‌ی دیگر که به نظر برخی مرادف فقه سیاسی است، «فقه حکومت» است؛ یعنی دانشی که متکفل بیان وظایف دستگاه حاکمیت و استنباط احکام شرعی تکلیفی و وضعی آن از منابع فقه می‌باشد. همان‌طور که «فقه افراد» وظایف مکلفین را در حیطه‌ی رفتارهای هر فرد انسان به طور معین معرفی می‌کند؛ هرچند ممکن است به شخصیت حقیقی و یا حقوقی افراد نظر داشته باشد (ر.ک: مرتضوی نژاد و میرباقری، ۱۳۹۶: ۱۲۶-۱۳۰ و ۱۴۴). بنا بر این تعریف، وظیفه‌ی تأمین امنیت توسط حکومت، در مباحث فقه سیاسی بررسی می‌گردد.

### ۳.۳ فقه حکومتی

مرگب‌واژه «فقه حکومتی» بیانگر یک رویکرد در استنباط فقهی است. رویکرد حکومتی در فقه، یک نظریه درباره روش استنباط است و به فقیه توصیه می‌کند تا در مقام استنباط احکام فقهی، با لحاظ مبانی همچون گسترش قلمرو دین به عرصه اداره جامعه، اجرای تمام احکام سعادت بخش اسلام در یک نظام حکومتی را مد نظر قرار دهد (ضیائی فر، ۱۳۹۰: ۷). در این رویکرد تمام احکام فقهی اعم از فقه عبادات (فقه الصلاة، فقه

الحج و ...، فقه معاملات (فقه التجاره، فقه النکاح و ...) و فقه حکومت (فقه القضا، فقه الجزا، فقه الجهاد و ...) با نگرش حکومتی بررسی می‌شوند. به این معنا که تأثیر احتمالی و حتمی هر حکم در کیفیت مطلوب اداره‌ی نظام معاش و معاد انسان‌های مهذب و تشکیل جامعه‌ی توحیدی لحاظ گردد؛ و هر فرد در قالب جامعه‌ای به هم پیوسته و در هویت جمعی آن نگرسته می‌شود (مشکانی سبزواری و سعادت، ۱۳۹۲: ۱۰۶؛ غلامی و میر احمدی، ۱۳۹۳: ۸۶).

### ۴.۳ امنیت

امنیت یک واژه‌ی عربی است که مصدر صناعی و از ریشه‌ی «أمن» می‌باشد؛ و به معنای آسودگی خاطر و داشتن طمئینه و عدم ترس، دلهره و نگرانی به کار می‌رود (ابن فارس، ۱۴۰۴، ج ۱: ۱۳۳؛ مصطفوی، ۱۴۳۰، ج ۱: ۱۶۴) و در زبان فارسی نیز به همین معنا به کار رفته است (حاجزاده و دیگران، ۱۳۹۵: ۲۵۵). امنیت در اصطلاح از معنای لغوی فاصله‌ای نگرفته و تنها با مصداق‌شناسی آن در گذر زمان و با توجه به «متعلق به» آن، از امنیت جانی، مالی و آبرویی به ابعاد گسترده‌ای همچون امنیت فکری، فرهنگی و مذهبی، روانی، قضائی، نظامی، زیست‌محیطی، شغلی و اقتصادی، سیاسی و ... توسعه یافته است (بهرامی، ۱۳۸۲: ۱-۳؛ حاجزاده و دیگران، ۱۳۹۵: ۲۵۵-۲۶۸). به نظر می‌رسد خطر از دست دادن هرآنچه مطلوب انسان است، به نحوی او را آزوده خاطر و نگران می‌کند؛ و هرآنچه بقای آن امور مطلوب را تضمین می‌کند، به او آرامش و احساس امنیت می‌دهد. بنابراین بسته به ارزش‌گذاری و تعیین امور مطلوب با توجه به جهان‌بینی انسان، اقسام امنیت استقرار و تعیین می‌شوند؛ و گاهی تهدید متوجه جسم یا روح فرد، جامعه و یا ساختار حاکمیت اسلامی می‌شود و تفاوتی ندارد که این تهدید در فضای فیزیکی نمود یابد و یا در فضای سایبری.

### ۴ مبانی نظری تحقیق

#### ۱.۴ علاوه بر ایجاد رفاه مادی، تأمین امنیت فرهنگی متناسب با فرهنگ اسلامی، از اهداف و وظایف حکومت اسلامی است

بر اساس مبانی نظری اسلام، مهم‌ترین هدف از تشکیل حکومت، بسترسازی برای اقامه‌ی توحید فردی و اجتماعی و اجرای احکام الهی است؛ و استقرار نظم، امنیت و عدالت، از مقدمات ضروری آن به شمار می‌روند؛ یعنی رسیدن به حیات طیب و گوارا تنها در گرو آبادانی حیات دنیوی نیست و آبادانی معنوی نیز از جمله اهداف حکمرانی می‌باشد (خامنه‌ای، ۱۳۹۷: ۱۵۵-۱۶۰؛ ورعی، ۱۳۹۷: ۱۲۲-۱۲۶)، که دستیابی کامل به امنیت همه جانبه و توحید، در حکومت مهدوی (عج) تحقق خواهد یافت (صرامی، ۱۳۹۷: ۵۷-۶۰). به تعبیر دیگر در اندیشه اسلامی، سیاست، خادم شریعت است و سیاست متعالیه به دنبال تربیت خلیفه الهی است (لک زایی و دلیر، ۱۳۹۱: ۷۲). این دیدگاه در اصول کلی قانون اساسی جمهوری اسلامی ایران [فصل اول] (نظر پور، ۱۳۸۹: ۴۸ و ۶۴-۷۸)، انعکاس یافته است. در حالی که مبنای مذکور در تقابل کامل با نظریه‌های اومانستی و لیبرالیستی است. به این معنا که هدف اصلی حکومت غیر الهی، ایجاد رفاه و استفاده حداکثری از مواهب مادی و دنیوی است و تأمین معنویت دینی مردم مورد اهتمام نیست (ر.ک: شبان‌نیا، ۱۳۹۵: ۱۳۹۵).



۴۳-۵۳؛ واعظی، ۱۳۸۶: ۲۱-۲۶). ولذا با تفکر لیبرالی، طراحی محصولات تکنولوژی و مدیریت استفاده از آن‌ها به همراه پیوست فرهنگی سکولار انجام می‌شود.

## ۲.۴ در منظومه فکری مقام معظم رهبری، تأمین امنیت وظیفه مهم حکومت اسلامی است و اقسامی دارد

بر اساس پژوهش‌های گسترده‌ای که در آثار شفاهی و مکتوب آیت الله خامنه‌ای (مد ظله) صورت گرفته، منظومه بودن دیدگاه‌های ایشان به اثبات رسیده است (ر.ک: خسروپناه و دیگران، ۱۳۹۸: ۴۴). در منظومه فکری ایشان در مقوله اهمیت امنیت و دفاع، امنیت به مثابه ضرورت وجود مستمر هوا برای تنفس انسان است؛ ایشان می‌فرماید: «اگر جامعه امنیت نداشته باشد، حالت اختناق پیدا میکند؛ مثل مجموعه‌های که هوا در اختیار نداشته باشد. این، اهمیت امنیت است» (همان: ۱۰۰۲). ایشان بر اساس انواع تهدیدات و تهاجمی که به امنیت مردم صورت می‌گیرد، امنیت را در دو دسته کلی نرم‌افزاری و سخت‌افزاری تقسیم نموده که هر کدام دارای زیر مجموعه‌هایی هستند. به طور مثال امنیت نظامی و انتظامی در حفظ جان و سلامت جسمی مردم، امنیت سخت‌افزاری اند و امنیت فرهنگی، اجتماعی، اقتصادی، قضایی و سیاسی، امنیت نرم‌افزاری هستند. ایشان امنیت فرهنگی را شامل امنیت اعتقادی و اخلاقی، و امنیت اجتماعی را نیز شامل امنیت روانی، آبرویی و امنیت حریم خصوصی محسوب می‌کند (همان).<sup>۱</sup>

## ۳.۴ به نظر مقام معظم رهبری تأمین امنیت همه جانبه در فضای سایبر از وظایف دستگاه‌های حکومتی است

مقام معظم رهبری در سیاست‌های کلی برنامه ششم توسعه، در بند ۳۳ و ۳۴؛ توسعه‌ی محتوا در فضای مجازی بر اساس نقشه‌ی مهندسی فرهنگی کشور تا حداقل پنج برابر وضعیت کنونی و بومی‌سازی شبکه‌های اجتماعی؛ و همچنین ایجاد، تکمیل و توسعه‌ی شبکه ملی اطلاعات و تأمین امنیت آن، تسلط بر دروازه‌های ورودی و خروجی فضای مجازی و پالایش هوشمند آن و ساماندهی، احراز هویت و تحویل در شاخص ترافیکی شبکه به طوری که پنجاه درصد آن داخلی باشد را؛ به عنوان سیاست‌های راهبردی در مورد فضای سایبر ابلاغ نموده است (خامنه‌ای، سیاست‌های کلی برنامه ششم توسعه، ۱۳۹۴/۴/۹)

همچنین در نکات مورد توصیه‌ی اکید ایشان در حکم انتصاب اعضای شورای عالی فضای مجازی، اهتمام ویژه به سالم‌سازی و حفظ امنیت همه‌جانبه فضای مجازی کشور و نیز حفظ حریم خصوصی آحاد جامعه و مقابله مؤثر با نفوذ و دست‌اندازی بیگانگان در این عرصه به‌عنوان راهبردی مهم ذکر شده است و تدوین و تصویب نظام‌های امنیتی، حقوقی، قضایی و انتظامی مورد نیاز در فضای مجازی، از وظایف این شورا دانسته شده است. در بندهای پنجم تا دهم این ابلاغیه آمده است: «۵- تسریع در راه‌اندازی شبکه ملی اطلاعات پس از تصویب طرح آن در شورای عالی و نظارت مستمر و مؤثر مرکز ملی بر مراحل راه‌اندازی و بهره‌برداری از آن. ۶- اهتمام ویژه به سالم‌سازی و حفظ امنیت همه‌جانبه فضای مجازی کشور و نیز حفظ حریم خصوصی

<sup>۱</sup> برخی پژوهشگران ابعاد امنیت را در هفت بُعد «نظامی، سیاسی، اجتماعی، فرهنگی، اخلاقی، اقتصادی، و قضایی» دسته‌بندی نموده‌اند (افتخاری و شهباز، ۱۳۹۸: ۳۱۹).



آحاد جامعه و مقابله مؤثر با نفوذ و دست‌اندازی بیگانگان در این عرصه. ۷- ترویج هنجارها، ارزش‌ها و سبک زندگی اسلامی ایرانی و ممانعت از رخنه‌ها و آسیب‌های فرهنگی و اجتماعی در این عرصه و مقابله مؤثر با تهاجم همه‌جانبه فرهنگی و نیز ارتقای فرهنگ کاربری و سواد فضای مجازی جامعه. ۸- احراز جایگاه و سهم مناسب برای اقتصاد دانش‌بنیان در فضای مجازی در چارچوب سیاست‌های اقتصاد مقاومتی کشور و برنامه‌ریزی همه‌جانبه برای بهبود شرایط کسب‌وکار مرتبط با فناوری‌های مجازی و بهره‌گیری از فرصت‌های اشتغال‌زایی و نیز رونق محتوا، خدمات و تجارت در این عرصه. ۹- توسعه محتوا و خدمات کارآمد و رقابتی منطبق بر ارزش‌ها و فرهنگ اسلامی ایرانی در تمامی قلمروهای مورد نیاز جامعه و جلب مشارکت‌های مردمی و بکارگیری ظرفیت‌های بخش خصوصی در این زمینه. ۱۰- تدوین و تصویب نظام‌های امنیتی، حقوقی، قضایی و انتظامی مورد نیاز در فضای مجازی.» (خامنه‌ای، حکم انتصاب اعضای شورای عالی فضای مجازی، ۱۳۹۴/۶/۱۴).

ایشان در بیانات خود می‌فرماید: «یکی وزارت ارتباطات [است]. این فضای مجازی امروز از فضای حقیقی زندگی ما چند برابر بزرگ‌تر شده؛ بعضی‌ها اصلاً در فضای مجازی تنفس می‌کنند؛ و زندگی‌شان در فضای مجازی است. جوانان هم سروکار دارند با فضای مجازی، با انواع و اقسام چیزها و کارها، با برنامه‌های علمی‌اش، با اینترنتش، با شبکه‌های اجتماعی‌اش، با مبادلات و امثال این‌ها سروکار دارند؛ خوب، اینجا لغزشگاه است. هیچ‌کس نمی‌گوید آقا جاده نکش. اگر شما در یک منطقه‌ای جاده‌ای لازم دارید، خیلی خوب، جاده بکش، جاده‌ی اتوبان هم بکش اما مواظب باش! آنجایی که ریزش کوه محتمل است، آنجا محاسبه‌ی لازم را بکنید. ما به دستگاه‌های ارتباطی خودمان، به مجموعه‌ی وزارت ارتباطات و شورای عالی مجازی - که بنده از آن هم گله دارم - سفارشمان این است. ما نمی‌گوییم این راه را ببندید؛ نه، اینکه بی‌عقلی است. یک کسانی نشستند، فکر کرده‌اند، یک راهی باز کرده‌اند به‌عنوان این فضای مجازی و به‌قول خودشان سایبری؛ خیلی خوب، از این استفاده کنید منتها استفاده‌ی درست بکنید؛ دیگران دارند استفاده‌ی درست می‌کنند؛ بعضی از کشورها طبق فرهنگ خودشان این دستگاه‌ها را قبضه کرده‌اند. ما چرا نمی‌کنیم؟ چرا حواسمان نیست؟ چرا می‌کنیم این فضای غیرقابل کنترل و غیرمنضبط را؟ مسئولند، یکی از مسئولین هم همین‌ها هستند؛ دستگاه وزارت ارتباطات است (خامنه‌ای، بیانات در دیدار با دانشگاه فرهنگیان، ۱۳۹۵/۲/۱۳).

بر اساس بیانات، سیاست‌های ابلاغی و احکام انتصابی ایشان، همانند ایمن‌سازی جاده‌ها و راه‌های ارتباط فیزیکی، که وظیفه واجب حکومت اسلامی است، ایمن‌سازی کامل فضای سایبر نیز لازم و ضروری است زیرا فضای تنفس آحاد جامعه محسوب می‌شود و مردم در فضای به‌اصطلاح مجازی، زندگی حقیقی دارند.

#### ۴.۴ رویکرد فقه حکومتی، تنها رویکرد فقهی مقبول و تمدن ساز است

مقام معظم رهبری نیز به‌عنوان یک مجتهد و فقیه، از رویکرد فقه حکومتی دفاع می‌کند (مشکانی سبزواری، ۱۳۹۰: ۱۵۵). در توضیح این رویکرد باید گفت: در روش‌شناسی فقه، تقسیم‌بندی سه‌گانه‌ی فقه موضوع محور، فقه نظام محور و فقه سرپرستی مطرح گردیده (مرتضوی نژاد و میرباقری، ۱۳۹۶: ۱۱۹)؛ و اتخاذ رویکرد سوم به‌منظور پیشگیری از انفعال فقه در برابر طراح‌های سبک زندگی مبتنی بر مدرنیته، و به‌عنوان یکی از مقدمات ضروری در تمدن‌سازی اسلامی و تنها روش صحیح فقه پژوهی [به عنوان اصلی‌ترین دانش

مستند به دین و کانون هدایت جامعه] ضروری شمرده شده است (مشکانی سبزواری و سعادت، ۱۳۹۲: ۱۰۶؛ خلف خانی، ۱۳۹۵: ۴۱). در فقه سرپرستی، جامعه به عنوان یک کل متغیّر و متحرک، و با تأثیر و تأثر درونی اجزاء خود بر یکدیگر، مورد تصرّف حکومت قرار می‌گیرد و طرّاحی چستی و مقادیر تمایلات اخلاقی و ذائقه‌ی عموم اعضای جامعه، مهم‌ترین لایه‌ی تصرّف در جامعه است (خلف خانی، ۱۳۹۵: ۴۴). و در واقع علاوه بر نگرش کلان و منسجم به نظامات اقتصادی، سیاسی، تربیتی و ...، حرکت تکاملی و اختیاری فرد و جامعه، در سه لایه‌ی فردی، اجتماعی و تاریخی، سرپرستی می‌شود که نیازمند ارتقاء فقه در ناحیه‌ی مبانی کلامی، فلسفه‌ی فقهی و فلسفه‌ی اصولی دانسته شده است (مرتضوی نژاد و میرباقری، ۱۳۹۶: ۱۰). اتخاذ رویکرد فقه حکومتی نتایج متعدّدی دارد که از جمله‌ی آن‌ها، توجه به کارآمدی و میزان اثربخشی احکام و قوانین است؛ که در فقه فردگرا، صرفاً شروط فعلیّت احکام لحاظ می‌شوند؛ و همچنین با این رویکرد، رجوع به اصول عملیه و مخصوصاً «أصل الإحتیاط» بسیار کاهش خواهد یافت. زیرا قوانین حقوقی که به جهت اجرا در محیط جامعه وضع می‌شوند، به صراحت و قاطعیّت نیاز دارند (ضیائی فر، ۱۳۹۰: ۲۵).

بنابراین دو رویکرد فقه حکومتی و فقه فردگرا، در موضوع، هدف، روش و مبانی با یکدیگر تفاوت‌هایی دارند که این اختلاف رویکردی، دارای ثمرات عملی قابل توجهی می‌باشد. و به نظر می‌رسد کشف راهکارهای بستر ساز و ذائقه‌پرور در زایش سبک زندگی و تولّد تمدّن از آن، و در نتیجه تأثیر تربیتی و سرپرستی حاکمیّت بر آحاد جامعه می‌بایست مبتنی بر مبانی انسان‌شناختی، هستی‌شناختی، ارزش‌شناختی و معرفت‌شناختی اسلامی باشد و با هدف پرورش انسان در همه ابعاد جسمی و روحی و همچنین فردی و اجتماعی او صورت گیرد. که این بایسته‌های کلی و اصول تربیت در سطح حاکمیّت به عنوان مرئی و عامل تربیتی و سرپرستی، در ماهیّت و چستی روش‌های تربیتی حاکمیّت تأثیر جدی دارد.

به‌منظور استکشاف مجدد احکام فقهی با رویکرد فقه حکومتی از منابع فقهی‌ای که غالباً با رویکرد فقه فردگرا تولید شده‌اند، انجام اموری لازم دانسته شده است. به‌طور مثال: استخراج مبانی از روبنا به زیرنا و استنباط نظام مقاصد شریعت، استنباط و اتخاذ منطق حجیّت به جهت هماهنگ‌سازی فهم‌های دینی، و استفاده کارآمدتر از عقل و مصلحت (خلف خانی، ۱۳۹۵: ۴۰ و ۴۷؛ غلامی و میراحمدی، ۱۳۹۳: ۱۰۳)، که توجّه به مقوله‌ی تشخیص مصالح احکام اولیه و ثانویه در عین خطیر بودن، حائز اهمیّت بسیار زیادی است؛ تا جایی که رأس هرم فقه اسلامی، مصلحت دانسته شده است (شاگری، ۱۳۹۲: ۱۱۹). البته در فقه شیعه استحسان مبانی استنباط نمی‌باشند و کشف ظنّی مقاصد شریعت، توان اثبات حکم شرعی را ندارد (سبحانی، ۱۳۹۴، ج ۲: ۸۱). اما در هدایت‌گری جامعه به سوی مصالح نفس‌الامری و تولید موضوع احکام، می‌توان توجه به مقاصد شریعت را ضروری دانست. به‌طور مشخص در بحث حاضر، قرار دادن فضای سایبری به منزله فضای زیست حقیقی و ایده گرفتن از بایسته‌های مدیریت فضای فیزیکی برای مدیریت فضای سایبری، یک راهکار مبتنی بر مقاصد شریعت است؛ با این توضیح که مقصود شارع از جعل حکم، تنظیم معاش انسان در شئون زندگی در جهت سعادت بخشی برای اوست، و فهم ارتکازی و عرفی مخاطبین احکام اسلام در بحث اعمال حاکمیّت بر فضای زندگی سایبری، تنزیل مذکور را می‌پذیرد و محل اجرای احکام را فضای زندگی می‌داند؛ درحالی که در استظهار از ادله مربوط به فضای زندگی فیزیکی، الغای خصوصیت می‌کند. البته بدیهی است که در هر تنزیلی چشم‌پوشی از اختصاصات و امتیازات ممکن نیست و موضوع‌شناسی تخصّصی

نسبت به فضای سایبر لازم است.

#### ۵.۴ در مقاصد شریعت اسلامی، تأمین امنیت جایگاه مهمی دارد

بر پایه آموزه‌های قرآن کریم، امنیت یکی از بزرگ‌ترین موهبت‌های الهی است (قریش، ۴؛ نحل، ۱۱۲؛ انفال، ۲۶؛ فصلت، ۴۰؛ انعام، ۸۲)؛ و بسیاری از فقیهان متقدم و فقه پژوهان معاصر، مقاصد اصلی شریعت و وظایف حاکمیت اسلامی در راستای اجرا و عینیت بخشی به شریعت را زیر چتر گسترده و چندبعدی امنیت گنجانده‌اند (صرامی، ۱۳۹۷: ۶۰؛ ورعی، ۱۳۹۷: ۱۲۶). شهید اول و فاضل مقداد قدس سرهما- در استنباطی جامع نسبت به قواعد و ارکان شریعت اسلام، بیان می‌دارند که: شریعت با احکام عبادات، معاملات و قضا و شهادات، برای حفاظت و بقای دین، جان، مال، نسب، و عقل و عقلانیت انسان، و به تعبیر دیگر تأمین امنیت در موارد یاد شده، نازل گردیده است (عاملی مکی، ۱۴۰۰، ج ۱: ۳۴-۳۹؛ حلی سیوری، ۱۴۰۳: ۶۰-۶۳).<sup>۲</sup>

#### ۵ یافته‌های تحقیق

با توجه به مبانی فوق می‌توان گفت: یکی از مطالبات جدی مقام معظم رهبری در سال‌های اخیر، تأمین امنیت همه‌جانبه مردم برای استفاده از فضای سایبر است و این دیدگاه را می‌توان همسو با مقاصد شریعت دانست. همچنین با توجه به تأکیدات ایشان نسبت به امنیت همه‌جانبه فضای سایبر در بیانات و سیاست‌های ششم توسعه، مطالبه ایشان در مورد برنامه‌ریزی برای مدیریت رسانه‌های فراگیر و مسئولیت دستگاه‌های حکومتی در بیانیه گام دوم، قطعاً شامل تأمین امنیت با تمام ابعاد و گونه‌های آن به عنوان وظیفه حکومت اسلامی می‌باشد؛ زیرا در توصیه چهارم بیانیه اعلام می‌دارد که توصیه‌های این بیانیه قبلاً در قالب سیاست‌های کلان بارها تکرار شده است و علاوه بر آن اشاره شد که بیانیه گام دوم مطابق با منظومه فکری ایشان و سایر فرمایش‌ها و دیدگاه‌های ایشان است.

در ادامه مستندات حکم فقهی به وجوب تأمین امنیت در فضای سایبر با رویکرد حکومتی بررسی می‌شود. یکی از مستندات روایی «وجوب تأمین امنیت در فضای سایبر»، فرمایش امیرالمؤمنین -علیه السلام- در باب تأمین امنیت در جامعه مخصوصاً نسبت به راه‌های ارتباطی، است که از وظایف اصلی حکومت اسلامی یاد شده است. ایشان می‌فرماید: «خدایا تو می‌دانی که جنگ و درگیری ما برای به دست آوردن قدرت و حکومت و دنیا و ثروت نبود، بلکه می‌خواستیم نشانه‌های حق و دین تو را به جایگاه خویش باز گردانیم، و در سرزمین‌های تو اصلاح را ظاهر کنیم، تا بندگان ستم‌دیده‌ات در امن و آمان زندگی کنند و قوانین و مقررات فراموش شده تو بار دیگر اجراء گردد» (نهج البلاغه، خطبه ۱۳۱). در این بیان نورانی یکی از اهداف تشکیل حکومت اسلامی تأمین امنیت مردم معرفی شده است. در جای دیگر می‌فرماید: «در حالی که مردم به

<sup>۲</sup> دیدگاه فوق در روایاتی که به فلسفه و حکمت احکام پرداخته‌اند، (نهج البلاغه، حکمت ۲۵۲؛ ابن بابویه شیخ صدوق، ۱۳۷۸ق، ج ۲: ۹۹-۱۳۲؛ و ۱۳۸۵، ج ۲: ۵۹۲)؛ قابل رهگیری و تایید است. مانند روایت مبسوط فضل بن شاذان نیشابوری از امام رضا علیه السلام- که بسیاری از فقها و حدیث‌شناسان همانند شیخ اعظم انصاری (قده) این روایت را صحیح می‌دانند و به آن عمل کرده‌اند (ر.ک: انصاری دزفولی، ۱۴۳۱، ج ۲: ۱۱ و ۴۴).

زامداری نیک یا بد، نیازمندان، تا مؤمنان در سایه حکومت، به کار خود مشغول و کافران هم بهره‌مند شوند، و مردم در استقرار حکومت، زندگی کنند، به وسیله حکومت بیت‌المال جمع‌آوری می‌گردد و به کمک آن با دشمنان می‌توان مبارزه کرد. جاده‌ها امن و امان، و حق ضعیفان از نیرومندان گرفته می‌شود، نیکوکاران در رفاه و از دست بدکاران، در امان می‌باشند» (نهج البلاغه، خطبه ۴۰). در این بیان، لزوم تأمین امنیت راه‌های ارتباطی به صراحت بیان شده است. که با الغای خصوصیت عرفی از راه‌ها و اماکن فیزیکی، می‌توان فضای ارتباطی و زیستی در محیط سایبر را مشمول کلام امام دانست. زیرا عرف مخاطب کلام امام - علیه السلام - با دقت در عناصر قوام‌بخش مفاهیمی همچون فضای زندگی شهری و فضاهای ارتباطی بین شهری، «احساس امنیت از سوی محیط پیرامون» را که مقدمه رفتار ارادی و بندگی آزادانه و مانع تعدی و ظلم می‌شود را عنصر قوام‌بخش می‌یابد، و در نظر عرف، محیط سایبری برای زیستن متناسب خود، با محیط زیست فیزیکی، از حیث تأمین ابعاد امنیتی متناسب هر فضا و در حیطه توان حاکمیت تفاوتی وجود ندارد. وانگهی با توجه به قابلیت‌های فضای سایبری برای تحصیل آگاهی و دانش و یا فعالیت‌های اقتصادی، هیچ تفاوتی میان امنیت حوزه‌های نشریات و یا بازار میان فضای سایبری و غیر آن وجود ندارد. بلکه از جهاتی تأمین امنیت و جلوگیری از ضرر رساندن افراد در فضای سایبری اولویت دارد (طباطبایی و لیالی، ۱۳۹۷: ۹۰ و ۱۰۰)؛ زیرا قابلیت انتشار مطالب با سرعت و وسعت زیاد، همان‌طور که می‌تواند در مسیر توحید و بندگی سهولت و آسانی را به دنبال داشته باشد، می‌تواند به آسانی ضررها و نامنی‌های نظامی، سیاسی، اجتماعی، فرهنگی، اخلاقی، اقتصادی و روانی را به دنبال داشته باشد که نسبت به نامنی‌های مرتبط با فضای فیزیکی بسیار بیشتر است. به طور مثال افشا شدن اسرار محرمانه شخصی در فضای مجازی به طوری گسترده و خارج از کنترل است که اعاده‌ی حیثیت در بسیاری از موارد ناممکن است؛ و یا ترویج خشونت و ارباب مردم در این فضا به آسانی و با گستردگی بسیار بیشتر نسبت به فضای فیزیکی صورت می‌گیرد.

نکته مهم آنکه بدیهی است تأمین امنیت در فضای فیزیکی و یا سایبری، گاهی موجب زحمت مردم و یا محدود شدن حق انتخاب و آزادی ایشان می‌گردد و در زمان صدور نصوص شرعی و عصر معصومین نیز این تقابل امنیت و آزادی به وجود می‌آمده اما در مقام تراحم حقوق (حق امنیت و حق انتخاب و آزادی مشروع، حق فرد و حق جامعه)، امنیت عموم مردم مقدم شده است و ادله وجوب تأمین امنیت از این حیث اطلاق دارند. بله، بر اساس اصل عدم ولایت، حاکم اسلامی تنها به مقدار ضرورت‌های امنیتی می‌تواند آزادی مشروع فردی را فدای امنیت همه جانبه عموم مردم کند.

در ادامه به گونه‌های امنیت و وجوب ایجاد امنیت فضای سایبر با رویکرد فقه حکومتی اشاره می‌گردد.

## امنیت فرهنگی

### الف) امنیت اعتقادی

کتاب ضلال در اصطلاح فقهی، حاوی اطلاعات گمراه کننده‌ای هستند که در سابق تنها به صورت مکتوب بودند و گاهی در میان آن‌ها اطلاعات صحیحی نیز وجود داشته است، اما به طور ضمنی و یا با دلالت التزامی مخاطب را از اعتقادات صحیح دینی منحرف می‌کنند. و می‌توان از روایات دال بر حرمت تولید، نگهداری،

نسخه برداری، انتشار، اجاره، خرید و فروش کتب حاوی مباحث گمراه کننده یا همان «کتب ضلال» (انصاری دزفولی، ۱۴۳۱، ج ۱: ۲۳۳-۲۳۸)، الغای خصوصیت کرده و حرمت امور فوق را در مورد سایتها، کانالها و منابع دیجیتال و اینترنتی گمراه کننده، استنباط کرد. زیرا از نظر عرف مخاطب این روایات میان کتاب کاغذی و کتاب دیجیتال تفاوتی وجود ندارد و هر بستری که کارکرد کتاب و روزنامه و مانند آن را داشته باشد و به تعبیری رسانه محسوب شود، مشمول همین حکم است. بنابراین اگر جلوگیری از انتشار کتب ضلال و حفظ بهداشت فکری جامعه وظیفه حتمی و مورد توافق و تسالم است، ممانعت حکومت از انتشار مطالب گمراه کننده در فضای سایبر نیز با استفاده از پالایش، اختلال سیگنال و مانند آن واجب است.

بلکه می توان گفت غرض شارع مقدس این است که مردم در معرض ارتباط با ویروس اعتقادی قرار نگیرند، و لذا ارتباط با کسی که خودش بدون واسطه کتاب، مردم را گمراه می کند، و خوف از انحراف وجود دارد نیز جایز نیست (خامنه ای، رساله آموزشی: ۳۳۹) و فراهم کردن فضای مناسب برای افرادی که علم داریم در آن فضا مرتکب حرام می شوند، هر چند مجانی، حرام است (انصاری دزفولی، ۱۴۳۱، ج ۱: ۱۲۳ و ۳۸۵؛ ج ۲: ۵۳؛ خامنه ای، رساله آموزشی: ۱۸۷). بنابراین، فراهم کردن بستری که علم داریم، گمراه کنندگان از آن فضا سوء استفاده می کنند جایز نیست؛ بلکه می توان گفت ایجاد چنین بستری [به صورت فعل یا ترک فعل]، از سوی حکومت دارای مفاسد بیشتر و گسترده تری است؛ و به طور مصداقی عدم اقدام جهت کنترل و نظارت فعال نسبت به تأسیس وبسایت، یا گروه و کانال در شبکه های اجتماعی که افراد منحرف اداره می کنند، جایز نیست، هر چند برخی مطالب صحیح هم در آن ها تبادل شود، اما خوف از گمراه کننده بودن در میان مطالب آن ها وجود دارد.<sup>۳</sup>

### ب) امنیت اخلاقی

ادله ی فقهی حرمت فحشا، لهو، غنا و سایر گناهان سمعی و بصری (انصاری دزفولی، ۱۴۳۱، ج ۱: ۱۱۶-۱۱۸ و ج ۲: ۴۱ و ۱۱۷) بدون نیاز به الغای خصوصیت و یا تنقیح مناط، شامل موضوعات این احکام در فضای سایبر می باشند؛ و همان طور که قرار دادن فضای فیزیکی برای انجام گناه یا با علم به انجام گناه، به صورت اجاره و یا مجانی حرام است (انصاری دزفولی، ۱۴۳۱، ج ۱: ۱۲۳ و ۳۸۵؛ ج ۲: ۵۳؛ خامنه ای، ۱۳۹۴: ۱۸۷)، فراهم کردن امکان ارتکاب محرمات فوق و مانند آن در فضای سایبر نیز، با الغای خصوصیت عرفی حرام می باشد؛ و بر اساس قاعده ی «تعزیر» از وظایف حتمی و بدیهی حکومت اسلامی، انجام پالایش و جلوگیری نسبت به انتشار و ترویج هر آن چیزی است که با اخلاق حسنه و مخصوصاً عفت جنسی آحاد جامعه منافات دارد (اسماعیلی و نصراللهی، ۱۳۹۵: ۶۵-۶۷). در حالی که دادن إذن به پیام رسانی های فحشارسان داخلی و خارجی، در حال حاضر در اختیار دولت و حکومت اسلامی است و بر اساس قاعده فقهی «حرمت اعانت و یاری بر گناه» می توان گفت هر چند قصد عرفی بر ارتکاب معصیت را در استفاده از این قاعده شرط بدانیم (انصاری دزفولی، ۱۴۳۱، ج ۱: ۱۳۶)، یا وقوع فعل مورد اعانت را در مفهوم اعانت و یاری قید بنیم (موسوی خویی، ۱۴۳۴، ج ۱: ۲۴۸)، در این جا عرف، مسئولین حاکمیت را دارای قصد شأنی می داند و نگاه کلان و حکومتی به فقه به روشنی بر حرمت سهل انگاری مسئولین در پالایش قضاوت می کند (طباطبایی و لیالی،

<sup>۳</sup> بحث در مورد مرجع قضاوت کننده نسبت به ضلالت اعتقادی افراد و آثار رسانه ای ایشان به جای خود موکول می شود.



۱۳۹۷: ۹۷). از طرف دیگر علاوه بر وجوب نهی و رفع منکر، وجوب دفع منکر مورد تأیید عقل مستقل است و در کلام برخی ستون‌های فقهت مورد استناد واقع شده است (انصاری دزفولی، ۱۴۳۱، ج ۱: ۱۴۱). شیخ اعظم انصاری (قده) معتقد است در جایی که می‌دانیم فردی اهتمام به معصیت دارد و در شرف انجام فعل حرام است، و در صورتی که مانع معصیت او نشویم ارتکاب حرام قطعی است، و مانع ایجاد کردن ما سبب و علت تامه در عدم صدور حرام است؛ از باب قاعده لطف و حکم عقل عملی و همچنین ادله نقلی<sup>۴</sup>، دفع منکر واجب است (انصاری دزفولی، ۱۴۳۱، ج ۱: ۱۴۱-۱۴۳). هرچند برخی فقها این بیان را مطابق ظاهر کلام مشهور دانسته‌اند ولی معتقدند حکم عقل به وجوب دفع منکر فقط در مواردی است که عدم تحقق آن‌ها مورد اهتمام شارع است، مانند تعرض به جان و مال و آبروی محترم و هدم اساس دین و شکسته شدن شوکت و اُبّهت مسلمین، و ترویج بدعت‌های گمراهان (موسوی خویی، ۱۴۳۴، ج ۱: ۲۵۲)؛ و موضوع‌شناسی فقهی نسبت به وضعیت کنونی فضای سایبری غیر بومی، نشان می‌دهد قدر متیقن ذکر شده در کلام محقق خویی (قده) یعنی مفاسدی که نبود آن‌ها مورد اهتمام شارع است، در فضای سایبری رها شده‌ی فعلی رخ می‌دهند.

## ۱.۵ امنیت اجتماعی

### الف) امنیت روانی

به طور کلی تخویف و ترساندن مؤمن از محرّمات الهی است (حرّ عاملی، ۱۴۰۹، ج ۱۲: ۳۰۳؛ انصاری دزفولی، ۱۴۳۱، ج ۲: ۱۰۹) و علاوه بر اخافه مؤمن، بر اساس آیات ۶۰ تا ۶۲ سوره‌ی احزاب، مجازات منافقان و بیماردلانی که با شایعه‌پراکنی و یا انتشار اخبار صحیح اما طبقه‌بندی شده [در مصادیق گوناگون مانند گرانی و یا حمله دشمن در آینده نزدیک و ...] تزلزل، ترس، ناامیدی، دلهره و اضطراب عمومی ایجاد می‌کنند، لعن الهی و اعدام می‌باشد (خسروپناه و دیگران، ۱۳۹۸: ۱۰۴۲) که این مجازات سنگین بر اساس اصل تناسب جرم و جزا و عدل جزائی، نشان می‌دهد ایجاد ناامنی اجتماعی تا چه اندازه مبعوض خداوند و به‌همین میزان امنیت اجتماعی تا چه اندازه باید مورد اهتمام حکومت اسلامی باشد. بنابراین، مقابله پیشگیرانه با اخلال کنندگان به امنیت روانی مردم از وظایف بدیهی حکومت است که تفاوتی میان شکل ظاهری و در فضای فیزیکی و یا سایبری بودن این ایجاد ناامنی وجود ندارد.

### ب) امنیت آبرویی

ادله‌ی فقهی حرمت غیبت، سخن‌چینی، تتبع از لغزش‌های مؤمنین، خار کردن مؤمن، تشبیب و ابراز عشق به زن مؤمن و عقیف و ذکر محاسن او، شایع کردن گناه سّری و پنهان افراد (حرّ عاملی، ۱۴۰۹، ج ۱۲: ۲۷۵-۲۷۹ و ۳۰۶؛ انصاری دزفولی، ۱۴۳۱، ج ۱: ۱۷۷ و ۳۲۷، و ج ۲: ۱۱۱-۱۱۴)؛ شامل ارتکاب این امور در فضای سایبر نیز می‌شود؛ و در صورتی که تخریب شخصیت افراد محترم و تعرض به عرض و آبروی ایشان در فضای سایبر به نحو خصوصی و یا عمومی انجام شود، با شکایت آن فرد، وظیفه‌ی مجازات بر عهده‌ی دستگاه

<sup>۴</sup> «فَقَالَ أَبُو عَبْدِ اللَّهِ ع لَوْ لَا أَنَّ بَنِي أُمِّيَّةَ وَجَدُوا لِهَيْبَةٍ مِّنْ يَّكْتُبُ وَ يَجِبِي لِهَيْبَةِ الْفَيِّءِ وَ يَقَاتِلُ عَنْهُمْ وَ يَشْهَدُ جَمَاعَتَهُمْ لَمَا سَلَبُونَا حَقَّنَا وَ لَوْ تَرَكَهُمْ النَّاسُ وَ مَا فِي أَيْدِيهِمْ مَا وَجَدُوا شَيْئاً إِلَّا مَا وَقَعَ فِي أَيْدِيهِمْ؛ الْحَدِيثُ» (حرّ عاملی، ۱۴۰۹، ج ۱۷: ۱۹۹).

حاکمیت است (ر.ک: ورعی، ۱۳۹۷: ۱۱۸) و ایجاد ساز و کاری که بستر ناامن سازی روانی و آبرویی توسط مجرمان، را ناهموار کند، بر عهده‌ی حاکمیت است (سید باقری، ۱۳۹۷: ۳۰-۴۲).

### ج) امنیت حریم خصوصی

اسلام حریم خصوصی را معتبر شمرده و شرط جواز ورود به حریم مسکونی و اختصاصی غیر را، تحصیل اذن او دانسته است (نور، ۲۷-۲۸ و ۵۹)؛ و با نهی از تجسس، تفتیش، استراق سمع و بصر، و افشاء سر، بر این حکم به شدت تأکید نموده است (حسینی و برزویی، ۱۳۹۶: ۱۱۹-۱۳۱؛ سید باقری، ۱۳۹۷: ۳۴-۳۶). همچنین بر اساس روایات صادر از پیامبر و اهل بیت (علیهم السلام) و اجماع فقها، در صورتی که فردی با نگاهش به حریم خصوصی افراد تجاوز کرده و اشراف و اطلاع حاصل کند و دفع او متوقف بر آسیب جسمانی و یا قتل او شود؛ خون او هدر است (نجفی، ۱۴۰۴، ج ۴۱: ۶۶۰). که این موضوع در مورد فضای سایبر نیز صدق می‌کند و با الغای خصوصیت عرفی، حریم خصوصی کاربران، مشمول این حکم می‌شود (حسینی و برزویی، ۱۳۹۶: ۱۲۶). از این روی، فراهم کردن امکان حفاظت از حریم خصوصی افراد، بر حکومت واجب بوده و عقوبت متجاوزان سایبری به حریم اختصاصی افراد، ضروری است. همان‌طور که پیامبر اعظم (ص) در ماجرای سمره بن جندب، با حمایت از حفظ حریم خصوصی مرد انصاری و خانواده‌اش، دستور به ریشه‌کنی درخت سمره دادند و فرمان حکومتی‌ای صادر کردند تا راه سوء استفاده‌ی متجاوزان و ضرر رسانندگان برای همیشه بسته شود (حر عاملی، ۱۴۰۹، ج ۲۵: ۴۲۹؛ موسوی خمینی، ۱۴۳۱، ج ۳: ۵۳۳).

### د) امنیت اقتصادی

در این مقوله از چند زاویه می‌توان سخن گفت. به‌طور مثال، طراحی قالب و نحوه‌ی دسترسی به صفحات اینترنتی توسط حکومت می‌تواند به‌گونه‌ای باشد که موجب نگرانی کاربر در استفاده از اینترنت و مصرف بیهوده از ذخیره‌ی اینترنت خریداری شده‌ی او گردد. چه به‌صورت کم شدن ناگهانی از ذخیره‌ی اینترنت کاربر در اثر فریب وی توسط برخی اپلیکیشن‌ها، و چه به‌سبب گران‌فروشی دولت به مردم و ارائه‌ی اینترنت در استفاده‌های داخلی اما با اخذ مبالغی متناسب با پهنای باند اینترنت بین‌الملل. در این مورد ایمن‌سازی فضای سایبر، همانند ایمن‌سازی فضای فیزیکی از وظایف حکومت می‌باشد؛ زیرا جلوگیری از هدر رفت سرمایه‌های مردم از وظایف حکومت اسلامی است (انصاری دزفولی، ۱۴۳۱، ج ۲: ۱۰۴-۱۰۶). از زاویه‌ی دیگر، ایجاد بازار تجاری ایمن، از نظر قیمت‌گذاری اجناس، جلوگیری از تدلیس، تغیر، و غش در معرفی کالاها در تجارت اینترنتی، از وظایف اقتصادی حتمی حکومت اسلامی بوده، و تخلف از قوانین حکومتی مستوجب تعزیر است (نهج البلاغه، نامه ۵۳)؛ تا محیط کسب‌وکار امنیت اقتصادی داشته باشد. به‌طور مثال یکی از کسب‌های حرام در اسلام، «نجش» می‌باشد؛ به این معنا که فروشنده با شخص ثالثی توافق کند که او در حین تجارت فروشنده با خریدار، تقاضای خرید کالا با قیمت بالاتر کند و بدین ترتیب قیمت کالا را بالاتر جلوه دهد. این توافق حداقل در جایی که با قصد اضرار به مسلمین صورت بگیرد، حرام بوده و وجهی هم که در قبالتش دریافت می‌شود، حرام بوده و از نظر ضمان در حکم غصب می‌باشد (موسوی خویی، ۱۴۳۴، ج ۱: ۵۹۰؛ انصاری دزفولی، ۱۴۳۱، ج ۲: ۶۱). چنین موضوعی در فضای سایبر هم اتفاق می‌افتد و مفاسد «نجش» یعنی تلبیس و غش (فربکاری)،

و اضرار به مشتری که مناط این حکم هستند، به وضوح مترتب می‌گردند.

### ه) امنیت اطلاعات محرمانه ملی

قاعده‌ی فقهی «نفی سبیل و سلطه‌ی کفار بر مؤمنین» (بجنوردی، ۱۴۳۰، ج ۱: ۱۸۷-۱۹۳)، لزوم حفظ عزت و اقتدار مؤمنین در برابر دشمنان و لزوم تجهیز تمام نیروها در مقابل بیگانگان (منافقون، ۸؛ انفال، ۶۰)، وجوب حفظ اطلاعات اقتصادی، سیاسی، اجتماعی و ... از دستبرد بیگانگان و ممانعت از جاسوسی و شکست اطلاعاتی در فتنه‌های منافقان (توبه، ۴۷؛ و ۱۰۷)، که حتی منجر به تخریب مسجد ضرار شد (سبحانی، ۱۳۸۶: ۸۸۲)؛ ضرورت مقابله‌ی حکومت اسلامی با اشراف اطلاعاتی و انجام عملیات داده‌کاوی بیگانگان<sup>۵</sup> نسبت به مسلمین را ثابت می‌کند؛ و همان‌طور که در فضای غیرمجازی حفظ اطلاعات طبقه‌بندی‌شده در گذشته با طراحی روش‌های نامه‌نگاری امن و استفاده از مهر و مانند آن صورت می‌گرفته، بر اساس موضوع‌شناسی رسانه‌های سایبری و امتیازات این فضا نسبت به فضای غیرمجازی، ایده‌ی شبکه ملی اطلاعات با تعریف خاص آن، یعنی به‌وسیله ایجاد زیرساخت‌ها و امکانات الکترونیکی و ایجاد فضایی برای تشکیل و توسعه اینترنت ملی، راهکار ایجابی مورد استفاده در بسیاری از کشورهاست (کهنوند، ۱۳۹۵: ۲۳-۳۰).

### خاتمه: پیشنهادهایی در جهت تأمین امنیت فضای سایبر

با توجه به اشراف و مدیریت ایالات متحده آمریکا بر ارتباطات اینترنت جهانی و از طرفی باتوجه به مبانی فرهنگی و ایدئولوژیک ملل مختلف و در نتیجه نبود قواعد مسلم و تعریف یکسان از گونه‌های امنیت (محسنی، صوفی زمر، ۱۳۹۶: ۱۶۷-۱۶۸)؛ قدم اول در تأمین امنیت فضای سایبر و استقلال، نسبت به تبادل اطلاعات در داخل کشور، ایجاد اینترنت مستقل و شبکه ملی اطلاعات است تا اختیار مدیریت آن نیز در دست بیگانگان نباشد. با این کار رصد ارتباطات اینترنتی با خارج از کشور هم که کاهش چشمگیری پیدا می‌کنند، ممکن می‌شود و فیلترینگ هوشمند آن نیز موفق‌تر می‌شود. همچنین با توجه به اینکه یکی از عوامل آسیب‌پذیری امنیتی کشورها، هویت پنهان کاربران است (همان: ۱۶۶)، ضروری است تولیدکنندگان اطلاعات و استفاده‌کنندگان نیز دارای شناسنامه و هویت معلوم باشند و همانند فضای فیزیکی، برای نشر مطالب خود و برپایی کرسی تدریس و تجارت، از حکومت اسلامی مجوز بگیرند<sup>۶</sup> و دلایل ضرورت شناسایی هویت افراد در فضای فیزیکی، به طریق اولی در مورد فضای سایبر قابلیت استناد دارند. زیرا همان‌طور که بیان شد، ایجاد نامنی در بستر سایبر آسان‌تر، سریع‌تر و با زبان‌های جبران‌ناپذیرتر رخ می‌دهد. در حالی که همان‌طور که گذشت، این پیشنهادها در سیاست‌های کلی برنامه ششم توسعه و حکم انتصاب اعضای شورای عالی فضای مجازی نیز بیان شده‌اند و لذا می‌توان گفت: سیاست‌های ابلاغی رهبر انقلاب یک مدیریت غیر منفعل و بلکه مبتکر را نشان می‌دهد و صرفاً به برخورد سلبی و انفعالی با اعمال پالایش محدود نمی‌شود؛ در حالی که با دکترین امنیتی و دفاعی اسلامی مطابقت دارد.

<sup>۵</sup> data mining

<sup>۶</sup> راهکار مذکور یک راهکار عقلانی است، همان‌طور که برخی کشورهای غیر اسلامی مانند چین هویت‌نمایی حقیقی کاربران فضای سایبر را ضروری کرده‌اند (۱۳۹۴/۶/۱۸) (<https://www.tasnimnews.com/fa/news/1394/6/18>).



## ۶ نتیجه گیری

با بررسی دیدگاه‌های مقام معظم رهبری بر اساس منظومه فکری ایشان، روشن شد که امنیت همه‌جانبه فضای سایبر که شامل امنیت فرهنگی، اجتماعی، اقتصادی و اطلاعات محرمانه فردی و ملی است، جزء مطالبه مهم ایشان در توصیه دوم بیانیه گام دوم انقلاب اسلامی است و این مطالبه، مستند به گزاره‌های فقه سیاسی است که با رویکرد فقه حکومتی قابل استنباط هستند. همچنین علاوه بر وضع قوانین کیفری بازدارنده، و انجام پالایش هوشمند به عنوان راهکار سلبی، لزوم ایجاد شبکه ملی اطلاعات و شناسنامه‌دار کردن افراد و کرسی‌های علمی، تجاری و خبرگزاری به عنوان راهکار اجباری تأمین امنیت در فضای سایبر پیشنهاد گردید.

## مراجع

- [۱] قرآن کریم.
- [۲] نهج البلاغه.
- [۳] ابن بابویه شیخ صدوق، محمد بن علی، ۱۳۷۸ق، عیون اخبار الرضا، اول، تهران: نشر جهان.
- [۴] ابن بابویه شیخ صدوق، محمد بن علی، ۱۳۸۵ش، علل الشرایع، اول، قم: کتابفروشی داوری.
- [۵] ابن فارس، احمد، ۱۴۰۴ق، معجم مقاییس اللغة، اول، قم: مکتب الاعلام الاسلامی.
- [۶] اسماعیلی، محسن و محمد صادق نصر اللهی، ۱۳۹۵ش، پالایش فضای مجازی، حکم و مسائل آن از دیدگاه فقهی، مجله پژوهشی دین و ارتباطات، سال ۲۳ ش ۴۹.
- [۷] اسماعیلی، محسن، ۱۳۹۷ش، حق بر امنیت و همگانی بودن آن، مجله فقه حکومتی، سال ۲، ش ۵.
- [۸] افتخاری، اصغر و حسن شهباز، ۱۳۹۸ش، کالبد شکافی ابعاد امنیت از منظر آیه الله مهدوی کنی، مجله پژوهشی دانش سیاسی، سال ۱۵، ش ۳۰.
- [۹] انصاری دزفولی، مرتضی، ۱۴۳۱ق، کتاب المکاسب، چهاردهم، قم، مجمع الفکر الاسلامی.
- [۱۰] ایزدهی، سیدسجاد، ۱۳۹۴ش، ماهیت فقه سیاسی، مجله پژوهشی حقوق اسلامی، سال ۱۲، ش ۴۴.
- [۱۱] بجنوردی، محمدحسن، ۱۴۳۰ق، القواعد الفقهیة، چهارم، قم، دلیل ما.
- [۱۲] بهرامی، محمد، ۱۳۸۲ش، قرآن و مسئله امنیت ملی، مجله پژوهشی پژوهش‌های قرآنی، ش ۳۵.
- [۱۳] تیممی آمدی، عبدالواحد، ۱۴۱۰ق، غرر الحکم و درر الکلم، دوم، قم: دار الکتب الاسلامی.
- [۱۴] حاجزاده، هادی و دیگران، ۱۳۹۵ش، جایگاه امنیت نظام سیاسی در فقه امامیه با تأکید بر مرجع امنیت، مجله پژوهشی تحقیقات بنیادین علوم انسانی اسلامی، ش ۳.
- [۱۵] حسینی، مهدی و محمدرضا برزویی، ۱۳۹۶ش، مبانی و مؤلفه‌های فقهی حمایت از حریم خصوصی افراد در فضای مجازی، مجله پژوهشی مطالعات حقوق بشر اسلامی، سال ۶ ش ۱۳.
- [۱۶] حسین نژاد، سید مجتبی و علی اکبر ایزدی فرد، ۱۳۹۶ش، فقه الکترونیک در الگوی اسلامی-ایرانی پیشرفت، مجله پژوهشی مطالعات الگوی پیشرفت اسلامی ایرانی، سال ۵ ش ۹.

- [۱۷] حلی سیوری، مقداد بن عبد الله، ۱۴۰۳ق، نضد القواعد الفقهیه علی مذهب الامامیه، اول، قم: کتابخانه آیه الله مرعشی.
- [۱۸] خامنه‌ای، سید علی، ۱۳۹۷ش، ولایت و حکومت، پنجم، قم: صهبا.
- [۱۹] خامنه‌ای، سید علی، ۱۳۹۴ش، رساله آموزشی ۲، پنجم، قم: فقه روز.
- [۲۰] خامنه‌ای، سید علی، ۱۳۹۴ش، سیاست‌های کلی برنامه ششم توسعه، بنگرید به: نشانی اینترنتی <https://www.leader.ir/fa/content/13369>
- [۲۱] خامنه‌ای، سید علی، ۱۳۹۴ش، حکم انتصاب اعضای شورای عالی فضای مجازی، بنگرید به: <https://www.leader.ir/fa/content/13542>
- [۲۲] خامنه‌ای، سید علی، ۱۳۹۷ش، بیانیه گام دوم انقلاب اسلامی، بنگرید به: نشانی اینترنتی <https://www.leader.ir/fa/content/22734>
- [۲۳] خامنه‌ای، سید علی، ۱۳۹۵ش، بیانات در دیدار با دانشگاه فرهنگیان، بنگرید به: نشانی اینترنتی <https://www.leader.ir/fa/content/14843>
- [۲۴] خامنه‌ای، سید علی، ۱۴۰۰ش، بیانات در دیدار نروزی، بنگرید به: نشانی اینترنتی <https://www.leader.ir/fa/speech/24900>
- [۲۵] خسروپناه، عبدالحسین و دیگران، ۱۳۹۸ش، منظومه فکری حضرت آیت الله العظمی خامنه‌ای، پنجم، تهران: پژوهشگاه فرهنگ و اندیشه اسلامی.
- [۲۶] خلف‌خانی، علی، ۱۳۹۵ش، بررسی و تحلیل مؤلفه‌های نظریات حوزه فقه حکومتی، مجله تخصصی پژوهشنامه فقهی، سال ۴ ش ۲.
- [۲۷] دفانس، کنفیدانسیل، دفانس، ۱۳۸۲ش، آژانس امنیتی ملی آمریکا چگونه جهان را شنود می‌کند، سیاحت غرب، سال اول، ش ۴.
- [۲۸] زاهدی، عاطفه [گردآورنده]، ۱۳۹۶ش، قانون مجازات اسلامی، دهم، تهران: جنگل.
- [۲۹] سبحانی، جعفر، ۱۳۹۴ش، الوسیط فی اصول الفقه، هشتم، قم: امام صادق (ع).
- [۳۰] سبحانی، جعفر، ۱۳۸۶ش، فروغ ابدیت، بیست و پنجم، قم: بوستان کتاب.
- [۳۱] سیدباقری، سیدکاظم، ۱۳۹۷ش، سازوکارهای تأمین امنیت روانی در فقه سیاسی، مجله ترویجی فقه حکومتی، سال ۲، ش ۵.
- [۳۲] شاکری، طوبی، ۱۳۹۲ش، فقه حکومتی فرامذهبی با تحلیل قاعده‌ی التعزیر بما یراه الحاکم، مجله پژوهشی فقه مقارن، سال ۱ ش ۱.
- [۳۳] شبان‌نیا، قاسم، ۱۳۹۵ش، فلسفه سیاست، سوم، قم: مؤسسه آموزشی امام خمینی (ره).
- [۳۴] شریعتمدار جزایری، سیدنورالدین، ۱۳۷۹ش، امنیت در فقه سیاسی شیعه، مجله پژوهشی علوم سیاسی، سال ۳، ش ۹.
- [۳۵] شریفی دوست، حمزه و وحید واحدجوان، ۱۳۹۸ش، درس‌نامه اخلاق در فضای مجازی، اول، قم: معارف.

- [۳۶] صرامی، سیف‌الله، ۱۳۹۷ش، ماهیت فقهی امنیت؛ حق یا حکم؟، مجله فقه حکومتی، سال ۲، ش ۵.
- [۳۷] ضیائی فر، سعید، ۱۳۹۲ش، فلسفه علم فقه، اول، قم: سمت.
- [۳۸] ضیائی فر، سعید، ۱۳۹۰ش، رویکرد فقه حکومتی در فقه، مجله پژوهشی علوم سیاسی، سال ۱۴ ش ۵۳.
- [۳۹] طباطبایی، سید علی‌رضا و محمدعلی لیالی، ۱۳۹۷ش، قواعد فقهی پالایش فضای مجازی در نظام حقوقی جمهوری اسلامی ایران، مجله پژوهشی حکومت اسلامی، سال ۲۳، ش ۱.
- [۴۰] عاملی، سیدسعیدرضا، ۱۳۹۰ش، رویکرد دوفضایی به آسیب‌ها، جرائم، قوانین و سیاست‌های فضای مجازی، اول، تهران: امیرکبیر.
- [۴۱] عاملی مکی، شهید اول، ۱۴۰۰ق، القواعد و الفوائد، اول، قم: مفید.
- [۴۲] غلامی، نجفعلی و منصور میراحمدی، ۱۳۹۳ش، فقه فردی و فقه حکومتی، بایسته‌ها و کاستی‌ها، مجله پژوهشی سیاست متعالیه، سال ۲ ش ۴.
- [۴۳] کهوند، محمد، ۱۳۹۵ش، آسیب شناسی شبکه اجتماعی تلگرام، مرکز مطالعات راهبردی فضای مجازی، دانشکده علوم اجتماعی و فرهنگی دانشگاه جامع امام حسین (ع).
- [۴۴] لکزایی، نجف و میرزا حسین فاضلی، ۱۳۹۷ش، پاسخ به پرسش‌های اصلی مکاتب امنیتی از منظر فقه با تأکید بر دیدگاه صاحب جواهر، مجله ترویجی فقه حکومتی، سال ۲ ش ۵.
- [۴۵] لکزایی، نجف و بهرام دلیر، ۱۳۹۱ش، غایات و اهداف نظام سیاست متعالیه، مجله پژوهشی علوم سیاسی، سال ۱۵، ش ۵۹.
- [۴۶] لکزایی، نجف، ۱۳۹۴ش، گونه شناسی امنیت پژوهی در علوم اسلامی، مجله پژوهشی مطالعات راهبردی، سال ۱۸، ش ۷۰.
- [۴۷] محسنی، فرید و محسن صوفی زمر، ۱۳۹۶ش، پلیس و چالش‌های اجرایی تأمین امنیت سایبری، مجله پژوهشی پژوهش‌های دانش انتظامی، سال ۲۰، ش ۴.
- [۴۸] مرتضوی نژاد، مهدی و سیدمهدی میرباقری، ۱۳۹۶ش، روش‌شناسی فقه حکومتی، مجله تخصصی پژوهش‌نامه‌ی میان‌رشته‌ای فقهی، سال ۵ ش ۲.
- [۴۹] مشکانی سبزواری، عباسعلی و ابوالفضل سعادت، ۱۳۹۲ش، فقه حکومتی نرم افزار توسعه انقلاب اسلامی، مجله پژوهشی مطالعات انقلاب اسلامی، سال ۱۰ ش ۳۲.
- [۵۰] مشکانی سبزواری، عباسعلی و عبدالحسین مشکانی سبزواری، ۱۳۹۰ش، درآمدی بر فقه حکومتی از دیدگاه مقام معظم رهبری، مجله پژوهشی حکومت اسلامی، سال ۱۶، ش ۶۰.
- [۵۱] مصطفوی، حسن، ۱۴۳۰ق، التحقيق فی کلمات القرآن الکریم، سوم، بیروت: دارالقلم.
- [۵۲] موسوی خمینی، روح‌الله، ۱۴۳۴ق، تحریر الوسیله، دوازدهم، قم: جامعه مدرسین.
- [۵۳] موسوی خمینی، روح‌الله، ۱۴۳۵ق، المکاسب المحرمه، چهارم، تهران: نشر آثار امام خمینی (ره).
- [۵۴] موسوی خمینی، روح‌الله، ۱۴۳۱ق، تهذیب‌الاصول [مقرّر: آیه‌الله جعفر سبحانی]، دوم، تهران: نشر آثار امام خمینی (ره).

- [۵۵] موسوی خویی، سید ابوالقاسم، ۱۴۳۴ق، مصباح الفقاهه، دوم، قم: فقاها.
- [۵۶] نجفی، محمد حسن، ۱۴۰۴ق، جواهر الکلام فی شرح شرایع الاسلام، هفتم، بیروت: دار إحیا التراث العربی.
- [۵۷] نظریور، مهدی، ۱۳۸۹ش، آشنایی با قانون اساسی جمهوری اسلامی ایران، بیست و یکم، قم: معارف.
- [۵۸] واعظی، احمد، ۱۳۸۶ش، حکومت اسلامی، پنجم، قم، حوزه علمیه قم.
- [۵۹] ورعی، سید جواد، ۱۳۹۷ش، امنیت از اهداف تشریح، مجله ترویجی فقه حکومتی، سال ۲، ش ۵.

# استراتژی امنیت ملی تعاملی سازنده بر توسعه دانش سایبرنتیک در عصر جنگ سایبری

امین حسنوند<sup>۱</sup>

<sup>۱</sup> وکیل دادگستری و عضو کمیسیون پژوهش مرکز وکلای قوه قضائیه  
amin\_hasanvand@yahoo.com

## چکیده

در قرن حاضر، عنصر «امنیت ملی» از ارزشمندترین و بالاترین ثروت‌هایی است که دولت‌ها همواره به دنبال آن می‌باشند و با تمام توان سعی در اثبات و ابقاء آن دارند. از شاخصه‌های مهم ثبات و پایداری هر حکومت امنیت ملی است و سخن گفتن از امنیت ملی مستلزم برخورداری از توسعه انسانی و توجه به جوانب مختلف سیاسی، فرهنگی و اجتماعی آن است. در عصر حاضر که به عصر اطلاعات و ارتباطات مشهور است یکی از ابزارهای پر قدرت و چالش‌برانگیز در امنیت هر کشور فضای مجازی است که می‌تواند به سهولت تهدیدات و زمینه‌های ناامنی ملل را فراهم آورد. بنابراین با توجه به جهانی شدن ارتباطات و اطلاعات و افزایش نقش فضای مجازی در زندگی مردم جهان، فضای سایبر یکی از منابع مهم کسب، حفظ و افزایش قدرت ملی به شمار می‌آید. از طرف دیگر، در راستای حفظ و ارتقای امنیت ملی جوامع، ضروری است تا عملکرد و تأثیرات فضای سایبر در زمینه‌های ایجاد یا سلب امنیت را مورد بررسی و تحلیل قرار داد تا تأثیرات مثبت و منفی بر جنبه‌های مختلف امنیت ملی را شناسایی نمود. پژوهش حاضر که به صورت توصیفی تحلیلی و در عین حال کتابخانه‌ای انجام شده است بر آن است که ضمن بسط مفهوم امنیت ملی، به بررسی مفهوم دانش سایبرنتیک و کاربرد آن در تعمیم دانش سازمانی و رابطه متقابل و معنادار سایبرنتیک و فرآیند مدیریت دانش می‌پردازد.

**کلمات کلیدی:** سایبرنتیک، امنیت ملی، فضای مجازی، مدیریت دانش.

## ۱ مقدمه

ابتدا به ساکن و قبل از ورود به بطن و بدنه موضوع پژوهش، تلاش نگارنده بر این است که عنصر امنیت ملی را به عنوان بازوان قدرت و سپر میدان نبرد معرفی و سپس استراتژی‌های موثر بر توسعه دانش سایبرنتیک را تجویز و تزریق نماید. امروزه امنیت ملی یکی از ارزشمندترین و بالاترین ثروت‌هایی است که دولت‌ها همواره به دنبال آن می‌باشند و با تمام توان سعی در ایجاد و حفظ آن دارند (حکیم، ۱۳۹۸: ۷). محرز است امنیت ملی به عنوان متغیر وابسته از موضوعات بسیار بزرگ روابط بین‌المللی محسوب می‌شود به طوری که بدون امنیت ملی زندگی با فروپاشی حکومت‌ها از بین خواهد رفت. گرچه این موضوع پیچیدگی‌های خاص خودش

را دارد و نظام‌های سیاسی مختلف بر اساس دیدگاه خود ابعاد متفاوت اقتصادی، نظامی، اجتماعی و فرهنگی یا سیاسی را تهدید یا تعیین کننده امنیت ملی و ضرورت زمان و تحولات در عرصه سیاست بین الملل نقش اساسی در تحول این نگرش‌ها داشته است طوری که اگر در مقطعی، ترس از حمله نظامی و قدرت تهاجمی دولت‌ها باعث تهدید ملی دولت‌ها می‌شد امروزه این مسئله تعدیل شده و ابعاد دیگر امنیت ملی اهمیت بیشتری یافته‌اند و در واقع از جنبه سخت افزاری به سمت عوامل نرم افزاری جهت پیدا کرده است (حاجی زاده، ۱۳۹۸: ۷). در حال حاضر با توسعه فضای سایبری، برقراری امنیت در این فضا به یکی از دغدغه‌های اساسی کشور ما تبدیل شده است. نو ظهور بودن این فضا به همراه سرعت بسیار بالای پیشرفت و توسعه فناوری‌های مرتبط با این فضا، کار کشورها و دولت‌ها را برای برقراری امنیت به چالش کشیده است. علاوه بر موارد ذکر شده، چالش‌هایی نظیر محدود نبودن فضای سایبری به مرزهای فیزیکی کشورها باعث شده تا برای برقراری کامل امنیت در این فضا نیاز به یک همکاری بین المللی قوی نیز وجود داشته باشد. فقدان قوانین و مقررات کامل در کشور در زمینه مدیریت امنیت سایبری، باعث ناشناس ماندن این فضا شده و کار را برای برقراری امنیت سایبری در کشور بیش از پیش چالش برانگیز کرده است (حاجی ملامیرزایی، ۱۳۹۸: ۱۳). طبق یک نقل قول معروف از کارشناسان امنیتی، نشت داده بالاخره اتفاق می‌افتد و هکرها راهی را خواهند یافت تا به سیستم‌های یک شرکت نفوذ کنند اما نکته با اهمیت، میزان خسارتی است که پس از این اتفاق به بار می‌آید. به عبارت دیگر، حمله سایبری و نشت داده، در دنیای کنونی گریز ناپذیر است و فقط با آمادگی قبلی و اتخاذ رویکردهای صحیح امنیتی می‌توان از میزان خسارت آن کاست (بلو و همکاران، ۱۳۹۹: ۶). پس از ذکر مقدمه، نقشه راه این پژوهش در تفسیر مبسوط مفهوم امنیت ملی و مبانی نظری دکترین و تئورسیس‌های عرصه استراتژیک تبلور می‌یابد.

## ۲ طرح مطلب و بیان مسئله

به عنوان قاعده باید قائل به این نظر بود که در حال حاضر اگر جنگی صورت گیرد هیچ مشابهتی با جنگ‌های گذشته نخواهد داشت. در جنگ گذشته، جبهه ما مشخص بود لذا انتخاب تاکتیک‌ها و ابزارهای مبارزه کار سختی نبود. اما در جنگ‌های آینده این جبهه‌ها نامشخص و منشأ حملات نامعلوم است. امروزه با توجه به گسترش فناوری‌های نوین تهدیدات، مخابرات و نقاط رخنه پذیر متعددی به وجود آمده است که اغلب مورد غفلت قرار می‌گیرند به طوری که به منظور حفاظت از امنیت ملی و مقابله با دشمنان سایبری، نیازمند تقویت نیروهای خودی در این گستره و ارتقا توانمندی‌ها در جهت صیانت از فضای سایبر کشور می‌باشیم وانگهی حفاظت از سایبر کشور به عنوان یکی از شریان‌های اصلی اطلاعات در روزگاری که عصر اطلاعات لقب گرفته است به اندازه حفاظت از مرزهای روی نقشه برای هر کشوری حائز اهمیت است. باری، تضمین امنیت و آسایش همواره از بزرگ‌ترین دغدغه‌های حکومت‌ها می‌باشد؛ ضرورت پرداخت به این موضوع در هزاره‌ای که دشمن با استفاده از تمام امکانات ممکن، مترصد تجاوز و رخنه به منظور پیشبرد اهداف سوء خود می‌باشد، امری کاملاً محسوس و ملزوم است (سمیعی، ۱۳۹۷: ۱۰). مشهور است که مهم‌ترین وظیفه دولت‌ها در همه نظام‌های حکومتی، تامین دفاع و امنیت کشور است و لازمه تحقق این رسالت، سیاست دفاعی است تا منبع

قدرت ملی به نحو موثر و هماهنگ در این جهت استفاده شود. بدون شک سیاست دفاعی از اسناد راهبردی مهمی به شمار می‌رود که هدایتگر و راهنمای زمامداران حکومت و مدیران دفاعی و امنیتی در سکانداری ثبات و امنیت کشور است به خصوص در محیط پرچالش و متلاطمی چون غرب آسیا که در کانون اهداف راهبردی قدرت‌های جهانی قرار دارد و عنوان هارتلند فعلی جهان را به خود اختصاص داده است (ریاضی و همکاران، ۱۳۹۸: ۱۳). پس از طرح مطلب و بیان مسئله به منظور پیشبرد ماموریت جاری و با مشایعت عنوان پژوهش، لازم است که صبغه تاریخی و پیشینه استراتژی نظام حقوقی ایران در قبال تهدیدات سایبری بررسی و تحقیق را به طور گذرا در قالب یک بند تلخیص می‌نماییم.

### ۳ پیشینه و مبانی نظری تحقیق

فضای مجازی یا فضای سایر اصطلاحی است که نخستین بار توسط ویلیام گیبسون در داستان علمی تخیلی «نیورومانس» به سال ۱۹۸۴ به کار برده شد و در سال ۱۹۹۰ واژه دنیای مجازی یا فضای مجازی کاربرد بیشتری پیدا کرده است و به کلیه فضاهای سه‌بعدی اطلاق می‌شود. در این دوره استفاده از اینترنت، شبکه و مخابرات دیجیتال سریعاً در حال رشد بود و لفظ «فضای مجازی» می‌توانست بسیاری از ایده‌ها و پدیده‌های نوظهور را نمایندگی کند. لفظ ما در فضای مجازی، سایبرنتیک است که از واژه یونانی *Kubernetes* گرفته شده که «راننده» و «سکاندار» معنی می‌دهد و منشأ واژه «حکمران» است. این واژه توسط نوبرت ویند کمی پس از پایان جنگ جهانی دوم اختراع شد. او بعداً کشف کرد که واژه *Cybernetique* در حدود یک قرن پیش توسط امپراتور به معنای دانش اداره حکومت استعمال شده است (مرادی، ۱۳۹۹: ۱۷). با برش مختصری که از پیشینه تاریخی استراتژی امنیت ملی در فضای سایبر مطرح شد، اکنون به مطالعه موردی و کنکاش تحقیقات انجام شده در این حوزه می‌پردازیم و ماحصل سبق تحقیقات انجام شده در این حوزه را به صورت مختصر و گذرا مستند و رفرنس خواهیم کرد. یکی از مطالبات مبسوطی که در این حوزه به رشته تقریر درآمده است کتاب «پیشگیری از جرایم سایبری علیه امنیت ملی در ایران» نوشته محمد شکری است که ضمن ساختار شناسی فضای سایبر، به علت شناسی جرایم سایبر پرداخته و نهایتاً به بررسی روش‌های پیشگیرانه علیه جرایم اینترنتی در جمهوری اسلامی ایران می‌پردازد. در بخشی از کتاب پیشگیری از جرایم سایبری می‌خوانیم: فضای سایبر و اینترنت جدا از مرزهای جغرافیایی عمل می‌کنند و به اصول خطوطی که دولتمردان در طراحی نقشه‌های سیاسی رسم می‌کنند محدود نمی‌شود. این فضای بی‌پاسبان و رها که هر لحظه بر گستره آن افزوده می‌شود فرصت بسیار مناسبی را برای ارتکاب و اختفای جرایم سایبری به مرتکب اعطا می‌کند و در این فضا هیچ گونه چارچوب اخلاقی، ارزشی یا هنجار مشخصی برای مبارزه و درگیری وجود ندارد (شکری، ۱۳۹۹: ۴۸). در همین راستا مقاله‌ای با عنوان «امنیت ملی در فضای سایبر، فرصت‌ها و تهدیدها با تاکید بر استقرار دولت الکترونیکی» که توسط محمدرضا موحدی تقریر و تحریر شده است که ضمن معرفی ویژگی‌های فضای سایبر، وضعیت کشور را بر اساس آمارهای موجود مورد ارزیابی قرار داده و پس از بررسی مسئله امنیت فضای سایبر، به اولویت بندی در استقرار آن پرداخت و به این اعتقاد است که نشت اطلاعات، سرقت داده‌های حیاتی کشور و آسیب پذیری شبکه‌های جامع اطلاع رسانی به عنوان مهم‌ترین اشکالات امنیتی در این فضا می‌باشد



که اگر از طرف حکومت توجه ویژه‌ای به آن نشود به عنوان یک تهدید جدی برای منافع پایه‌ای کشور تلقی می‌شود (موحدی صفت، ۱۳۸۶: ۷). بدیهی است که با مطالعه کتب، مقالات و ابزار آلات علمی و عملی که آماس تجارب ادوار مختلف است می‌توان به نقطه نظری جامع به منظور توسعه دانش سایبرنتیک پرداخت.

## ۴ متدولوژی و روانشناسی تحقیق

تحقیق فرآیند رسیدن به سوال پژوهش است (سیابیدی، ۱۳۹۶: ۵). هدف از یک پژوهش، تکمیل پاسخ در ازای پرسش مطرح است، علی القاعده با طرح موضوع تحقیق، فرآیند پژوهش رسماً آغاز و انتخاب موضوع مهم‌ترین مرحله تدوین فرآیند پژوهش است. روش پژوهش حاضر کتابخانه‌ای (اسنادی) است که با بهره‌گیری از کتب، مجلات، اینترنت و اینترانت به بررسی، گفتگو و چاره اندیشی کنش فضای مجازی بر جهان متغیر کنونی می‌پردازد که اصل این کنکاش تزریق یک پژوهش مبسوط به عرصه فضای سایبر است.

## ۵ مفهوم شناسی و مبانی نظری

### الف. استراتژی

مشهور است در دوران سخت، بهترین حمله دفاع خوب است (کالکینز، ۱۳۹۳: ۷). استراتژی واژه‌ی پیچیده‌ای است که بی‌نظمی گسترده‌ای ایجاد می‌کند. کتاب‌ها و آثار بیشماری وجود دارد که تلاش کرده‌اند تا با به کارگیری استراتژی در مسائل خاص، اسرار و پیچیدگی آن را آشکار سازند اما در بسیاری از موارد تنها مسئله را پیچیده‌تر کرده‌اند. در مقابل اگر به مفاهیم بنیادین استراتژی فکر کنیم مفهوم این واژه واضح‌تر خواهد شد. مسئله حیاتی که یک استراتژی را تعریف می‌کند این است که استراتژی مستلزم تعامل هوشمند و سازگارانه با دیگران یعنی دوستان، افراد و گروه‌های بی طرف و دشمنان است؛ اما باید توجه داشت که این تعامل اجتماعی نوع خاصی را دراد. هر یک از طرفین درگیر، به طور مستمر جایگاه، نیت و اقدامات خود را بر مبنای ادراکات و اقدامات سایر بازیگران اصلاح می‌کنند. در این خصوص دنیای راز آلود و پنهان نظریه بازی‌ها و حرف‌های مفیدی برای گفتن دارد. این تعاملات «اساساً موقعیت‌های چانه‌زنی هستند که در آن توانایی دستیابی یکی از طرفین، به اهداف، انتخاب‌ها یا تصمیمات سایر طرف‌ها بستگی دارد». (لیتون، ۱۳۹۸: ۲۵). در تعریف استراتژی پلان‌های متفاوتی از سوی اندیشمندان نظام استراتژی ارائه شده است که در این بخش از پژوهش ضمن ارائه دو تعریف جامع از استراتژی، نُه دیدگاه متفاوت از اندیشمندان شهیر این عرصه را مستند می‌کنیم. در تعریف نخست می‌خوانیم: «استراتژی فرضیه‌ای در مورد روابط علی و معلولی بین زنجیره‌ای از متغیرهاست که یک موقعیت بالقوه را هبردی را بالفعل می‌کند». در تعریف دوم آمده است: «استراتژی فرآیندی است جهت تعیین اهداف بلندمدت و راه رسیدن به آن هدف و منابعی که برای این کار تخصیص داده می‌شود». همانطور که اشاره شد عنصر استراتژی مفهومی بس گسترده و باز است که برای به تصویر کشیدن این مفهوم بسیط می‌توان نقشه راهی را ترسیم و به مخاطبان تحویل داد. در همین راستا به منظور شناسایی بیشتر این مفهوم به مبانی نظری اندیشمندان عرصه استراتژیک به طور مختصر گریزی می‌زنیم:

از دیدگاه:

• کاپلان:

استراتژی بدین معناست که سازمان چگونه می‌خواهد برای سهامداران، مشتریان و شهروندان ارزش آفرینی نماید. برای پیاده سازی استراتژی بایستی به بسیج دارایی‌های نامشهود پرداخت.

• فرد آر. دیوید:

هنر و علم تدوین، اجرا و تصمیمات وظیفه‌ای چندگانه که سازمان را قادر می‌سازد به اهداف بلندمدت خود دست یابد.

• جک واش:

استراتژی یعنی این که ما تصمیم‌های شفاف و دقیق در مورد نحوه رقابت با دیگران بگیریم.

• مایکل پورتر:

استراتژی یعنی اینکه کاری که دیگران انجام می‌دهند را با منابع کمتر انجام دهیم و کارهایی انجام دهیم که هیچ کس غیر از ما انجام نمی‌دهند.

• شرون اوستر:

استراتژی داشتن یعنی وقتی مجموعه تصمیمات ما دیده می‌شود بتوان الگوی خاصی را در آن مشاهده کرد.

• آلفرد دی چندلر:

استراتژی یعنی تعیین هدف‌های درازمدت در سازمان و آماده کردن برنامه‌های فعالیتی مناسب و تخصیص دادن منابع مورد نیاز برای تحقق این اهداف.

• هافر و شندل:

استراتژی یعنی فعالیتهایی که تامین کننده هماهنگی بین منابع داخلی و قابلیت‌های سازمان با فرصت و تهدیدهای محیط بیرونی است.

• هنری مینتزربرگ:

مفاهیمی چون استراتژی را نمی‌توان در قالب یک تعریف استراتژی آورد و برای آن باید تعاریف مختلفی را ارائه داد.

• گری پیسانو:

گری بیان می‌کند که استراتژی هیچ چیز به جز تعهد به یک الگوی رفتاری مشخص به منظور پیروی در یک رقابت نبوده و یک فرض اساسی منتج می‌شود که عبارتست از این که چه چیزی موجب پیروزی می‌شود (حاجی میر، ۱۳۹۶: ۷).

### ب. امنیت ملی

«والتر لیپمن» محقق و نویسنده آمریکایی اولین کسی است که مفهوم امنیت ملی را به روشنی تعریف نموده است. وی می‌گوید: یک ملت وقتی دارای امنیت است که در صورت اجتناب از جنگ بتواند ارزش‌های اساسی خود را حفظ کرده و در صورت اقدام به جنگ، بتواند آن را پیش ببرد. «رابرت مک نامار» نیز می‌گوید: اگر امنیت دال بر وضعیتی باشد آن وضع حداقل نظم و ثبات خواهد بود. «ریچارد کوپر» نیز معتقد است که توان جامعه در حفظ و بهره‌گیری از فرهنگ و امنیت ملی است. تعریف دیگری که در این زمینه موجود است در چارچوب منافع ملی است. اگر منافع ملی را مجموعه منافع و اهدافی که دولت‌ها در پی کسب آن هستند بدانیم، حفظ و حراست از دستاوردهای منافع ملی بر عهده امنیت ملی خواهد بود. از سوی دیگر «رابرت ماندل» امنیت ملی را چنین تعریف کرده است: «امنیت ملی شامل تعقیب روانی و مادی و جزء مسئولیت‌های حکومت‌های ملی است تا از تهدیدات مستقیم خارجی نسبت به بقای رژیم، نظام شهروندان و شیوه زندگی شهروندان خود ممانعت به عمل آورند». با توجه به آنچه گفته شد می‌توان نتیجه گرفت که امنیت ملی به فرآیندی زیر اطلاق می‌گردد:

۱. حفظ تمامیت ارضی، حفظ جان و دین مردم، بقا و ادامه سیستم اجتماعی و حاکمیت کشور

۲. حفظ و ارتقا منافع حیاتی کشور

۳. فقدان تهدید جدی از خارج نسبت به منافع ملی و حیاتی کشور

اگر در تعاریف مزبور دقت شود می‌توان چنین برداشت شود که نقطه مشترک در تمام تعاریف فوق، بر ضرورت حفظ وجود خود متمرکز می‌باشد. به عبارت دیگر می‌توان امنیت را «حفظ ذات و صیانت نفس از اساسی‌ترین خطرات» خواند. باری، برخی از صاحب‌نظران حفظ خود یا «صیانت ذات و نفس» را در پنج مقوله زیر خلاصه نمودند:

۱. حفظ جان مردم

۲. حفظ دین، باورها و ارزش‌های مردم

۳. حفظ تمامیت ارضی

۴. حفظ نظام اقتصادی و سیاسی

## ۵. حفظ استقلال و حاکمیت کشور

پنج فاکتور فوق به عنوان جوهره امنیت ملی این پیام را دارد که تمامی کشورها، افراد و گروه‌ها و احزاب بدون توجه به گرایش‌ها، سلیق و اختلافات فردی و گروهی، طبقاتی، سیاسی و اجتماعی روی آن اتفاق نظر دارند (بیات، ۱۳۹۸: ۳۱).

## ج. دانش سایبرنتیک

سایبرنتیک از جمله علمی 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. سایبرنتیک توانسته به عنوان دانشی مستقل و در عین حال علمی بین‌رشته‌ای مطرح شود. در این علم به طبقه بندی و سازماندهی اطلاعات توجه زیادی می‌شود و از این رو در مدیریت اطلاعات و نیز در طراحی نظام‌های اطلاع‌رسانی از اهمیت ویژه‌ای برخوردار است (هوپ و همکاران، ۱۳۹۵: ۴). اگر بخواهیم علم و اصطلاح سایبرنتیک را که در حوزه علوم تجاری روزمره اندکی مجمل است را کالبد شکافی کنیم. باید گفت: سایبرنتیک علم میان رشته‌ای است که با سیستم‌های ارتباط و کنترل در موجودات زنده، ماشین‌ها و سازمان‌ها سر و کار دارد، یعنی سایبرنتیک علم مطالعه و کنترل مکانیزم‌ها در سیستم‌های انسانی، ماشینی «کامپیوترها» است. از زمان هومر تا کنون لغت یونانی کوبرنانتیس معادل سکان‌دار بوده که معادل آن به انگلیسی سایبرنتس است که سایبر نیز بخشی از این کلمه است. اصطلاح سایبرنتیک نیز برگرفته از همین واژه یونانی است که نخستین بار توسط ریاضیدانی به نام نوربرت واینر در کتابی با عنوان «سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین» در سال ۱۹۴۸ به کار برده شده است. از نظر تئوری سایبرنتیک به مطالعه روانشناسی، هوش مصنوعی، علم اقتصاد، عصب‌شناسی، مهندسی سیستم‌ها و مطالعه سیستم‌های اجتماعی می‌پردازد. پیشوند «سایبر» که در مسائل مربوط به کامپیوتر به کار می‌رود بیشتر با انتقال پیام در اینترنت سر و کار دارد. به عنوان مثال لغت مرکب جنگ سایبر که در فرهنگ اصطلاحات جنگ‌های اطلاعاتی مترادف کلمه جنگ اطلاعاتی آمده است، به معنی جنگ از طریق شبکه‌های ارتباطی، علی‌الخصوص اینترنت می‌باشد. باری، انقلاب اطلاعات به گونه‌ای مفهوم نبرد را تغییر داد که پیش از این دیگر شاهد نبرد فرسایشی خونین نیروهای نظامی نخواهیم بود. در عوض، نیروهای کوچک و چالاک که به اطلاعات بلادرنگ ماهواره‌ها و حسگرهای صحنه نبرد مسلح شده‌اند، با سرعت اعجاب‌آوری به محل‌های غیرمنتظره حمله می‌برند. مفروض است اطلاعات در حال تبدیل شدن به یک منبع استراتژیک می‌باشد و تواند خود را به عنوان یک عنصر با نفوذ و ارزشمند در عصر فراصنعتی، همانند نقش سرمایه و کار در عصر صنعتی، همانند نقش سرمایه و کار در عصر صنعتی مطرح کند (میرسمیعی، همان: ۳۱).

## د. نبرد سایبری

بالاترین سطح و پیچیده‌ترین نوع از تهاجم سایبری «عملیات سایبری» است که علیه منافع ملی سایبری کشورها انجام شده است و شدیدترین پیامدها را به همراه خواهد داشت. ویژگی‌های این نوع از تهاجم‌های سایبری، برای آن است که دولت‌ها آن‌ها را جنگ علیه منافع ملی خود تلقی نمایند. جنگ سایبری با جنگ رایانه‌ای یا نبرد مجازی به نوعی جنگ اطلاق می‌گردد که طرفین در آن از رایانه و شبکه‌های رایانه‌ای به خصوص شبکه اینترنت به عنوان ابزار استفاده کرده و نبرد را در فضای مجازی جاری می‌سازند. با توجه به این که جنگ‌های سایبری بعد از زمین، هوا، دریا و فضا، به بعد پنجم جنگ تبدیل شده است بنابراین جنگ سایبری، عبارتست از بهره‌برداری از ابزارها و شبکه‌های اطلاعاتی برای ضربه زدن به دیگران از طریق حمله مخفیانه به زیرساخت‌هاست. جنگ سایبری به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستم‌های اطلاعاتی با هدف به مخاطره انداختن عناصر اطلاعاتی مبتنی بر شبکه‌های رایانه‌ای دشمن در یک فضای سایبری است. چنین عملیاتی به طور مشخص و با اهداف نظامی، تجاری، سیاسی، مالی و ... انجام می‌گیرد. نبرد سایبری در ساده‌ترین تعریف خود عبارتست از به کارگیری کامپیوترها برای حمله به زیرساخت‌های اطلاعاتی دشمن، در عین حفاظت از زیرساخت‌های اطلاعات خودی است. تهدیدات جنگ سایبری می‌تواند دامن گیر بخش‌های مختلف خصوصی و دولتی در هر کشور شود. سرقت اطلاعات راهبردی، اقتصادی، نظامی و ... یا تخریب و از کار اندازی سرویس‌ها و خدمات عمومی یا خصوصی می‌تواند نمونه‌ای از نتایج نبرد سایبری باشد. جنگ سایبری را می‌توان به صورت کلی تحت عنوان حمله عمدی به زیرساخت‌های اطلاعاتی دشمن از طریق استفاده از تکنیک‌های نفوذگری به کامپیوترها در عین جلوگیری کامل از انجام اقدامات مشابه از طرف دشمن تعریف نمود.

## ه. ژئوپلیتیک امنیت سایبری

با رشد و توسعه فناوری و توسعه فضای سایبر که در رأی آن می‌توان به فراگیر شدن شبکه جهانی اینترنت اشاره کرد، فهم جغرافیای مربوط به این فضا و نیز رقابت‌های افراد، گروه‌ها، دولت‌ها و ... در این فضا را می‌توان احساس نمود. در واقع علیرغم بی حد و حصر بودن فضای سایبر به لحاظ مکانی و تحلیل‌های فضایی می‌توان تلاشی را برای شناخت قلمرو سازی در این محیط پیشنهاد نمود و به تبع قلمروهایی که ساخته می‌شود می‌تواند، چه تأثیرات جغرافیایی گذاشته و یا بر تحولات ژئوپلیتیک تأثیر بگذارد؟ پرداختن به این موضوع اولاً منجر به تعریف جغرافیایی و ظرفیت کارکرد ژئوپلیتیکی از فضای سایبر خواهد شد و ثانیاً می‌تواند به تحلیل رقابت‌های مختلف سیاسی، اقتصادی، و اجتماعی که نمود آن در جغرافیای فیزیکی وجود دارد بیانجامد. (پاشایی و همکاران، ۱۳۹۹: ۷). در قرن حاضر، امنیت، بزرگ‌ترین چالشی می‌باشد که زیست بوم فناوری اطلاعات و ارتباطات با آن مواجه می‌شود و با گسترش فناوری‌های کوانتومی، بلاک چین و حمل و نقل هوشمند بر دامنه فراگیری آن افزوده خواهد شد به طوری که طی سالیان اخیر امنیت سایبری جزء پنج مخاطره مهم جسمانی شمرده می‌شود و به عنوان یک روند مهم بنا بر افزایش وابستگی سایبری نقش مهمی در معادلات بین‌المللی دارد (کمالی، ۱۳۹۸: ۷). چرا که امنیت سایبری یک عنصر اساسی برای تحقق اهداف

اجتماعی - اقتصادی اقتصادهای مدرن است (براهیماسانو، ۱۳۹۸: ۳).

از شاخصه‌های مهم پایداری و ثبات و حکومت، امنیت ملی است و سخن گفتن از امنیت ملی مستلزم برخورداری از توسعه انسان و توجه به جوانب مختلف سیاسی، فرهنگی، اقتصادی و اجتماعی آن است. دشمنان هر حکومت برای براندازی آن، از ابزارها و روش‌های مختلفی استفاده می‌کنند تا ثبات سیاسی، فرهنگی، اقتصادی و اجتماعی آن کشور را به چالش بکشند. از آنجا که امنیت کشورها در گرو کسب، حفظ و ازدیاد قدرت می‌باشد در عصر حاضر که به عصر اطلاعات و ارتباطات مشهور است یکی از ابزارهای پر قدرت چالش برانگیز در امنیت هر کشور فضای مجازی است که می‌تواند به سهولت تهدیدات و زمینه‌های ناامنی ملل را فراهم آورد. بنابراین با توجه به جهانی شدن ارتباطات و اطلاعات و افزایش نقش فضای سایبر در زندگی مردم جهان ژئوپلیتیک امنیت و فضای مجازی ترسیم می‌نماییم. در بیان رابطه بین فضای مجازی و امنیت فرهنگی می‌توان ادعان کرد که فضای سایبر به عنوان مولود تعامل انسان با فناوری اطلاعاتی و ارتباطی، امکانات و الگوهای نوینی را برای تعاملات فکری و اندیشه‌ورزی فراروی جوامع عصر کنونی قرار داده است. اگرچه فضای سایبر بدون ارتباطات با واقعیات عینی و معمول در جوامع نیست اما به دلیل فضا، امکانات، زیرساخت‌ها، ابزارها، ویژگی‌های تعاملی و ذهنیت کاربران، گفتمان‌هایی که در آن شکل می‌گیرد ویژگی‌ها و ابعاد و سازکارهای مختص به خود دارد.

بنا به رویکرد «بلومر» بین گفتمان و تکنولوژی رابطه‌ای جداناپذیر وجود دارد. اکنون فناوری‌های اطلاعاتی و ارتباطی، با اثرگذاری بر ابعاد گوناگون ارتباطات، موجب پیدایش پدیده‌ای به نام «فرهنگ سایبر» شده است. در فضای سایبر، الگوهای نوین گفتمانی شکل گرفته است که دامنه و ماهیت آن ناشناخته مانده است. در این فضا به نوعی، موضوع ایجاد فضای کاملاً شخصی، به چالش کشیدن افکار و اندیشه، نضج گرفتن پاره فرهنگ‌های مجازی، تعامل بین فرهنگی، و قواعد گفتمانی مبتنی بر ارزش‌های فرهنگ سایبر مطرح است. کنشگران علمی، فرهنگی و اجتماعی نیز از اینترنت برای پیشبرد راهبردها و بسط الگوهای گفتمانی مورد نظر، از فضای سایبر سود می‌جویند. این مورد در چهارچوب وبلاگستان و شبکه‌های اجتماعی محیط سایبر انجام می‌شود. در حقیقت این باور خواهد بود که غیرقابل تطبیق بودن آنچه در فضای سایبر می‌گذرد با واقعیت بیرونی و وجود فاصله زیاد بین آن‌ها امری خطرناک می‌باشد و پیامدهای خطیری به دنبال دارد. روشن نبودن انواع ابعاد، الگوها، میدان پایداری، حوزه‌های گفتمانی، ماهیت‌های گفتمانی‌های فضای سایبر، از یک طرف و ساز و کارهایی که اینترنت در خدمت این گفتمان‌ها می‌گذارد، از نوع دیگر، موجب ناشناخته شدن قانون ماهیت گفتمان‌ها و فقدان دسترسی به نقشه روشنی از این فضا خواهد شد. به واقع، گفتمان‌های رایج در فضای سایبر و نیز ساز و کارها و ابزار اینترنتی آن، در ایجاد، توسعه و شکل دادن به دانش سهیم می‌باشند. باری، ابعاد تاثیر اینترنت بر شکل‌گیری و توسعه گفتمان در فضای مجازی در بسیاری از جوامع مانند ایران ناشناخته است و هویت و الگوهای این نوع گفتمان‌ها نیز ناشناخته مانده است. (حیدری و همکاران، ۱۳۹۸: ۱۱). یکی از مهم‌ترین نکات تحلیلی در زمینه ژئوپلیتیک، واکنش ممکن نسبت به حمله سایبری یا روش مقابله با آن و همچنین شیوه درک این روش می‌باشد. به عنوان قاعده و اهرم بحث می‌توان گفت: ژئوپلیتیک به روابط میان دولت‌ها و درگیری‌شان با جوامع جهانی و بزرگ‌تر اشاره می‌کند و تاکید ویژه‌ای را بر روی روابط میان جغرافیا و سیاست‌های دولتی دارد. عنصر ژئوپلیتیک وظیفه خود را اختلال در گفتمان‌های ژئوپلیتیکی



می‌داند؛ این حوزه نمی‌خواهد جغرافیای سیاسی را در مکان‌های مشخص مطالعه کند بلکه می‌خواهد پیش زمینه‌های سیاسی را از مناطق جغرافیایی مختلف ارائه نماید. از یک سو، دیپلماسی و سیاست خارجی به عنوان مسائل روشن فکرا نه مطرح هستند که با پنهان کاری همراه خواهند بود. از سوی دیگر و به موازات وابستگی خاصی که به زبان مخصوص خودشان دارند گفتمان در زمینه‌ی امنیت و ژئوپلیتیک، به شکل سنگینی به روایت‌های مشترک در زمینه‌ی مکان‌ها و هویت‌ها بستگی دارد (گیورا، ۱۳۹۸: ۵۱).

## ۵. تروریسم سایبری

یکی از پدیده‌های مهم و بحث برانگیز بین‌المللی، منطقه‌ای و داخلی در دهه نخست سده بیست و یک و یکی از اساسی‌ترین معضله‌ها و چالش‌های جامعه جهانی در خصوص حقوق ملت‌ها و ثبات بین‌المللی مسئله تروریسم بوده است. در عصر ما، تروریسم از تهدید ملی به تهدیدی بین‌المللی و جهانی مبدل شده است و حتی این نگرانی وجود دارد که با گسترش آن صلح و امنیت بین‌المللی به مخاطره می‌افتد. در عصر جهانی شدن و پیشرفت فناوری، دیگر تروریسم در مرزهای ملی و منطقه‌ای محصور نمی‌ماند. تروریست‌ها همگام با روند جهانی شدن، پیشرفت کرده‌اند اما هرگز در قید و بندهای بین‌المللی ناشی از آن گرفتار نیامده‌اند. از این رو هیچ منطقه، دولت یا ملتی از اقدامات آن‌ها در امان نمی‌ماند. گروه‌های تروریستی با انگیزه‌های گوناگون دست به عملیات تروریستی می‌زنند و نگرانی از احتمال وقوع این گونه عملیات زمانی بیشتر می‌شود آنان از تسلیحات هسته‌ای، شیمیایی و بیولوژیک استفاده کنند. هرچند این تهدیدات در حال حاضر، به صورت بالفعل صلح و امنیت بین‌المللی را تخریب می‌کند باید اذعان کرد که تروریسم سایبری، تهدیدی بالقوه علیه جامعه بین‌المللی است که روش نوینی از اقدامات تروریستی به شمار می‌آید و نه گونه دیگری از تروریسم؛ چنان که مجمع عمومی سازمان ملل در سال ۱۹۹۵ با صدور قطعنامه‌ای این موضوع را مورد عنایت قرار داد. تروریسم سایبری که از جمله مصادیق جرایم تروریستی نوین است، زنگ خطری جدی برای تمام مردم دنیا و نیز دولت‌ها تلقی می‌شود. با وجود این، فرآیند برخورد با تروریسم سایبری به نسبت تروریسم کلاسیک و سنتی نه در سطح تقنینی و نه در سطح حمایت‌های اجتماعی، چندان قابل ملاحظه و توجه نیست. مشهور است تروریسم سایبری به مثابه تهدیدی نوین است که گروه‌های تروریستی از اینترنت برای اهداف گوناگونی همچون اطلاع رسانی، تبلیغات، جذب نیروی انسانی و جمع‌آوری اطلاعات استفاده می‌کند. شبکه اطلاع رسانی رایانه‌ای برای تروریست‌های اطلاع رسان، مطلوب به نظر می‌رسد؛ چرا که به دلیل متمرکز نبودن، کنترل یا محدودسازی آن دشوار است و امکان دستیابی را برای هر شخصی ممکن می‌سازد. با این حال به طریق دیگری هم می‌توان هم به عنوان یک ابزار مستقیم برای حمله و هم به عنوان یک صلاح مستقیم از فضای مجازی استفاده کرد (نماین، ۱۳۹۱: ۱۷ و ۱۴). باری، تروریسم سایبری به عنوان گونه‌ای جدید از تروریسم نشانگر آسیب پذیر بودن تابعان حقوق بین‌الملل در فضای سایبر است. اگر تروریست‌ها زیرساخت‌های یک دولت مانند حمل و نقل هوایی، سدها، نیروگاه‌های هسته‌ای و تولید برق، سیستم بانکی و مالی را با انواع بدافزارها مورد حمله قرار دهند و از این طریق باعث رعب و وحشت عمومی می‌گردند و با داشتن انگیزه‌های سیاسی یا ایدئولوژیک این اقدامات را در راستای اجبار دولت یا سازمان انجام دهند آنگاه تروریسم سایبری محقق می‌گردد. در حال حاضر جامعه جهانی بر سر تعریف جامعی از تروریسم به توصیفی دست نیافته‌اند و



حتی سند جامع الزام آوری نیز در این موضوع وجود ندارد اما این شکل از تروریسم به همراه دیگر گونه‌های نوینی چون بیوتروریسم، تروریسم هسته‌ای و اکوتروریسم ممکن است خسارت زیان بارتری نسبت به انواع کلاسیک تروریسم ایجاد کند. بنابراین می‌توان اظهار کرد که تروریسم سایبری تهدیدی علیه صلح و امنیت بین‌المللی است و در عین حال ناقض قواعد حقوق بشر در هر چهار نسل شناخته شده آن به شمار می‌آید (میربد و همکاران، ۱۳۹۸: ۲).

به عنوان طبقه بندی مفهوم و چیستی نبرد سایبری باید قائل و مشعو بر این باور بود که تروریسم سایبری امروزه به نگرانی‌های حقوقی و سیاسی بین‌المللی در زمینه تروریسم اهمیت دو چندانی بخشیده است. شکل فقدان تعریف موجود در تروریسم سنتی بر سر این نوع جدید از تروریست سایه افکنده و آن را با پیچیدگی‌های فزاینده‌ای همراه کرده است. از دیگر سوی، چالش‌های ذاتی فضای سایبر نیز مزید بر علت شده و این اصطلاح را به چالش برانگیزترین مباحث روز مبدل ساخته است. (میرعباسی و همکاران، ۱۳۹۵: ۱۷). چرا که بزرگ‌ترین خطر برای صلح و امنیت ملی و بین‌المللی شمرده می‌شود (شکری، همان: ۹۴). و نفوذگران یا افراد هکر، بارزترین بزهکاران فضای سایبر در زمینه نفوذ و رخنه در دیواره‌های امنیتی ایجاد شده در سیستم‌های رایانه‌ای هستند (حاجی رضایی، ۱۴۰۰: ۲۰).

## ۶ یافته‌ها و پیشنهادها

همان‌طور که پیش‌تر اشاره شد جامعه و مسائل امنیتی همزاد یکدیگر هستند و نمی‌توان جامعه‌ای را تصور کرد که فارغ از مسائل امنیتی و راهبردی باشد. شکل‌گیری دولت‌ها با بروز همین مسائل و بحران‌ها تعریف و تعیین یافته و جمهوری اسلامی ایران هم از این قاعده مستثنی نیست. کشور ایران در بیش از چهار دهه از عمر خود همواره با مسائل امنیتی و راهبردی متعدد داخلی و خارجی روبه‌رو شده است. برخی از این مسائل بنیان‌های وجود جمهوری اسلامی را هدف قرار داده و ضربات سنگینی را بر آن وارد آورده‌اند و برخی به بحرانی مزمن و مخاطره آمیز تبدیل شده است (قاضی زاده، ۱۴۰۰: ۷). در حال حاضر بسیاری از امکانات فنی و تکنولوژی‌های خارجی امروزی که در کشور مورد استفاده قرار می‌گیرد مربوط به سال‌ها قبل بوده که هم اکنون نزد ماست و هرچند معاونت پژوهشی وزیر علوم در مورخه ۲۴ مرداد ماه ۱۳۹۵ اعلام نمود که کشورمان از نظر رشد علمی رتبه سوم جهان را داراست ولی به نظر می‌رسد باید قدمی جهشی برداشته و سبقتی اساسی در علوم فنی بگیریم تا در زمینه‌های سایبری و ... بتوان مقابله کرد. لذا در قالب پیشنهاد، فعالیت‌های ملی و بین‌المللی در آینده بایستی بر موضوعات ذیل متمرکز شود:

- الف.** در زمینه‌های جدید حقوقی باید مطالعات تطبیقی و همکاری بین‌المللی بیش از گذشته گسترش یابد.
- ب.** علوم آکادمیک باید نقش بیشتری در پروسه‌های هماهنگ سازی حقوق ایفا کند.
- ج.** با توجه به فراملی بودن ماهیت جرایم سایبری، لزوم تعاون بین‌المللی در تدوین قوانین و تعقیب بین‌المللی مجرمین سایبری بسیار اهمیت می‌یابد.

۶. مهم‌ترین ویژگی جرایم سایبری در جهانی بودن آن‌هاست که این ویژگی در گرو ماهیت فضای سایبر است. از این رو اگر نگوئیم تنها راه ولی مهم‌ترین راهکار پیشگیرانه از جرایم سایبری، امنیتی همکاری‌های بین‌المللی است.

۷. یکی دیگر از رموز موفقیت سیاست‌های هماهنگ دولت برای مدیریت فضای مجازی، افزایش قدرت سایبری از طریق دکترین و مفاهیم، تجهیزات، آموزش و توسعه و توانمند سازی کارکنان بخش‌های مختلف و مهم سازمان‌های اطلاعاتی و امنیتی برای شناسایی تهدیدات و مقابله با آن در فضای سایبر است (شکری، همان: ۱۶۳).

به هر حال صرف‌نظر از بسط و اطاله کلام، به عنوان پیشنهاد سازنده در راستای تقویت ماشین امنیت ملی کشور در فضای سایبری، اقدامات کشورهای پیشرو در زمینه امنیت سایبری را در قالب نمودار را در پنج بُعد اصیل ترسیم می‌نماییم (شکل ۱).

## ۷ نتیجه‌گیری

امروزه تروریسم سایبری به یکی از چالش‌های عمده نظام‌های حقوقی به خصوص نظام‌های کیفری تبدیل شده است. باری، بزه تروریسم دیگر از رویکردهای سنتی خود رنگ باخته و به سوی فناوری‌های نوین روی آورده است. از همین رو می‌توان گفت که زیرساخت‌های حیاتی و اطلاعاتی به عنوان عمده‌ترین بزه دیدگاه تروریسم سایبری، بیشترین جذابیت و مطلوبیت را برای تروریست‌های دارند. در حال حاضر، فضای سایبر حاصل پیشرفت تکنولوژی بشر در زمینه دیجیتال و علوم رایانه است بنابراین بایستی اظهار داشت که در عصری که ملاک و نژاد فکر برتر بر مدار ارضی دانش سایبرنتیک و گستره حدود و ثغور آن می‌چرخد امنیت مفهومی گیرا و چند بُعدی پیدا می‌کند پرده‌های محدودی واژه امنیت پاره و گدازه‌های آتشفشان عظیم واژگان امنیت بر دامنه و گستره آن فوران می‌کند. در نظم حقوقی کنونی بایستی از معنای تک پر امنیت که تمامیت جامعه را در آفند و پدافند تلخیص می‌کند رها شده و زنجیره‌های محدودیت و اسارت در قفس خودکامگی شکسته و جامعه را در مسیر ایمن کاشت. صرف‌نظر از تعبیر مضیق واژه امنیت در جنگ و میدان نبرد، باید قائل به این نظر بود که امنیت صرفاً در حوزه شلیک و گلوله خلاصه نمی‌شود بلکه یکی از مجاری رگه‌های مهم عنصر امنیت، در تامین آسایش مجازی در راستای القاء تفکرات سازنده در فضای واقعی است. کاربر مجازی باید در امن‌ترین فضای ممکن بتواند به دور از تهدیدات و سرقت‌های هکری یا سیاسی، تخم افکار نوین و متناسب با فرهنگ کنونی را در بطن جامعه کاشته و در اثنا کشمکش‌های مجازی آن را نگاه‌داری، پرورش و در گهواره قانون جامعه تزریق نماید. این مهم جز با تعاون و تعاملات سازنده با دنیای بیرون، شایسته‌گزینی متخصصین امر، تقنین بزه و تعقیب بزهکاران مجازی ممکن نیست.



شکل ۱: اقدامات کشورهای پیشرو در زمینه امنیت سایبری

## مراجع

- [۱] بیات، بهرام، نظریه‌های امنیت ملی، انتشارات دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.
- [۲] چگینی، حسن، نظام مدیریت استراتژیک، جلد اول، انتشارات دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.
- [۳] چگینی، حسن، نظام مدیریت استراتژیک، جلد دوم، انتشارات دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.
- [۴] حاجی رضایی، عسل، جایگاه تروریسم سایبری با نگاهی به اسناد بین المللی، نشر قانون یار، تهران، ۱۴۰۰.
- [۵] حاجی زاده، قباد، امنیت ملی، نشر قانون یار، تهران، ۱۳۹۸.
- [۶] حاجی ملامیرزایی، حامد، قوانین امنیت سایبری، انتشارات دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.
- [۷] حاجی میر، سید ابوالقاسم، نگاهی به مدیریت استراتژیک، انتشارات سخنران، تهران، ۱۳۹۶.
- [۸] حکیم، حمید، غلامی، سعید، منصور قوام آبادی، سهیلا، امنیت ملی و فضای سایبری، نشر پشتیبان، تهران، ۱۳۹۸.
- [۹] حیدری، سعید بیگی، علی، تاثیر فضای سایبری بر امنیت از منظر حقوقی، اجتماعی و سیاسی، نشر فانوس دنیا، تهران، ۱۳۹۸.
- [۱۰] ریاضی، وحید، دهقان، حسین، سیاستگذاری دفاع ملی، انتشارات دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.
- [۱۱] شگری، محمد، پیشگیری از جرایم سایبری علیه امنیت ملی در ایران، نشر قانون یار، تهران، ۱۳۹۹.
- [۱۲] قاضی زاده، علیرضا، مسائل راهبردی امنیت ملی جمهوری اسلامی ایران، نشر پژوهشکده مطالعات راهبردی، تهران، ۱۴۰۰.
- [۱۳] کریمی پاشا، سجاد، بردبار، مهرداد، مقدمه‌ای بر جغرافیای فضای سایبر، دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.
- [۱۴] کمالی، سید تقی، امنیت سایبری، انتشارات پشتیبان، تهران، ۱۳۹۸.
- [۱۵] مرادی، سهیلا، قدسی، سید ابراهیم، نقش فضای سایبری در وقوع جرم، انتشارات ماهواره، تهران، ۱۳۹۹.
- [۱۶] میرسمیعی، سید محمد، اصلی نژاد، مهدی، ماهیت نبرد سایبری، انتشارات پشتیبان، تهران، ۱۳۹۷.
- [۱۷] بلو، الکس، برات اندرو، امنیت سایبر، مترجم کشت ورزه فاطمه، نشر راه پرداخت، تهران، ۱۳۹۹.
- [۱۸] سانو، براهیما، راهنمایی بر توسعه استراتژی امنیت سایبری ملی، ترجمه چمندار، مهدی، فضلی، حسن، نشر ناقوس، تهران، ۱۳۹۸.
- [۱۹] کلکینز، تیم، استراتژی دفاعی برند، ترجمه حیدرزاده، کامبیز، شجاعی، نیما، نشر شرکت چاپ و نشر بازرگانی، تهران، ۱۳۹۳.
- [۲۰] گیورا، آموس، امنیت سایبری: ژئوپلیتیک، قانون و سیاست، ترجمه موسوی، سید علی، نشر نسل روشن، تهران، ۱۳۹۹.
- [۲۱] لیتون، پیترو، استراتژی بزرگ، ترجمه سلیمی، غلامرضا، نشر دانشگاه عالی دفاع ملی تهران، تهران، ۱۳۹۸.

- [۲۲] لوهمان، ولفگانگ، مارکل هابرت، سایبرنتیک، نشر مینوفر، ترجمه رئیسی، سلیمه، تهران، ۱۳۹۵.
- [۲۳] موحدی صفت، محمدرضا، امنیت ملی در فضای سایبر، مطالعات دفاعی استراتژیک، ۱۳۸۶، شماره ۳۰.
- [۲۴] میربد، لیلا، سلیمی، صادق، نیاورانی، صابر، زمانی، سید قاسم، تروریسم سایبری: نقض حقوق بشر و آزادی‌های بنیادین، فصلنامه حقوق پزشکی، ویژه‌نامه حقوق بشر و حقوق شهروندی، ۱۳۹۸.
- [۲۵] میرعباسی، سید باقر، کورکی نژاد فدایی، قابلیت تحقق سایبر تروریسم و ارتباط آن با حق ذاتی دفاع مشروع مقرر در ماده ۵۱ منشور سازمان ملل متحد، فصلنامه مطالعات حقوق عمومی، ۱۳۹۷.
- [۲۶] نامیان، پیمان، مواجهه با تروریسم سایبری در حقوق بین الملل کیفری، فصلنامه پژوهش‌های ارتباطی، سال بیستم، ۱۳۹۲.



# نظام حقوقی مطلوب و حق بر حریم خصوصی در آفند سایبری شبکه‌های مجازی

امین حسنوند<sup>۱</sup>

<sup>۱</sup> وکیل دادگستری و عضو کمیسیون پژوهش مرکز وکلای قوه قضائیه  
amin\_hasanvand@yahoo.com

## چکیده

در قرن حاضر و در هزاره‌ی سوم با انقلاب تولید محتوا روبرو هستیم. طی چند دهه اخیر نهاد خانواده و نظام خویشاوندی متأثر از ورود موجی سهمگین و تحولاتی ژرف در دو سطح رسانه و شبکه‌های مجازی را تجربه کرده است. این پژوهش، گونه‌ی گفتمان حریم خصوصی افراد را در پهنای حقوق شهروندی مورد بررسی قرار می‌دهد تا با مقایسه و ویژگی نظام حقوقی مطلوب، به شناسایی خطوط ناقض حریم خصوصی می‌پردازد. رساله حاضر باشد الهام از واژگان حقوق حریم خصوصی با مطالعه بیش از یکصد مرجع ورود درگاه مستند با روش توصیفی تحلیلی درصدد تفهیم و صیانت از حریم خصوصی افراد در هیاهوی آفات مخرب شبکه‌های مجازی در عصر سایبری است. بازبینی اسناد اخیر این پژوهش اعلان می‌دارد پیشرفت و توسعه یک جامعه در گرو استیفا از یک نظام مطلوب و قانون‌مدار در بستر مجازی است. باری سواد رسانه‌ای یکی از مباحث جذاب در حوزه ارتباطات و به عنوان یک اندیشه‌ی کلیدی مطرح است که در نتیجه آن افراد خود را به رسانه‌ها اعلان می‌نمایند تا معنای پیام‌هایی که با آنها مواجه می‌شوند تعبیر و تفسیر نمایند. باز الهام از مقدرات فوق، خاطرنشان میکنیم که یکی از مهم‌ترین اصول حقوق شهروندی، حفظ داده و اطلاعات کاربری در محیط سایبر است. از همین رو عدم دسترسی به اطلاعات شخصی و عدم سوء استفاده از آن از توجیهات بلیغ تقنینی حقوقی است که تفصیل آن را در پژوهش جاری مورد کنکاش قرار خواهیم داد.

**کلمات کلیدی:** حریم خصوصی، رسانه، سواد رسانه‌ای، شبکه‌های مجازی.

## ۱ مقدمه

حریم خصوصی که از مفاهیم مهم در حقوق مدرن می‌باشد را می‌توان یکی از بنیادی‌ترین و اساسی‌ترین حقوق اخلاقی تلقی کرد که با شخصیت انسان ارتباط تنگاتنگی دارد. نقض این حریم باعث ناامنی روانی و اجتماعی انسان‌ها از هر قشر و دوره‌ای می‌شود و می‌تواند پیامدهای جبران ناپذیری به همراه داشته باشد لذا حمایت از این حریم از ضرورت‌های جدید حقوقی می‌باشد که با توسعه فناوری‌های ارتباطی اهمیت بیشتری یافته است تا جایی که اسناد بین‌المللی هم متوجه این موضوع شده‌اند و موادی را به این مهم اختصاص داده‌اند.



لذا به نظر می‌رسد که علیرغم اهمیت این حق، به عنوان یک اصل تضمین شده در قوانین بسیاری از کشورها از جمله ایران هنوز جایگاه اصلی خود را پیدا نکرده است چرا که به صورت صریح و مشخص حمایت نشده بلکه به صورت ضمنی و در بطن سایر قواعد حقوقی ایران هرچند به صورت ناقص مورد حمایت قرار گرفته‌اند. وانگهی تنها منبعی که به طور صریح بر حمایت حریم خصوصی در نظام حقوقی ایران تاکید دارد «میثاق بین المللی حقوق مدنی و سیاسی» است که دولت ایران به آن ملحق شده است. در چنین وضعی علاوه بر این که تدوین قانون حمایت از حریم خصوصی برای خلأ قانونی در این باره ضرورت دارد. آگاهی دادن و اطلاع رسانی درباره مفاهیم و مصادیق آن و تجربیات سایر کشورها در زمینه حمایت از حق حریم خصوصی، مطالعه تطبیقی قلمرو دخالت دولت‌ها نسبت به حریم خصوصی افراد، سیاست کشورها در قبال ماهواره و اینترنت نیز می‌تواند تاثیر مهمی در مشخص شدن جایگاه این حق در روابط فردی و اجتماعی داشته باشد (میرزایی، امین و همکاران، ۱۳۹۹: ۵). امروزه تحولات عظیمی در تکنولوژی به وقوع پیوسته و شاهد انقلابات بزرگ در زمینه فناوری ارتباطات فراملی طی چند دهه اخیر بوده‌ایم. اینترنت علیرغم تمامی امکانات و اطلاع رسانی در عرصه بین المللی که برای ما به ارمغان آورده است ولی متأسفانه بعضی از افراد سودجو و فرصت طلب با فرا گرفتن مهارت و دانش لازم، راه‌های ورود به سیستم‌های کامپیوتری دولتی و خصوصی را به دست آورده که به موجب بروز مشکلات و خسارات فراوانی گردیده است و با توسعه و تحول اینترنت، در مقابل انقلاب عظیمی در ایجاد جرایم در سطح بین المللی به وجود آمده است لذا در بیشتر کشورهای دنیا جرایم اینترنتی به عنوان یک معضل حاد و بسیار مهم تلقی می‌گردد و دولت‌ها در صدد پیدا نمودن راه حل‌های مختلفی در جهت جلوگیری از وقوع آن می‌باشند (دوکوهکی، محمدرضا، ۱۳۹۶: ۳). در رساله جاری تلاش نگارنده بر این است که با شناسایی خطوط ناقص حریم خصوصی طرق تثبیت و تفهیم حریم خصوصی را تشریح و با بررسی قوانین ایران در زمینه حقوق مخاطب الگوریتم‌هایی به منظور بسط امنیت شبکه‌های مجازی را تجویز و تزییق نماید.

## ۲ طرح مطلب و بیان مسئله

در قرن حاضر اصطلاح «حقوق مخاطب» از جمله حقوقی است که به دلیل گسترش کمی و کیفی رسانه‌های گروهی در سال‌های اخیر مورد توجه صاحب‌نظران حوزه حقوق و رسانه قرار گرفته است. اهمیت این حقوق زمانی دو چندان می‌شود که نقض آن‌ها تبعات منفی بسیاری بر حیثیت و شخصیت افراد وارد می‌کند. از جمله این حقوق حق احترام به حریم خصوصی و حق تصحیح و پاسخگویی اشخاص می‌باشند. باری، یکی از مهم‌ترین و اصلی‌ترین مفاهیم در شبکه‌های اجتماعی «حریم خصوصی» است. علیرغم این که حفظ حریم خصوصی به عنوان یکی از پرکاربردترین حقوق برای هر فردی شناخته شده است هنوز صاحب‌نظران برجسته دنیا نتوانسته‌اند به تعریفی واحد به توافق برسند زیرا تعریف حریم خصوصی در جوامع مختلف، عواملی مثل فرهنگ و زمینه‌های اجتماعی و محیطی که شخص در آن قرار دارد وابسته است لذا گستردگی این مفهوم تا جایی است که گفته‌اند: «تمامی موارد حقوق بشر، جنبه‌ها و ابعادی از حریم خصوصی هستند». در نظام حقوقی جمهوری اسلامی ایران توجه ویژه‌ای به حقوق و آزادی‌های فردی افراد قائل شده و برای صیانت از

احکام و مقررات خود، افزون بر ضمانت اجرای کیفری که در تمامی نظام‌های حقوقی متداول است از ثواب و عقاب نیز به عنوان ضمانت اجرای اخلاقی (مذهبی) بهره می‌برد. در عرصه بین الملل نیز حق حریم خصوصی در کنوانسیون‌ها و اسناد بین المللی و منطقه‌ای حقوق بشر پیش بینی شده است. میثاق بین المللی حقوق مدنی و سیاسی و کنوانسیون اروپایی حقوق بشر و همچنین اعلامیه جهانی حقوق بشر از جمله اسنادی هستند که این حق را مورد شناسایی قرار داده‌اند. در رساله جاری ضمن تشریح مبانی حریم خصوصی در صدد پاسخگویی به پرسش‌های ذیل است:

- در نظام حقوقی جمهوری اسلامی ایران چه قوانین و سیاست‌هایی برای حفاظت از حریم خصوصی اطلاعات اجرا می‌شوند؟
- کدامین اصول زیربنای سیاست‌ها و قوانین مربوط به حفاظت از حریم خصوصی را تشکیل می‌دهند؟
- منظور از فرآیند تاثیرپذیری حریم خصوصی چیست؟

### ۳ پیشینه و مبانی نظری تحقیق

پذیرش و شناخت حریم خصوصی ریشه در تاریخ دارد. در قوانین حمورابی<sup>۱</sup> به این حق توجه شده چنین که: «اگر کسی دیوار منزل دیگری را سوراخ کند و وارد منزل غیر شود عامل را باید در جلو همان دیوار کشت و در همان دیوار مدفون سازند». سقراط نیز معتقد است که برای بشر حقوق مسلمی از قبیل آزادی قائل است پیروی کند. در آنچه که در این دیدگاه مربوط به حریم خصوصی است می‌توان به دو نکته اشاره کرد: ۱. آزادی‌های مسکن و مهاجرت ۲. آزادی فردی.

در انجیل و قوانین یهود نیز از این حق سخن به میان آمده است. دین اسلام نیز برای شان و منزلت انسان ارزش قائل شده و حریم خصوصی را به رسمیت شناخته است. برای مثال در آیات ۲۷ و ۲۸ سوره «نور» می‌خوانیم: «ای کسانی که ایمان آورده‌اید به خانه‌هایی که خانه‌های شما نیست داخل شوید تا اجازه بگیرید و بر آن سلام گوئید. این برای شما بهتر است باشد که پند گیرید». آیه ۲۸ نیز در ادامه می‌فرماید: «و اگر کسی را نیافتید پس داخل آن مشوید تا به شما اجازه داده بشود و اگر به شما گفته شد برگردید، برگردید که آن برای شما سزاوارتر است و خدا به آنچه انجام می‌دهید داناست».

با سیری تطبیقی در تاریخ نظام حقوقی انگلستان رصد می‌کنیم که در سال ۱۳۶۱ میلادی یک قاضی انگلیسی حکم دستگیری کسانی را صادر کرد که دزدانه به خانه افراد سرک می‌کشیدند. در سال ۱۷۶۵ میلادی، لرد کامدن انگلیسی قانونی را وضع کرد که بر اساس آن برای مصادره یادداشت و مکتوبات افراد داشتن مجوز الزامی می‌باشد. در سال ۱۸۵۸ قانونی وضع شد که انتشار مسائل خصوصی را ممنوع کرد (اسدی، عباس، سلطانی سمیرمی، رسول، ۱۳۹۴: ۶۶).

<sup>۱</sup>قدیمی‌ترین و کامل‌ترین قوانین مدنی است که مربوط به حدود چهار هزار سال پیش است که ضمن کاوش‌های باستان شناسی در شوش بین سال‌های ۱۸۹۹ - ۱۹۰۲ توسط گروه «Demargan» فرانسوی کشف شد.

بررسی اصول قانون اساسی جمهوری اسلامی ایران نشانگر این است که عبارت «حریم خصوصی» در هیچ یک از اصول قانون اساسی به صراحت ذکر نشده است اما به طور کلی در مواردی حق بر حریم خصوصی در این قانون به رسمیت شناخته شده است که این حق را می‌توان در چند اصل مشاهده کرد. اصل ۲۲ قانون اساسی مقرر می‌دارد: «حیثیت جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است مگر در مواردی که قانون تجویز کند.» این اصل به وضوح از حریم خصوصی جسمانی، منازل و اماکن شخص حمایت می‌کند و از عبارت «حیثیت» در این اصل می‌توان به حمایت از اسرار شخص حکم کرد.

اصل ۲۳ قانون اساسی مقرر می‌دارد: «تفتیش عقاید ممنوع و هیچ کس را نمی‌توان به صرف داشتن عقیده‌ای مورد تعرض و مواخذه قرار داد». آزادی عقیده عبارت از این است که افراد بتوانند به انتخاب خود، در هر زمینه‌ای اشتغال ذهنی داشته باشند، خواه این اشتغال امری باطنی و درونی و خواه به صورت موضع گیری عمومی باشد یعنی آن که هر کس بتواند به دور از هر تحمیل و فشاری بیندیشد و بدون ترس باور خود را بیان نماید (چقامیرزا، ۱۳۹۵: ۳). امروزه در حوزه موضوع حریم خصوصی در فضای مجازی کتب، تقریرات و مقالات بسیاری تفصیل و منتشر شده است که دامنه مفهوم عنصر حریم خصوصی را گسترده و تحت الشعاع قرار داده است. یکی از مراجعی که عنصر حریم خصوصی را در بطن حقوق مخاطب مطبوعات مورد بحث و بررسی قرار داده است. کتاب «حقوق مخاطبان مطبوعات با تاکید بر حریم خصوصی و حق تصحیح و پاسخگویی» اثر دکتر عباس اسدی و رسول سلطانی سمیرمی است که در بخش اول مفهوم و ماهیت حقوق مخاطب را مطرح و در بخش دوم حریم خصوصی و حوزه‌های آن را به عنوان یک حق اساسی مورد کنکاش قرار داده است که برشی از مطالب کتاب فوق را در رساله حاضر گنجانیده‌ایم. در همین راستا کتاب‌هایی نظیر مسئولیت کیفری و تامین امنیت در فضای سایبر، امنیت در زندگی آنلاین، حریم خصوصی در فضای رسانه‌ای را به رشته تقریر درآورده‌اند. افزون بر مراجع فوق مقالاتی نیز در همین حوزه تقریر شده‌اند که مقاله «صیانت از حریم خصوصی در فضای مجازی بر اساس هنجارهای اسلامی» نوشته فهیمه سعید ساداتی قابل تامل و اشاره است.

## ۴ متدولوژی و روش‌شناسی تحقیق

تحقیق فرآیند رسیدن به سوال پژوهش است (سیابیدی، ۱۳۹۶: ۵). هدف از یک پژوهش، تحلیل پاسخ در ازای پژوهش مطرح است، علی القاعده با طرح موضوع تحقیق، فرآیند پژوهش رسماً آغاز و انتخاب موضوع مهم‌ترین مرحله تدوین فرآیند پژوهش است. روش پژوهش حاضر با توجه به اهداف توصیفی تحلیلی و در عین حال کتابخانه‌ای است. ابزار جمع آوری داده و اطلاعات در این پژوهش تمام اسناد چاپی اعم از کتب، دایرة المعارف، فرهنگ مجله، سالنامه، همایش‌های علمی و فنون چاپی نمایه شده در بانک اطلاعاتی، اینترنت و اینترانت است. پژوهش حاضر به منظور توصیف عینی و کیفی محتوای مفاهیم، به صورت نظام‌دار انجام می‌شود که قلمرو مطالعاتی آن با بهره گیری از بیش از یکصد مرجع و درگاه مستند نظیر کتب، مقالات و مجلات معتبر به تجزیه و تحلیل داده‌های حریم خصوصی در عصر سایبری می‌پردازد.

## ۵ مفهوم‌شناسی موضوعی حریم خصوصی

اصطلاح حریم خصوصی از ترجمه واژه لاتین privacy گرفته شده که به خلوت، پنهان داری، پوشیده داری، پوشیدگی، افتغا، محرمانه بودن، شخصی و خصوصی گفته می‌شود و در معنای خاص آن حریم خصوصی از فرهنگ اروپایی در فرهنگ‌های مختلف راه یافته است. حریم خصوصی در فارسی با تعبیرهای دیگری بیان شده که از جمله می‌توان به حریم شخصی، قلمرو شخصی، چهار دیواری اختیاری و حق خلوت هر فرد اشاره کرد که مقصود از تمامی آن‌ها همان حریم خصوصی است (عبدالصمدی، ۱۴۰۰: ۳).

از بین فهرست موضوعات حقوق بشر، شاید دشوارتر از همه تعریف «حریم خصوصی» باشد. در حقیقت، تعریف حریم خصوصی بستگی تام به فرهنگ و زمینه‌های اجتماعی و محیطی دارد. در بسیاری از کشورها این مفهوم با مقوله حفظ اطلاعات که حریم خصوصی را در معنای مدیریت اطلاعات شخصی تفسیر می‌کنند پیوند خورده و در هم ادغام شده است. «حریم خصوصی» یک مفهوم سیال است که امروزه مواردی از جمله آزادی وجدان و اندیشه، کنترل بر جسم خود، خلوت و تنهایی در منزل، کنترل بر اطلاعات شخصی، آزادی از نظارت‌های دیگران، حمایت از حیثیت و اعتبار خود و حمایت در برابر تفتیش‌ها و تجسس‌ها را شامل می‌شود. دشواری تعریف حریم خصوصی باعث شده است که بر حق نظریه پردازان هویت مستقلی برای حریم خصوصی قائل نشوند و حمایت از آنچه را که به حریم خصوصی موسوم شده است به دیگر حقوق تشبیه شده احاله دهند، بنابراین امروزه دو رویکرد مختلف در مورد هویت استقلالی حریم خصوصی وجود دارد: ۱- برخی صاحب نظران با نظری شکاکانه و انتقادی حق حریم خصوصی را مورد مطالعه قرار می‌دهند. مهم‌ترین ادعای این افراد آن است که حق مستقلی به نام حق حریم خصوصی وجود ندارد و حق مذکور، مفاد و موضوع تازه‌ای ندارد و مطلب خاصی هم نمی‌گوید زیرا می‌تواند هر امری که به عنوان امر خصوصی مورد حمایت حق حریم خصوصی قرار می‌گیرد در قالب دیگر تبع‌ها یا حق‌ها به ویژه حق مالکیت و حق امنیت و حق تمامیت جسمی جای داد. از این گروه به «تحول‌گرایان» یاد می‌شود. در فرانسه و آلمان و سایر کشورهای عضو خانواده «حقوق نوشته» این گرایش غلبه دارد. ۲- بسیاری از نظریه پردازان بر این باورند که حق حریم خصوصی مفهومی مستقل و جدا از سایر حقوق فردی است. این گرایش در انگلستان و آمریکا و سایر کشورهای عضو خانواده حقوقی «کامن لا» غلبه دارد. اینان تعاریف مختلفی از حریم خصوصی ارائه کرده‌اند که این تعاریف را می‌توان در شش دسته کلی آورد:

۱. حریم خصوصی عبارت است از حق بر تنها ماندن
۲. حریم خصوصی یعنی دسترسی محدود دیگران به انسان و توانایی ایجاد مانع در برابر دسترسی‌های ناخواسته و ناخوانده به انسان
۳. حریم خصوصی یعنی محرمانگی و پنهان ساختن برخی امور از دیگران
۴. حریم خصوصی یعنی کنترل بر اطلاعات شخصی
۵. حریم خصوصی یعنی حمایت از شخصیت و کرامت

## ۶. حریم خصوصی یعنی حق بر عالم صمیمیت و کرامت انسان‌ها

در توجیه تعاریف فوق باید قائل به این نظر بود که این تعاریف و برداشت‌ها برای افاده مفهوم حریم خصوصی به وسیله متوسل شده‌اند و برخی به هدف که بین این برداشت‌ها تداخل و هم‌پوشانی وجود دارد (اسدی، عباس، سلطانی سمیرمی، رسول، همان: ۶۶).

به عنوان یک اصل، برخورداری از حریم خصوصی حق آشکار و مسلم هر فردی به شمار می‌رود که داشتن مرز و محدوده در تمام ابعاد زندگی به مثابه یک فیلتر، رفتار و اعمال مورد پذیرش فرد را معین می‌کند لذا ارزش و احترام قائل شدن برای فرد در پرتو وجود حریم خصوصی شخصی امکان پذیر می‌شود. بنابراین چنانچه ارزش قائل شدن برای این حد و حدود کم رنگ شود ارزش، اعتبار و احترامی که دیگران نیز برای فرد قائل می‌باشد به تدریج کمرنگ شده و از بین می‌رود. بر همین اساس افرادی که برای حریم خود هیچ حد و مرزی را ترسیم ننموده‌اند برای حریم خصوصی دیگران نیز ارزش و احترامی قائل نمی‌باشند.

## ۶ ماهیت حریم خصوصی در نظم تطبیقی

### الف. حق حریم خصوصی به عنوان یک حق بشری

حقوق بشر حقوقی هستند که انسان‌ها به صرف انسان بودن و صرف نظر از جنس و نژاد دارند. هدف از این حقوق، حمایت از شأن و کرامت انسان است. این حقوق بر خلاف حقوق طبیعی، ریشه الهی یا طبیعی نداشته و جنبه قراردادی دارند. حقوق بشر در سه مقوله یا نسل دسته بندی می‌شود که حق برخورداری از حریم خصوصی در مقوله مدنی و سیاسی قرار می‌گیرد. این حقوق در زمره حقوق منفی شناخته می‌شوند که تکلیف منفی بر عهده دولت قرار می‌دهند، دولت برای تحقق این حق علی‌الاصول لازم نیست کاری انجام دهد بلکه تکلیف دولت مانع نشدن در برابر اعمال این حق است.

### ب. حق حریم خصوصی به عنوان یک حق اساسی

اهمیت حریم خصوصی به اندازه‌ای است که امروزه تقریباً تمام کشورها این حق را به گونه‌ای صریح یا ضمنی در قوانین اساسی خود پذیرفته‌اند و دست کم به حق قابل تعرض نبودن مسکن و خصوصی بودن ارتباطات اشاره کرده‌اند.

## الگوریتم چندبُعدی حریم خصوصی

حریم خصوصی را می‌توان به چهار حوزه مجزا اما مرتبط با یکدیگر تقسیم کرد:

### ۱. حریم خصوصی اطلاعات<sup>۲</sup>

عبارت است از حق اولیه افراد در محرمانه ماندن و جلوگیری از تحصیل، پردازش و انتشار داده‌های شخصی مربوط به ایشان مگر در موارد مصرح قانونی

<sup>2</sup>Information privacy

## ۲. حریم خصوصی ارتباطاتی<sup>۳</sup>

حق اشخاص در امنیت و محرمانه باقی ماندن محتوای کلیه اشکال و صور مراسلات مربوط به آن. منظور از کلیه صور مراسلات امنیت پست‌های الکترونیکی را نیز شامل می‌شود.

## ۳. حریم خصوصی جسمانی<sup>۴</sup>

حق اشخاص در حمایت و مصون از تعرض بودن تمامیت جسمانی و بدنی از جمله جنبه‌های مرتبط با سلامت جسمانی و روحی و همچنین مشخصات و خصوصیات محرمانه بدنی آن‌ها.

## ۴. حریم خصوصی مکانی<sup>۵</sup>

که به اعمال مجموعه‌ای از محدودیت‌ها و نظارت‌ها در محیط کار و زندگی افراد و همچنین اماکن عمومی مربوط می‌شود. حریم مکانی معمولاً توسط نظارت ویدیویی و یا چک کردن هویت افراد، مورد تجاوز قرار می‌گیرد.

## ۷ توازن حریم خصوصی و آزادی بیان در فضای سایبر

آزادی بیان مستلزم آن است که هر گونه اطلاعات حائز نفع عمومی انتشار یابد اما حق حریم خصوصی ایجاب می‌کند که اطلاعات مربوط به زندگی خصوصی افراد برای دیگران افشا نشود. در نتیجه بین آزادی بیان و حق حریم خصوصی تعارض ایجاد می‌شود. در تعابیر چهارگانه که معمولاً در تدقیق حریم خصوصی به کار می‌رود دو تعبیر به طور خاص به موضوع اطلاعات شخصی به عنوان مصادیق حریم خصوصی دلالت دارند: نخست «حریم اطلاعات» که شامل تصویب قوانینی است که چگونگی دسترسی به اطلاعات شخصی نظیر اطلاعات مالی، پزشکی و دولتی افراد را تعیین می‌کند، دیگری «حریم ارتباطات» که به موضوع امنیت پست‌های الکترونیکی، تلفن‌ها، پست و سایر اشکال ارتباطات توجه دارد (اسدی، سلطانی، همان: ۷۳).

آزادی بیان و آزادی مطبوعات بسیار مربوط و وابسته به هم هستند و هر دو در بند ۱۹ اعلامیه جهانی حقوق بشر آمده‌اند که شرح داده شده است که هر فردی باید آزادی حفظ عقایدش را بدون دخالت داشته باشد و بتواند از طریق رسانه و بدون محدودیت، نظرات و اطلاعات را جست و جو و دریافت کند و از آن بهره‌مند شود. با ظهور رقابت‌های جدید رسانه‌ای، در توازن میان حریم خصوصی و آزادی بیان، چالش‌هایی به وجود آمد. رسانه جمعی با محو کردن مرز میان روزنامه نگاران و مخاطبان‌شان منجر به افزایش وسیع تولید کنندگان خبر شده است. تکنولوژی جدید کار انتشار بدون مرز و بی نام و نشان را سهولت بخشیده است. این پیشرفت‌ها چالش‌هایی را برای قانون رسانه به بار می‌آورد که مانع تعادل میان حریم خصوصی و آزادی بیان می‌شود (وزارت فرهنگ و ارشاد اسلامی، ۱۳۹۳: ۱). باری، حریم خصوصی و حق بر آن یکی از محدودیت‌های فعالین حوزه رسانه محسوب می‌شود. این تعریف در مقابل آزادی بیان قرار می‌گیرد که قوانین و مقررات مدنی و کیفری در پی ایجاد توازن بین دو حق مذکور هستند.

عموماً حریم خصوصی در تقابل با آزادی بیان قرار می‌گیرد. آزادی بیان بر اصل آزادی اطلاعات استوار

<sup>3</sup>Communication privacy

<sup>4</sup>Bodily privacy

<sup>5</sup>Location privacy



است که متأسفانه قوانین و مقررات ایران در این موضوع مرزهای روشنی را تعیین نکرده اما غرب دو رویکرد متفاوت از آزادی اطلاعات دارد که عبارتند از: آزادی مطلق و آزادی محدود. در رویکرد آزادی محدود اطلاعات، حریم خصوصی به شکل تخصیصی از اصل آزادی اطلاع رسانی استثناء شده است. در حالت کلی آزادی اطلاعات دو بُعد اساسی دارد که عبارتست از آزادی اطلاعات و آزادی اطلاع رسانی. در همین راستا برای افراد، حق دسترسی به اطلاعات پیش بینی شده که به نوعی پیش نیاز بعد دوم آزادی اطلاع رسانی است. تعرض به حریم خصوصی اشخاص در فضای مجازی در مقایسه با فضای حقیقی، به دلیل ویژگی این فضا، سهل الوصول تر است. این تعرضات می‌توانند فرامرزی باشند چرا که اشخاص در اقصی نقاط جهان می‌توانند به طور همزمان در فضای سایبری فعالیت داشته و با فعالیت‌های خود، به حریم خصوصی دیگران لطمه وارد کنند. از بارزترین تعرضات فرامرزی می‌توان به اقدامات هکرها و سرقت اطلاعات اشخاص اشاره کرد. با حضور و ظهور شبکه‌های اجتماعی و حضور اشخاص در قالب کاربران شبکه‌های اجتماعی، هویت کاربران در آن شبکه‌ها به اشتراک گذاشته می‌شود و به نوعی حریم خصوصی آن‌ها بیش از پیش در معرض نقض و تعرض قرار می‌گیرد (مهردوست، مریم، موسسه حقوقی اندیشه، ۱۳۹۸: ۱).

آزادی بیان و حریم خصوصی هر دو از بنیادی‌ترین حقوقی هستند که به طور مساوی در اعلامیه جهانی حقوق بشر در معاهده‌های بین‌المللی همچون کنوانسیون اروپایی حقوق بشر و در قانون اساسی بسیاری از کشورها نیز به رسمیت شناخته شده‌اند. اما ارتباط این دو به حق چگونه است؟

باور عمومی بر این است که این دو در تعارض با یکدیگر قرار گرفته‌اند. در بعضی موارد این تعارض اتفاق می‌افتد به خصوص هنگامی که روزنامه‌ای و یا وبلاگی در صدد افشای قسمتی از زندگی خصوصی یک فرد مشهور بر می‌آید مشخصاً زمانی که جزئیاتی از زندگی جنسی یک شخص برملا می‌شود جزئیاتی که فرد مشهور ترجیح می‌دهد فقط بین خودش و اندکی از دوستانش بماند اما در اغلب موارد حریم شخصی لازمه‌ی آزادی بیان است. دوستان و یا معشوقان نمی‌توانند به راحتی و بی‌دغدغه با یکدیگر حرف بزنند مگر اینکه اطمینان یابند که گفتگویشان توسط حکومت شنیده نخواهد شد و یا در رسانه‌های جمعی درز نخواهد کرد. اما چگونه می‌توان تضاد بین آزادی بیان و حریم خصوصی را حل کرد؟ در مواقع ایجاد تضاد قانون قادر نیست از هر دو محافظت کند و هیچ یک به طور کامل تحت حمایت قانون قرار نمی‌گیرد. اگرچه ترجیح حریم خصوصی در اولویت است (بارنت، اریک، آزادی بیان و حریم شخصی، ۱).

## ۸ حق بر حریم خصوصی در نظام حقوقی ایران

در نظام حقوقی ایران حریم خصوصی به صورت مشخص و مصرح مورد حمایت قرار نگرفته است بلکه در بطن قوانین برخی از مصادیق آن که در اصطلاح به حریم خصوصی معروف شده است مورد توجه مقنن قرار گرفته است. مبانی فقهی اسلامی نظام حقوقی ایران، قانون اساسی، قانون مجازات اسلامی، آیین دادرسی در امور کیفری و ... از جمله مقرراتی هستند که از برخی مصادیق حریم خصوصی حمایت کرده‌اند. مجموع احکام پیش بینی نشده در این مواد نشان می‌دهد که قانون‌گذار اولاً تمامی مصادیق حریم خصوصی را به نحوی که در حقوق کشورهای غربی مورد توجه می‌باشد مد نظر قرار نداده است، ثانیاً در قسمت‌هایی که



مورد حمایت قرار گرفته، حمایت‌های لازم و کافی به عمل نیامده و اساسی‌ترین بحث یعنی مسئولیت مدنی ناشی از نقض حریم خصوصی مغفول مانده است. با این اوصاف شاید صرفاً بتوان میثاق بین المللی حقوق مدنی و سیاسی که دولت ایران به آن ملحق شده است را تنها منبعی دانست که در نظام حقوقی ایران به طور صریح بر حمایت از حریم خصوصی در آن تاکید شده است (دفتر وکالت علی محسن زاده، بی‌تا). باری، فلسفه وجودی دستگاه قضا در هر کشوری الزام آحاد آن جامعه به رعایت و اجرا قانون و قانون پذیر کردن جامعه است. گرچه متولیان فرهنگ می‌بایست در جهت فرهنگی در قانون پذیر کردن آحاد جامعه تلاش نمایند (عامری: ۱۳۹۸: ۹). بررسی اصول قانون اساسی جمهوری اسلامی ایران نشانگر این است که عبارت «حریم خصوصی» در هیچ یک از اصول قانون اساسی به صراحت ذکر نشده است اما به طور کلی در مواردی حق بر حریم خصوصی در این قانون به رسمیت شناخته شده است. این حق را می‌توان در چند اصل مشاهده کرد: اصل ۲۲ قانون اساسی مقرر می‌دارد: «حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است مگر در مواردی که قانون تجویز کند». این اصل به وضوح از حریم خصوصی، جسمانی، منازل و اماکن شخص حمایت می‌کند و از عبارت «حیثیت» در این اصل می‌توان به حمایت از اسرار شخص حکم کرد. در همین راستا اصل ۲۳ قانون اساسی مقرر می‌دارد: «تفتیش عقاید ممنوع و هیچ کس را نمی‌توان به صرف داشتن عقیده‌ای مورد تعرض و مواخذه قرار داد». آزادی عقیده عبارت از این است که افراد بتوانند به انتخاب خود، در هر زمینه‌ای اشتغال ذهنی داشته باشند خواه این اشتغال امری باطنی و درونی خواه به صورت موضع گیری عمومی باشد؛ یعنی آن که هر کس بتواند به دور از هر تحمیل و فشاری، بیندیشد و بدون ترس، باور خود را بیان نماید. با وجود آن که آزادی عقیده به عنوان یک حق طبیعی مسلم قابل درک است ولی دارای آنچنان تبعات فردی، اجتماعی، سیاسی، اخلاقی و ارزشی است که هم در عالم واقع، مواجهه به برخوردهای متفاوت است و هم اینکه در نظام‌های سیاسی و حقوقی برای انتظام آن تدابیری اتخاذ شده است (چقامیرزا، ۱۳۹۵: ۳).

امروزه در عصر فناوری اطلاعات و با توسعه فضای مجازی، حریم خصوصی بیش از هر زمان دیگری در خطر است و در این میان شبکه‌های اجتماعی از وضعیت ممتازی در باب اخذ، جمع آوری و استفاده از اطلاعات اشخاص در فضای مجازی برخوردارند. این شبکه‌ها با رصد کردن رفتار افراد در شبکه و افزودن این اطلاعات به بانک داده خود، مجموعه‌ای از اطلاعات را جمع آوری کرده و از طریق داده کاوی، پروفایل‌های شخصی برای اعضا می‌سازند که حاوی اطلاعات بسیار زیادی از زندگی خصوصی افراد است و به این ترتیب به حریم خصوصی تعداد بیشتری از مردم جهان وارد می‌شوند. لذا حساسیت نسبت به نقض حریم خصوصی در فضای دیجیتال در سطح بین المللی، منطقه‌ای و ملی ایجاد شده ولی هنوز مقررات کافی برای حفاظت مناسب از حریم خصوصی وجود ندارد که این فقر قانونی در نظام حقوقی ایران چشمگیرتر بوده و نیاز به تصویب مقررات حمایت کننده از حریم خصوصی احساس می‌شود (حبیبی، حق بر حریم خصوصی در شبکه‌های اجتماعی: ۱).

## ۹ آفند سایبری شبکه‌های مجازی

مدت‌هاست که رسانه‌های اجتماعی، فقط ابزاری برای انتشار عکس‌های تعطیلات یا گربه خانگی کنار شومینه نیست. هر کس به رایانه یا تلفن هوشمند دسترسی داشته باشد به راحتی می‌تواند از ابزارها و اپلیکیشن‌های رسانه اجتماعی به عنوان سلاحی موثر در مناقشات و اختلافات استفاده کند به طوری که تعداد این افراد روز به روز در حال افزایش است. از این رو نهادهای نظامی و حاکمیتی باید به طور موثرتر استفاده دشمنان خود از رسانه اجتماعی باشند با حملات رسانه اجتماعی پیش رو مقابله کنند و از رسانه اجتماعی به عنوان سلاحی برای تحقق اهداف خود بهره بگیرند. آموختن فرآیند حملات تهاجمی در رسانه اجتماعی برای دامن زدن به شورش‌ها یا کنش‌های اجتماعی به صرف زمان چندانی نیاز ندارد اما خبره شدن در این کار، درست مانند دیگر راهبردها و تاکتیک‌های جنگی، نیازمند تلاش و مطالعه قابل توجهی است (مهدیان و همکاران، ۱۴۰۰: ۲). در عصر کنونی گسترش تکنولوژی‌های حوزه رسانه و افزایش داده‌های ارتباطی، رسانه را به ابزاری جنگی و نفوذی تبدیل کرده است که سلاحی قدرتمند در دست حاکمان سیاسی قرار می‌دهد. قدرتمندان عرصه سیاست با استفاده از این وسیله اهداف و منافع خود را پیگیری می‌کنند و بدون به راه انداختن جنگ‌های پیر سر و صدا به شکلی نرم و نامحسوس رقیبان خود را شکست می‌دهند. لذا اصطلاح «جنگ نرم» یک کلیدواژه شناخته شده در علوم سیاسی است که به درگیری‌های بدون آتش و خونریزی در بین حکومت‌ها اطلاق می‌شود. وسایل به کار رفته در جنگ نرم کاملاً با ابزارها و سلاح‌های جنگ سخت متفاوت است. رسانه‌ها به ویژه برنامه‌های کانال‌های خبری، فرهنگی و سیاسی به عنوان ابزار جنگ نرم مورد استفاده سیاستمداران، دولت‌ها و حتی ارتش‌های بزرگ جهان قرار می‌گیرند.

## ۱۰ نتیجه‌گیری

مشهور است جهان مجازی محیطی پایدار، ترکیبی و آنلاین مبتنی بر رایانه است که می‌تواند به صورت همزمان در دسترس میلیون‌ها نفر قرار گیرد که با فرآیند رشد هندسی خود مسائل مرتبط با زندگی انسان‌ها را به چالش طلبیده و مسائل جدی را در علوم موجود مطرح کرده که با تئوری‌ها، ایدئولوژی‌ها و دانش‌های قبل قابل پاسخگویی نیست و انگهی دسترسی به فضای مجازی پاکیزه و امن، تدوین قانون جامع با تلفیقی از تنقیح و تقنین را می‌طلبد؛ لهذا تاسیس یک نظام حقوقی مطلوب و قانون جامع اینترنت و فضای مجازی باید در فرآیند متشکل از تنقیح (تجمیع و بازنویسی قوانین قبلی در قالب قانون کلی) و تضمین شکل بگیرد تا از جامعیت رافع مشکلات برخوردار باشد. باری، نظامات حقوق ارتباطات و رسانه شامل نظام مالکیت و تاسیس، نظام مقررات گذاری و نظام جرم انگاری بیشتری است متعالی که با نقد و بررسی اجمالی نظامات برای رسانه‌های نوین اهمیت بازنگری در قوانین، مقررات و نظام حقوقی کشور را گوشزد می‌نماید.

لهذا با نگاهی به مسیر پر پیچ و خم و ناکام سال‌های اخیر، برای تدوین قانون جامع رسانه‌های همگانی کشورمان مفروض است که تحقق این آماج بدون استفاده از توان و نظرات کارشناسان و فعالان این حوزه‌ها دشوار و شاید غیرممکن باشد. تدوین نظام جامع حقوقی اینترنت و فضای مجازی نیز از این قاعده مستثنی نیست. در این زمینه باید تیمی فعال با حضور کارشناسان خبره و مدیران همه نهادهای دست اندرکار به عنوان

هیئت اندیشه‌ورز تشکیل شود. مرکز پژوهش‌های مجلس یا دبیرخانه شورای عالی فضای مجازی می‌توانند نقش هسته مرکزی را در فرآیند تدوین این نظام حقوقی جامع ایفا کنند اما حضور موثر سایر نهادهای مربوطه برای کارشناسانه‌تر شدن محتوای حاصل ضروری است علی‌حال نباید از توان فعالان بخش خصوصی این عرصه نیز غفلت شود چرا که مردمی‌تر بودن فرآیند مقررات‌گذاری ضمانت اجرای سند حقوقی حاصله را ارتقا خواهد بخشید. از نظر نگارنده پژوهش، بستر برخط فضای مجازی و متعلقات آن به مثابه شمشیری دو لبه برهنه و بزران است که سازنده یا کوبنده بودن آن بستگی به هنر مبارز و خط مشی سیاسیون حاکم دارد. در این ورطه به شدت حساس و شکننده، هر گونه افراط و تفریط از جانب سیاسیون و غیر متخصصین، کاشتن تخم جهالت و ظهور هیولا کرنش‌گر می‌باشد که خوراک و طعمش با تاختن در شبکه‌های مجازی و شکار نوجوانان و کاربران با حُسن نیت تامین می‌گردد. هر چقدر سیاست حقوقی و قضایی در عرصه مجازی و انتفاع از آن تخصصی و فارغ از نظرات خام و دیکتاتوری باشد این فضا، آسمان پرواز و سکوی تعامل و تکامل یک جامعه بالغ است. برعکس چنانچه سیاست و خط مشی حاکم بر این گُرسی، غیرتخصصی و قبيله‌ای باشد فضای مجازی به عنوان ابزاری توفنده و ویرانگر در استیلاء غول‌های مجازی دنیا خواهد بود.

## سپاسگزاری

تشکر و سپاس بی پایان مخصوص خدایی است که بشر را آفریده و به او قدرت اندیشیدن داده و توانایی‌های بالقوه را در او به وجود آورد و او را امر به تلاش و کوشش نموده و راهنمایی را برای هدایت بشر فرستاده است. پس از ارادت خاضعانه در پیشگاه پروردگار، نگارنده پژوهش جاری، از کمال اهتمام و همفکری برگزارکنندگان کنفرانس فضای سایبر در دانشکده‌گان فارابی دانشگاه تهران که در پیشبرد اهداف در محیط پژوهش دلسوزانه سعه صدر به خرج دادند صمیمانه کمال تشکر و قدردانی را دارم.

## مراجع

- [۱] اسدی، عباس، سلطانی سمیرمی، رسول، حقوق مخاطبان مطبوعات، نشر آوای نور، تهران، ۱۳۹۴.
- [۲] چقامیرزا، سونیا، جرم شناختی حریم خصوصی اماکن و اشخاص، نشر قانون یار، تهران، ۱۳۹۵.
- [۳] دوکوهگی، محمدرضا، بررسی جزایی جرایم رایانه‌ای و سایبری، نشر قانون یار، تهران، ۱۳۹۶.
- [۴] رضایی سیابیدی، راهکارهای مبارزه با جرائم اداری و فساد اقتصادی در سازمان‌های دولتی، نشر قانون یار، تهران، ۱۳۹۶.
- [۵] عامری، آرزو، جایگاه پلیس در پیشگیری از جرایم سایبری و اینترنتی، نشر قانون یار، تهران، ۱۳۹۸.
- [۶] عبدالمحمدی، محمد، گستردگی و محدودیت‌های حریم خصوصی، نشر آرمان ارشد، ۱۴۰۰.
- [۷] میرزایی، امین، آقابابائیان، اکبر، درایتی، حامد، حکومت و حریم خصوصی افراد، نشر قانون یار، تهران، ۱۳۹۹.
- [۸] حبیبی، همایون، حق بر حریم خصوصی در شبکه‌های اجتماعی، وزارت علوم، ۱۳۹۵.

- [۹] جایگاه حریم خصوصی در قوانین ایران و بین الملل، وب سایت دفتر علی محسن زاده، ۱۴۰۰/۰۳/۰۵، مشاهده شده در تاریخ ۱۴۰۱/۰۵/۱۹، قابل دسترسی در [www.alimohsenzadeh.com](http://www.alimohsenzadeh.com).
- [۱۰] چالش های حریم خصوصی، آزادی بیان و آزادی مطبوعات، وزارت فرهنگ و ارشاد اسلامی، سامانه شفاف سازی، ۱۳۹۳/۱۰/۱۳، مشاهده شده در تاریخ ۱۴۰۱/۰۵/۱۶ قابل دسترسی در [www.cfoio.farhang.ir](http://www.cfoio.farhang.ir).
- [۱۱] نظام حقوقی جامع اینترنت و فضای مجازی کشور، وبسایت گرداب، بی تا، مشاهده شده در تاریخ ۱۴۰۱/۰۵/۱۷ قابل دسترسی در [www.gerdab.ir](http://www.gerdab.ir).
- [۱۲] نظام حقوقی مجازی، وبسایت بیستا، بی تا، مشاهده شده در تاریخ ۱۴۰۱/۰۵/۱۸، قابل دسترسی در [www.vista.ir](http://www.vista.ir).

# خلوت عالم‌سازی یا جلوت فرهیخته‌ساز (بررسی مؤلفه گمنامی یا هویت‌مندی در فرآیند عمومی‌سازی علم)

سید محمد مهدی شرف‌الدین<sup>۱</sup>

<sup>۱</sup> دانشجوی دکتری، دانشکده علوم اجتماعی (رشته فلسفه علوم اجتماعی)، دانشگاه باقرالعلوم (ع)، قم  
sharafoddin614@gmail.com

## چکیده

صاحبان علم در هر دوره‌ای از تاریخ بشریت، به دنبال آن بودند تا دستاوردهای خود را با مردم جامعه به اشتراک گذاشته و مسائل را به گوش آنان برسانند. در دوران سنتی این فرآیند از طریق ارتباطات خصوصی و رسانه‌هایی همچون کتاب و منبر (خطابه) صورت می‌پذیرفت؛ اما در دوران مدرن و پست‌مدرن، با پیدایش رسانه‌های آنالوگ و دیجیتال، فرآیند عمومی‌سازی علم، سرعت و وسعت بیشتری پیدا کرده و محدودیت‌های زمانی و مکانی خود را از دست داد. یکی از تفاوت‌های مهم این سه دوره را می‌توان در مقوله گمنامی عالم سنتی و هویت‌مندی اندیشمند معاصر دانست. پژوهش حاضر به دنبال کشف علل این تفاوت است که از آن جمله می‌توان به تغییر ماهیت علم، تغییر ماهیت رسانه و همچنین تغییر هدف از عمومی‌سازی علم اشاره کرد. در دوران سنتی علم به مثابه کشف حقیقتی است که در عالم نفس‌الامر حضور داشته و از طریق فیضان الهی، به عقل و نفس بشری وارد می‌شود؛ اما در قرائت جدید علم برداشتی شخصی است که خود انسان سازنده آن خواهد بود. علاوه بر این در دوران سنتی، رسانه منبر به خودی خود توانایی خاصی نداشته و قوام آن به توانایی خطیب در تهنذب و جذب مخاطب است؛ اما در دوران معاصر به دلیل کارکرد برندسازی بالای رسانه‌ها، این صاحبان علم هستند که قوام خود را به رسانه‌ها دانسته و به سراغ فراگیری تمام تکنیک‌های کسب شهرت می‌روند. مضاف بر این که در دوران سنتی هدف از عمومی‌سازی علم، هدایت بشر و نشان دادن راه صحیح زندگی به اوست؛ اما در دوران معاصر این هدف به کسب هویت و شهرت برای شخص منتشرکننده مبدل می‌گردد.

**کلمات کلیدی:** عمومی‌سازی علم، گمنامی، هویت‌مندی، برندسازی، هدایت.

## ۱ مقدمه

وجود قوه ناطقه در ذات بشر، همواره او را به سمت کشف حقایق و یادگیری بیشتر می‌کشاند. انسان هیچگاه از آموختن سیر نشده و خیالش آرام نمی‌گیرد؛ از این رو مدام به دنبال راه‌هایی می‌گردد که معرفت خود را افزایش داده و درهای بیشتری از علم را در برابر خود بگشاید. در گذشته هم به دلیل قلیل بودن حوزه‌های

علمی، هم به دلیل نگاه جامع‌الاطراف که عرف جامعه به انسان حکیم و عالم داشت و هم به دلیل وجود نگاه طبقاتی به علم، یک نفر به سراغ فراگیری همه علوم مورد نیاز جامعه رفته و به عنوان مرجع عرف معرفی می‌شد. به مرور زمان و تحت تاثیر صنعتی شدن زندگی بشر، شاخه‌های معرفتی به طور فزاینده‌ای رشد پیدا کرده و امکان تجمیع آنها در یک نفر از بین رفت. تخصص‌محور شدن علوم تنها راهی بود که در این میان پیشنهاد شد و جوانان و افراد جویای علم را به سمت مراکز آموزشی کشاند؛ در این فضا در اثر بالارفتن سطح علمی عمومی جامعه، از بین رفتن اُبَهِت علم در انظار و همچنین ضرورت سنجش علوم مختلف با یکدیگر، هر یک از جویندگان علم، حوزه‌ای را انتخاب کرده و راه آگاه‌سازی دیگران را نسبت به حوزه مورد تخصص خود در پیش می‌گرفتند.

به بیان ساده‌تر، صاحبان علم در هر دوره‌ای از تاریخ بشریت، به دنبال آن بودند تا دستاوردهای خود را با مردم جامعه به اشتراک گذاشته و مسائل را به گوش آنان برسانند. این دغدغه و فرآیند عملی آن را بعدها در دوران مدرن با عبارت «عمومی‌سازی علم»<sup>۱</sup> نامگذاری نمودند. برای این عبارت تعاریف متعددی ذکر شده که متداول‌ترین آنها این است: ترجمه پژوهش‌های علمی برای جمعیت غیرمتخصص؛ به بیان دیگر عمومی‌سازی علم یعنی همه‌فهم کردن آن برای مردم با حفظ سطح علمی لازم؛ جی.اس.کید<sup>۲</sup> در مقاله‌ای تحت عنوان «عمومی‌سازی علم» لوازم فرآیند عمومی‌سازی علم را اینگونه برمی‌شمرد [۴]:

الف) ارتباط مداوم بین دانشمندان و متخصصان علم با عامه مردم که باید دو طرفه باشد.

ب) بررسی اطلاعات علمی قبل از در اختیار قرار دادن آنها به عموم مردم.

ج) گزینش‌گری اخبار علمی برای ترویج آنها بر اساس نیاز عرف جامعه.

د) ضرورت تطابق زبان علمی با زبان عامیانه در فرآیند عمومی‌سازی علم.

گرچه معنایی که بعد از خواندن عبارت عمومی‌سازی علم در ذهن تداعی می‌شود، با تعریف علمی آن تفاوت زیادی ندارد، ولی این تعریف به هیچ‌وجه گویای منازعات همراه آن نیست. در مورد فرآیند عمومی‌سازی عمل سوالات مبنایی زیادی وجود دارد؛ مثل اینکه آیا این فرآیند می‌تواند شکاف بین دانشمندان و جامعه را پر کند؟ آیا هدف از این فرآیند صرفاً انتقال یک‌طرفه دانش و جلب حمایت (خصوصاً حمایت اقتصادی) مردم جامعه از قشر فرهیخته است یا می‌توان از گفتگوی متقابل در ضمن این فرآیند سخن گفت؟ [۱۱]

فارغ از اختلاف‌نظرهای موجود در این باب، باید اعتراف کرد که فرآیند عمومی‌سازی علم نقش کلیدی در ارتقاء دانش عمومی و آگاهی اقشار مختلف یک جامعه از علوم و فناوری‌های مختلف دارد. به‌طور قطع افزایش اطلاعات عمومی در میان افراد مختلف هر کشور منجر به ارتقاء دانش و آگاهی کلی آن جامعه و حرکت روبه‌جلو می‌شود. از در دسترس‌ترین و تأثیرگذارترین ابزارهای ممکن برای عمومی‌سازی علوم و بالابردن سطح علمی هر جامعه‌ای، می‌توان به رسانه‌های موجود در آن اشاره کرد [۵]. رسانه وسیله‌ای است که نقش حامل

<sup>۱</sup>scientific popularization

<sup>۲</sup>J. S. KIDD



اطلاعات و پیام‌های از پیش طراحی شده را ایفا کرده و به عنوان واسطه‌ای بین انتقال دهنده و گیرنده پیام، در طول زمان دچار تحول و پیشرفت شده است [۱]. از سنگ‌نوشته‌ها، طومارهای گلی، چرمی، و پوستین گذر کرده تا به کتاب‌های چاپی، روزنامه‌ها، رادیو، و تلویزیون رسیده و در نهایت در اینترنت و شبکه‌های اجتماعی استقرار پیدا کرده است [۹].

با مروری گذرا بر تاریخ چند هزار ساله تمدن بشری، درمی‌یابیم که نشر اطلاعات علمی در رسانه‌ها، همواره یکی از عوامل عمده تکوین، تکامل و ماندگاری اندیشه‌ها و تمدن‌ها بوده است. برای مثال فلاسفه و متفکرین یونان باستان، با نگارش کتاب‌ها و رساله‌های مختلف تمدن خود را پی‌ریزی کردند؛ ائمه معصومین و علمای مسلمان نیز با خطابه و منبر، اندیشه‌های خود را ماندگار کرده و اقوام دیگر از طریق سینما و تلویزیون، مبانی تمدنی خود را به جهان صادر کردند [۷]. به دلیل همین اهمیت، از نیمه اول قرن بیستم موضوعی تحت عنوان «ارتباطات علمی»<sup>۳</sup> به منزله یکی از سازوکارهای اصلی مؤثر بر نهاد علم، در کانون مطالعات جامعه‌شناختی رسانه قرار گرفته و درباره اهمیت آن در تولید دانش بحث و گفتگو به میان آمده است. ارتباط علمی به فرایندهای رسمی و غیررسمی اطلاق می‌شود که از طریق آن فعالیت‌های تحقیقاتی پژوهشگران خلق، ارزیابی، سازماندهی، توزیع، دست‌یافتنی، و آرشیو می‌شود [۸].

## ۲ تاریخچه عمومی سازی علم

به طور کلی می‌توان در تاریخ عمومی‌سازی علم توسط صاحبان آن، سه دوره را از یکدیگر تفکیک کرد [۷]:

۱. **دوران سنتی**: در این دوران اکثر ارتباطات علمی بین اندیشمندان و مردم از نوع ارتباطات خصوصی و رودررو بوده و رسانه‌هایی همچون کتاب و منبر (خطابه) به عنوان حلقه وصل این دو طایفه معرفی می‌شدند.

۲. **دوران مدرن**: در این دوران با ظهور رسانه‌های آنالوگ، رادیو و تلویزیون به عنوان ابزار عمومی‌سازی علم معرفی شده و مردم از این طرق، با آخرین دستاوردهای دانشمندان آشنا می‌شدند.

۳. **دوران پست‌مدرن**: با ظهور رسانه‌های دیجیتال و آنلاین، فرآیند عمومی‌سازی علم سرعت و وسعت بیشتری پیدا کرده و در کسری از ثانیه، نظریات علمی در سطحی جهانی منتشر می‌شوند. این رویداد تغییرات بنیادین و آشکاری را در روش‌های جستجوی اطلاعات، برقراری ارتباط اندیشمندان با مردم، و گزارش‌های علمی ایجاد کرده است.

در مورد تفاوت‌های روشی عمومی‌سازی علم در این سه دوره بحث‌های مختلفی را می‌توان مطرح کرد؛ مثلاً اینکه در دوره سنتی محتوای کلام خطیب بسیار مهم‌تر از رنگ و لعاب ظاهری آن بوده و در دوران مدرن و پست‌مدرن، فرم انتقال اندیشه، به مراتب با اهمیت‌تر از محتوای آن، دانسته می‌شود. یکی از تفاوت‌های مهم بین این سه دوره، مقوله گمنامی یا هویت‌مندی شخص عالم و اندیشمند است؛ در دوران سنتی علما

<sup>3</sup>Scientific communication



و اندیشمندان، سعادت و برتری خود را نسبت به دیگران در گمنامی بیشتر دیده و علم خود را به دادگاه سنجشی می‌سپاردند که قاضی آن نور عقل و دیگر شهودات الهی است؛ از این رو، همواره خود را از دخالت و اظهار نظر نسنجیده در تمام مسائل علمی برحذر می‌داشتند و حتی در زمینه مورد تخصص خود نیز واژه نمی‌دانم را بر لب می‌راندند؛ اما امروزه و در قالب «ژورنال‌لیسم اندیشه سایبری» موجود، هم دادگاه علم تغییر کرده و هم قاضیان آن متعدد شده‌اند. اهمیت یک مساله علمی امروزه از روی تعداد اعضای کانال و بازدید مخاطبان آن کشف می‌شود؛ از این رو داعیه‌داران دانش نیز به ناچار جلوت را انتخاب کرده و به دنبال آن هستند تا بیش از پیش، هویت‌مندی خود را در جهان اجتماعی به اثبات برسانند؛ از این رو آنها برای دفاع از هویت خود و رقابت با هویت‌مندان علمی دیگر، به ناچار نه تنها در مسائل مورد تخصص خود، بلکه در تمام مسائل اندیشه‌ای موجود در جامعه اظهار نظر می‌نمایند.

سؤال‌ی که در این بین خودنمایی می‌کند این است که چرا این تفاوت بین دو دوره از فرآیند عمومی‌سازی علم به وجود آمده است؟ به بیان دیگر چه شده که صاحبان علم روزی گمنامی را افتخار خود و روزی دیگر هویت‌مندی را با چنگ و دندان طلب می‌کنند؟ به منظور یافتن پاسخ این سوالات باید به تفاوت‌های این سه دوره توجه کنیم.

## ۳ تفاوت دوره‌های مختلف

### ۱.۳ تغییر ماهیت علم

یکی از مهمترین اتفاقاتی که در جهان اندیشه بشری رخ داده، تغییر ماهیت علم از دوران سنتی تاکنون است. در ادبیات سنتی و دینی، علم به مثابه کشف حقیقتی است که در عالم نفس‌الامر حضور داشته و از طریق فیضان الهی، به عقل و نفس بشری وارد می‌شود. در این بین شخص عالم صرفاً وظیفه اجتماعی‌سازی یعنی نزول آن حقیقت به عالم ماده را بر عهده دارد. بر اساس این نگاه به ماهیت علم، شخص عالم صرفاً کاشف حقیقت بوده و نمی‌توان قوام علم را به آن شخص دانست چرا که ممکن بود هر شخص دیگری در زمان‌ها و مکان‌های دیگر یا به‌طور همزمان نیز به آن حقیقت دست یابد. در این پارادایم، ارزش عالم در پرتو عیار آن حقیقتی است که برای او نمایان شده نه نام و نشان خودش تا بخواهد با خودنمایی و تاکید بر هویت‌مندی، آن حقیقت را تحت عنوان یک نظریه اختصاصی، به نام خود سند بزند. در تاریخ اسلام نمونه‌های زیادی را می‌توان یافت که همچون شیخ عباس قُمی تن به چاپ کتاب خود با نام دیگری داده و پای منبر کسی بنشینند که از روی کتاب خود او مساله می‌گوید؛ یا همچون ابن‌سینا که با کوهی از علم، واژه نمی‌دانم را مدام زیر لب تسبیح می‌کند. دادگاه سنجش علم این افراد، خلوت و قاضی آن نور عقل و دیگر شهودات الهی است. از این‌رو هیچگاه جز در موارد ضروری داعیه دیده‌شدن نداشته و از دخالت در مسائل ناآشنا پرهیز می‌کنند. برخلاف دیدگاه سنتی به علم، در دوران مدرن و پست‌مدرن، جایگاه علم ابتدا از جهان نفس‌الامر به جهان محسوس سقوط کرده و بعد قوام آن به ذهن آدمی و فرهنگی که ساختارهای آن ذهن را می‌سازد، تعلق گرفت تا انسان به عنوان سازنده حقیقت معرفی شود نه کاشف آن. برای فهم بهتر این مساله، لازم است تا سه دوره از تحولات معنای علم را در دوران معاصر پی گرفت: [۳]

## ۱. رویکرد پوزیتویستی کلاسیک

مراد از علم در تلقی پوزیتویستی، دانش آزمون‌پذیر تجربی است که از قرن نوزدهم شکل گرفته و در کشور ما نیز وجود دارد. در تعریف پوزیتویستی از علم، درباره نقش آزمون اختلافاتی وجود دارد: اثبات، تأیید یا ابطال؛ اما به هر حال، این آزمون تجربی است که درست و غلط بودن را نشان داده و مرز علم با معرفت‌های غیر علمی را مشخص می‌کند. نتیجه این تعریف این است که همه علوم باید روش‌مند، و به نحو تجربی آزمون‌پذیر باشند. این معنای از علم، ابتدا در علوم طبیعی جریان پیدا کرده و بعد از آن توسط آگوست کنت وارد علوم اجتماعی و انسانی شد. طبق این تلقی، ما تنها در صورتی علم انسانی خواهیم داشت که بتوانیم انسان را به صورت تجربی و آزمون‌پذیر مورد شناسایی قرار دهیم؛ چراکه در این نگاه، روش عقلی و دیگر روش‌های معرفتی، ارزش علمی ندارند. البته روش عقلی نظم و نظامی دارد؛ اما تنها در ذهن است و به جهان خارج ارتباطی ندارد. طبق این نگاه، علوم انسانی آگاهی‌های روشمند، تجربی و آزمون‌پذیر درباره انسان است و با علوم طبیعی نظیر فیزیک و شیمی تفاوت جوهری ندارد و تنها پیچیده‌تر از آنها است؛ چراکه انسان، یک محصول پیچیده در عالم طبیعت است.

## ۲. رویکرد تفهیمی یا تفسیری

از اواخر قرن نوزدهم، جریان دیگری در غرب به وجود آمد که بر تفاوت حوزه حیات انسانی با موجودات طبیعی تأکید کرد. بر اساس این رویکرد، ما نمی‌توانیم انسان و جامعه را مانند موجودات طبیعی مشاهده و تجربه کنیم، بلکه امور انسانی را باید بر اساس قصد و هدف افراد فهم کرد. در عالم انسانی، ممکن است یک کار واحد، در زمینه‌های مختلف و بر اساس قصد افراد مختلف، معانی و تحلیل‌های متفاوتی داشته باشد. بنابراین حوزه حیات انسان، فهمیدنی است و با مشاهده صرف درک نمی‌شود. این بحث‌ها را ابتدا کسانی مثل دیلتای و ریکرت مطرح کردند و در آثار ماکس وبر ادامه پیدا کرد. طبق این رویکرد، آگاهی‌های انسانی بی‌ارزش نیستند؛ آنها شیوه زندگی را به ما می‌آموزند؛ مانند اینکه چگونه حرف بزنیم، چگونه فکر کنیم و چه مقرراتی داشته باشیم. فراگرفتن این معارف به معنای مشارکت در یک عقلانیت توافقی تاریخی است که بین انسان‌ها شکل گرفته است. به بیان دیگر از نظر اینان انسانیت یک سری آگاهی‌های غیر علمی و درعین حال مفیدی است که انسان‌ها آنها را برای زندگی خود ساخته‌اند و با این آگاهی‌ها، انتقال تجارب انسانی و تعاملات انسانی تداوم پیدا می‌کند.

## ۳. رویکرد مابعدتجربی و پست‌مدرن

به تدریج تلقی تجربه‌گرایانه از علم با مسائلی مواجه شد که موجب تغییر در تعریف علم شد. صاحبان علم در برابر این پرسش قرار گرفتند که آیا مفاهیم و قضایای پایه‌ای که به کار می‌بریم، از طریق حس و تجربه به دست آمده‌اند و یا از طریق آزمون تجربی قابل اثبات یا ابطال هستند؟ مفاهیم اولیه‌ای مانند ماده و انرژی؛ یا قواعد و احکامی چون اصل علیت و حتی خود همین گزاره که علم محدود به شناخت حسی و تجربی است. از

آنجا که در تلقی پوزیتیویستی، علم به معرفت آزمون‌پذیر محدود است، این مفاهیم و قضایای بنیادی در خارج از قلمرو معرفت علمی قرار می‌گیرند و به انسانیات، باورهای اجتماعی و باورهای جامعه علمی ارجاع داده می‌شوند. در نتیجه علم هویت و تعریف خود را از حوزه فرهنگ و قلمرو معرفت‌های غیر علمی می‌گیرد. در این صورت، چون علم نمی‌تواند از مفاهیم، مبانی و مبادی خود (که گاه با عنوان «پارادایم‌های علمی» از آنها یاد می‌شود) دفاع علمی کند، هویت مستقل خود را از دست می‌دهد؛ با این اتفاق، دیگر علم حوزه مستقلی از حوزه فرهنگ نخواهد بود و اگر فرهنگ بشری و خصوصاً فرهنگ جامعه علمی عوض شود، پارادایم علم تغییر می‌کند. پست‌مدرن‌ها با استفاده از همین مطلب، علم را نیز به معرفت‌هایی که بر اساس نگاه پوزیتیویستی غیر علمی بودند، ملحق کردند. علم در این تلقی، هم هویت مستقل و تمایز خود از معرفت‌های غیر علمی و هم خصلت روشنگری و حکایت‌گری از حقیقت را از دست می‌دهد. در این تلقی علوم طبیعی، کاشف از چیزی به اسم طبیعت نیست، بلکه بخشی از تفسیر تاریخی انسان نسبت به حیات و زندگی او است و کسی که علوم طبیعی را می‌آموزد، همانند کسی است که ادبیات و هنر را فرامی‌گیرد. او یاد می‌گیرد تا با نوع تفسیری که می‌کند، حیات و زندگی خود را بسازد و یا در حیات و زندگی معاصر خود شریک شود. کسی که پزشکی می‌آموزد، در طول مدت آموزش خود، در یک توافق جمعی مشارکت می‌کند و یاد می‌گیرد که چگونه آنچه را که به حسب فرهنگ خود بدن می‌نامند، تغییر دهد و چگونه مسائل خود را حل کند.

بعد از بیان این سه رویکرد، باید اعتراف کرد که رویکرد غالب در فرآیند بازتولید محتواهای علمی در بسترهای سایبری مثل شبکه‌های اجتماعی، بخاطر ماهیت برساختی بودن این تکنولوژی، همین رویکرد پست‌مدرن و فراتجربی به علم است. بر این اساس امروزه قوام علم و نظریه علمی به شخصی است که آن را برساخت می‌کند و برای فهم آن باید به ذهنیات و فرهنگی که آن شخص در آن تنفس می‌کند، رجوع کرد. بر این اساس طبیعی است که شخص عالم از هویت‌مندی خود دفاع کرده و برای اقناع‌سازی و تاثیر روی مخاطبین در فرآیند عمومی‌سازی علم، اسم و رسم خود را یادآوری نماید؛ همچنین این شخص باید برای حفظ نظریه و هویت خود، همواره در مقابل دیدگان مخاطبین حضور داشته و از این باب، برای تمام مسائل بشری، راه حلی ارائه بدهد.

### ۲.۳ تغییر ماهیت رسانه

دومین مساله‌ای که در خلال قرون گذشته ناظر به مقوله عمومی‌سازی علم مورد تغییر و تحول قرار گرفته، ماهیت رسانه است. رسانه در واقع وسیله انتقال پیام و اطلاعات به دیگران است که در قالب‌های مختلف ظهور و بروز می‌نماید؛ روزی مردم از طریق کبوترهای نامه‌بر از احوال یکدیگر آگاه می‌شدند و روز دیگر، با فشردن یک دکمه؛ به هر حال به طور کلی می‌توان سیر تطور رسانه‌ها را در طول حیات بشری به چهار دوره تقسیم کرد [۱۰]:

#### دوره اول: رسانه‌های شنیداری

اولین رسانه‌های عمومی بشری، یا جارچینانی بودند که با صدای بلند اخبار را به سمع مردم کوچه و بازار می‌رساندند و یا وُعاطی بودند که بر بلندی منبر قرار گرفته و راه و رسم زندگی را به مردم می‌آموختند.

#### دوره دوم: رسانه‌های مکتوب

اگرچه که نوشتار کم و بیش از ابتدای خلقت در زندگی بشر وجود داشته اما با اختراع ماشین چاپ به یکی از رسانه‌های مهم و پرطرفدار جوامع مختلف تبدیل شد. روزنامه‌ها و مطبوعات رسانه‌های پر قدرتی بودند که توانایی نشر اخبار، تعلیم دروس و حتی بازاریابی برای کاسبان را با خود یدک می‌کشیدند.

### دوره سوم: رسانه‌های دیداری و شنیداری

اختراع رادیو، تلویزیون و سینما در قرن بیستم میلادی باعث آن شد که ذهن مخاطبین بیش از پیش درگیر رسانه‌ها شده و تولیدکنندگان محتوا بتوانند پیام خود را در زمان واحد به هزاران مخاطب منتقل کنند. به خاطر جذابیت‌های بصری و شنیداری رسانه‌های جدید، کم کم مولفه سرگرمی بر کارکردهای دیگر این رسانه‌ها مستولی شده و محتوای این رسانه‌ها از مسائل مهم و کلان جامعه، به سخنان عامه‌پسند مبدل گشت.

### دوره چهارم: رسانه‌های مجازی

در دوران معاصر، تمام مرزهای زمانی و مکانی رسانه‌ها شکسته شده و مخاطبین به کاربرانی با قابلیت ارتباط دوسویه با این ابزار تبدیل شده‌اند. امروزه رسانه عضوی از خانواده شده که بدون حضور آن، کارهای زیادی مختل می‌گردد؛ همچنین در این دهکده جهانی که رسانه‌های جدید برایمان درست کرده‌اند، ارتباطات انسان‌ها وسعت بیشتری پیدا کرده و زوایای جدیدی از خود نمایان ساخته است.

بعد از بیان تطورات رسانه باید گفت که متاثر از همین تحولات و به دلیل تغییر ویژگی‌ها و عناصر رسانه‌ای از دوران سنتی تاکنون، می‌توان از تغییر ماهیت رسانه‌ها در ارتباط با تولیدکننده پیام سخن گفت. در دوران سنتی، خطابه و رسانه منبر به خودی خود توانایی خاصی نداشته و قوام آن به توانایی خطیب در جذب مخاطب بود؛ به بیان دیگر این منبر است که باید به خود ببالد تا بزرگانی امثال شیخ عباس قمی بر روی آن بنشینند نه آنکه علما برای قرارگرفتن روی آن شوقی داشته باشند. زمانی که قوام رسانه به فرد باشد، دیگر مقوله برندسازی از کارکردهای آن رسانه به حساب نیامده و فرد عالم نیز به جای آن که برای هویت‌مندی و شهرت خطابه خود دست و پا بزند، به سراغ تهذیب اخلاقی خود می‌رود تا تاثیرگذاری کلامش را بالا ببرد؛ مضاف بر اینکه نفس تهذیب اخلاقی و سلوک معنوی، عالم را به خضوع و سربیزی بیش از پیش رهنمون می‌سازد.

برخلاف آنچه که گفته شد، در دوران معاصر هم به دلیل اقتضائات زمانی و هم به دلیل ویژگی‌های منحصربه‌فرد رسانه‌های مجازی مثل قدرت بالای فراگیری، توده‌ای بودن مخاطبین و توان برندسازی به وسیله برساخت حقایق و تبلیغ آنها، این اندیشمندان و صاحبان علم هستند که قوام خود را به رسانه‌ها دانسته و به سراغ فراگیری تمام تکنیک‌های کسب شهرت می‌روند. آنان به خوبی می‌دانند که در دوران کنونی به دلیل غلبه «فرهنگ شهرت‌محور» و به دلیل انحصار عنصر برندسازی در فعالیت رسانه‌های سایبری، باید تمام تلاش خود را در جهت دیده‌شدن بیشتر توسط مخاطبین این رسانه‌ها به کار گرفته و خود را بر زبان‌ها بیندازند تا بدین وسیله بتوانند تاثیرگذاری علمی داشته باشند. در این فضا توصیه به گمنامی امری مذموم بوده و تمام نظریات علمی مطرح‌شده در رسانه‌ها، با نام و منصب نظریه‌پرداز و نویسنده آنها شناسایی می‌گردد؛ طبیعی است که هرچقدر این نام برای مردم آشنا تر و در نظر آنها بزرگ‌تر جلوه کند، تاثیرگذاری و تلاش برای ترویج آن نظریه مضاعف خواهد شد.

## ۳.۳ تغییر هدف از عمومی سازی

یکی دیگر از اموری که در فرآیند عمومی سازی علم از دوران سنتی تاکنون مورد تغییر و تحول قرار گرفته، هدف و غایت آن است. بدین منظور لازم است تا با هدف از عمومی سازی علم در دوران‌های مختلف زندگی بشری آشنا شویم:

### ۱. هدایت بشر با نور علم

در دوران سنتی از آنجایی که علم به عنوان نور معرفی می‌شد، عالمان نیز از آن به عنوان ابزار هدایت بشر و نشان دادن راه صحیح زندگی بهره می‌جستند. از طرف دیگر علم صرفاً به دانستنی‌های ذهنی محدود نشده و در تمام بخش‌های زندگی شخص عالم خود را نمایان می‌ساخت. بر این اساس می‌توان گفت که در این دوران، اولاً هدف از عمومی سازی علم، هدایت مخاطبین بوده؛ ثانیاً این هدایت‌گری از سر دلسوزی و احساس تکلیف بوده نه به مثابه فروشنده‌گی و معامله؛ ثالثاً در فرآیند هدایت‌گری صرفاً انتقال دانستنی‌ها صورت نگرفته و گاهی مردم صرفاً با دیدن چهره عالم و منش او، راه خود را پیدا می‌کردند؛ رابعاً همین که در یک شهر یا کشور، عالم یا عالمانی باشند که مردم را به سرمنزل هدایت نزدیک کنند، مطلوب حکومت نیز تامین خواهد شد و خامساً در این مدل از عمومی سازی، از آنجایی که هدف هدایت‌گری است، شخص عالم داعیه دیده‌شدن خود را ندارد و اگر این هدف به دست دیگری حاصل شود، او خود را کنار می‌کشد و سکوت خواهد کرد [۲].

به منظور فهم بهتر این مدل از عمومی سازی، کافی است بدانیم در تعالیم دینی ما معلم به عنوان پدر روحانی معرفی شده و رعایت تمام حقوق والدین را در حق او ضروری شمرده می‌شود. نام معلم چنان با عظمت است که در جای‌جای متون اسلامی از او تجلیل به عمل آمده تا به آن حد که خداوند علیم خود را معلم خوانده و رسول الله (ص) خود را اینگونه معرفی می‌کنند: انما بعثت معلماً؛ در این تصویر، معلم در واقع جانشین خداوند و رسولان او در امر تربیت انسان‌هاست تا آنها را از مقام حیوانیت بالا برده و به مقام انسانیت برساند [۶]. معلم، ایمان را بر لوح جان و ضمیرهای پاک حک می‌کند و ندای فطرت را به گوش همه می‌رساند؛ همچنین سیاهی جهل را از دل‌ها می‌زداید و زلال دانایی را در روان بشر جاری می‌سازد. دغدغه معلم همیشه این است که حیات بشر، بر مدار ارزش‌ها و کرامت انسانی بچرخد و شناخت خدا و مکتب و دین، همت اساسی آدمی باشد و هیچ بیگانه‌ای را مجال تجاوز به فرهنگ ارزشی دین و میهن فراهم نیاید.

### ۲. انتقال دانش به دیگران

به دلیل محدود شدن دایره علم به حوزه تجربه و عقل بشری و همچنین از بین رفتن عنصر روشنگری علم در دوران مدرن، عمومی سازی علم به مثابه انتقال دانش از ذهنی به ذهن دیگر تلقی شده که اغراض دیگری غیر از هدایت را دنبال می‌کند. در دوران مدرن، یکی از معیارهای توسعه‌یافتگی جوامع انسانی، زوال بی‌سواد و هم‌سطح‌شدن علمی تمام افراد جامعه معرفی می‌شد؛ از این رو حکومت‌ها تلاش می‌کردند تا با به‌کارگیری معلمان و فراهم کردن شرایط تحصیل رایگان و اجباری برای همه،

دانش عقلی و تجربی را به سراسر جامعه تزریق کرده و بعد از آن به توسعه‌یافتگی خود افتخار کنند. در این مدل از عمومی‌سازی، هدف صرفاً انتشار یک سری نظریات علمی در سطح گسترده است که گاهی حتی همین انتشار، باعث بروز مشکلات زیادی همچون قیام طبقات فرودست می‌شد. در این مدل حکومت‌ها بیشتر از اصحاب علم داعیه دیده‌شدن داشته و برای نشر بیشتر مکاتب علمی تمام تلاش خود را به کار می‌گیرند.

### ۳. فروشنده دانستنی‌ها

با رشد روند نسبیت‌گرایی و بین‌الذهانی شدن علم در دوران پست‌مدرن، دانش از اختیار اصحاب حقیقی آن درآمده و به برساختی اجتماعی تبدیل شد که هرکسی می‌تواند با کمترین درصد از آگاهی، به آن ورود کرده و اظهارنظر نماید. در این فضا که دکان‌های زیادی به عرضه نظریات علمی پرداختند، طبیعی است که بر اساس قوانین بازار اقتصاد، تقاضا کمتر شده و هر یک از فروشندگان باید تمام تلاش خود را برای دیده‌شدن در نظر مخاطبین و جذب آنها به کار بندند. از طرف دیگر با رشد و تکامل رسانه‌ها، شبکه‌های اجتماعی سایبری به عنوان ویتربینی خوش‌رنگ و لعاب برای تبلیغ محصولات تجاری شناخته می‌شوند که توانایی زیادی در برندسازی و انحصاربخشی شهرت در اختیار گروهی خاص دارند؛ بر این اساس اصحاب علم در دوران معاصر صرفاً با برندشدن و شهرت در این رسانه‌هاست که می‌توانند نظریات خود را به گوش دیگران رسانده و خود را به عنوان اندیشمند معرفی کنند؛ از این رو تمام تلاش خود را به کار می‌بندند و تمام تکنیک‌های لازم برای برندشدن در این رسانه‌ها را فرامی‌گیرند تا همواره بتوانند در اذهان مخاطبین و جلوی چشم آنان حضور داشته باشند. با توجه به تمام این مطالب می‌توان اذعان کرد که هدف از عمومی‌سازی علم در دوران معاصر، صرفاً کسب هویت و شهرت است نه هدایت یا صرفاً انتقال دانش؛ در این فضا اصحاب علم نیز به مثابه فروشندگانی هستند که با داد و فریاد و جنجال، سعی در جمع‌کردن مشتریان در فروشگاه خود را دارند.

### ۴ نتیجه‌گیری

بعد از بیان مطالب پیشین، حال می‌توان به سؤال اصلی این پژوهش یعنی علت تفاوت ادوار عمومی‌سازی علم در گمنامی یا هویت‌مندی عالمان، پاسخ داد. به دلیل وقوع تغییر در ماهیت علم، رسانه و هدف از عمومی‌سازی، دیگر امروزه سخن از گمنامی و تواضع اصحاب علم بی‌معنا بوده و پارادوکسیکال است چرا که در دوارن معاصر با تلقی جدیدی که از علم وجود دارد و با تحولاتی که رسانه‌های جدید به وجود آوردند، هرکسی بیشتر از بقیه در عالم مجازی مقابل دیدگان مخاطبین حضور داشته باشد، بهره بیشتری از علم و دانش برده و افراد گمنام در این فضا، فرومایه و عقب‌مانده محسوب خواهند شد. از این رو طبیعی است که دادگاه علم تغییر کرده و ارزش یک مسئله علمی و جایگاه عالم، از روی تعداد اعضای کانال و بازدید مخاطبان آن کشف شود.



## مراجع

- [۱] احمدزاده کرمانی، روح‌الله. بازانديشي در فرهنگ و رسانه. چاپار، ۱۳۹۰.
- [۲] امام، سيدمحمدرضا، دادگر، سيد امين‌الله و منوچهری، سيدعلي. بررسی کارکرد و نقش تربیتی و هدایت‌گری معلم از منظر قرآن. فصلنامه مطالعات آموزشی و آموزشگاهی، شماره ۳۶، ۱۳۹۹.
- [۳] پارسانیا، حمید. تطورات معنای علم. خبرگزاری مهر، ۸ بهمن، ۱۳۹۵.
- [۴] حیدری، آزاده. راهکارهای ارتقاء وضعیت ترویج علم در ایران؛ با بررسی دیدگاه صاحب‌نظران و متولیان. در مجله تخصصی دانش‌شناسی، دوره ۴، شماره ۱۵ (۱۳۹۰).
- [۵] رپسم، هانیچ و دیگران. درآمدی بر مطالعات ژورنالیسم، ترجمه مرتضی رستمی. روزنامه همشهری، ۱۳۸۹.
- [۶] علاء‌الدین، سيدمحمدرضا. جایگاه، نقش و رسالت معلم و مربی از دیدگاه قرآن و روایات. دوفصلنامه کوثر، شماره ۳۲، ۱۳۸۸.
- [۷] فرهادی، ربابه. فناوری اطلاعات و ارتباطات: اصول و کاربرد. کتابدار، ۱۳۹۰.
- [۸] قانع، محمدرضا. ارتباط علمی: از مجله چاپی تا مجله دسترسی آزاد. در کلیات کتاب ماه، شماره ۴۴ (۱۳۸۸).
- [۹] کرامتی، محمدهادی. چگونه از رسانه‌های اجتماعی به منظور برقراری ارتباطات واقعی استفاده کنیم؟. ماهنامه وب، شماره ۱۶۲، ۱۳۸۸.
- [۱۰] کیتلر، فدریک. تاریخچه رسانه‌های ارتباطی، ترجمه سارا پاک‌ضمیر. ۱۳۸۷.
- [۱۱] کیهانیان، کیانوش. پارادایم تعمیم علم. نشریه قاف، ۱۳۹۵.



# پروتکل توافق کلید امن احراز اصالت شده برای کاربرد در گواهی (تصدیق) دیجیتال

امیرحسین رحیمی<sup>۱</sup>

<sup>۱</sup> کارشناس ارشد رمز و مربی دانشگاه آزاد اسلامی، واحد قم، گروه ریاضی، قم  
amir.rahimi361@gmail.com

## چکیده

پروتکل توافق کلید احراز اصالت شده یک مؤلفه اساسی در برقراری کلید جلسه به منظور ایجاد کانال امن برای ارتباطات شبکه‌ای در محیط‌های باز و توزیع شده می‌باشد. تاکنون پروتکل‌های زیادی بر اساس تعیین هویت اشخاص برای فراهم کردن احراز اصالت متقابل قوی و برقراری کلید جلسه عمومی در محیط‌های باز و دوگانه برای ارتباطات امن پیشنهاد شده‌اند. اما اکثر پروتکل‌های موجود توافق کلید احراز اصالت شده فقط امنیت پیشرو جزئی و نسبی را فراهم می‌کنند. بنابراین چنین پروتکل‌هایی برای کاربردهای تکنولوژی روبه رشد جهان واقعی که امنیت پیشرو کامل را نیاز دارند مناسب نیستند. در این مقاله یک پروتکل توافق کلید احراز اصالت شده براساس شناسه‌ی هویت امن دو بخشی ارائه می‌شود که اکثر مشخصه‌های امن مطلوب شامل: امنیت کلید معلوم، امنیت پیشرو کامل، امنیت پیشرو، PKG قابلیت ارتجاع در برابر جعل هویت کلید کشف رمز شده، قابلیت ارتجاع در برابر تسهیم کلید نامعلوم، کنترل نکردن کلید، شناسایی نکردن اطلاعات کلید جلسه ثابت - موقتی را با بازدهی بالا به انجام می‌رساند و همچنین الگوریتم پیشنهادی زمان اجرای کوتاه‌تر، هزینه‌ی محاسباتی و ارتباطی کمتر و روش ذخیره‌سازی مؤثر نسبت به سایر الگوریتم‌های پیشنهادی مشابه دارد و گذشته از این اخلال‌گر به آسانی نمی‌تواند در روند تبادل داده، کلید جلسه توافقی را کشف رمز کند.

**کلمات کلیدی:** توافق کلید، احراز اصالت کاربر، مؤد کلید خصوصی (PKG)، گواهی دیجیتال، تابع درهم‌ساز، لگاریتم گسسته، کلید جلسه محرمانه.

## ۱ مقدمه

اصولاً پروتکل توافق کلید برای فراهم کردن ارتباطات امن در محیط‌های باز و توزیع شده بکار می‌رود و برقراری کلید شیوه‌ای است که بوسیله آن دو (یا بیشتر) هویت‌ها می‌توانند یک کلید محرمانه تسهیم شده (کلید جلسه) را بعد از فعل و انفعالات پیام بین خودشان برقرار کنند؛ از این رو دو شیوه مختلف برای برقراری

جدول ۱: نمادگذاری‌ها

نماد	تعریف	نماد	تعریف
$ID$	شناسه‌ی هویت کاربر	$\oplus$	عملگر XOR
$r_{ID}$	عدد تصادفی	$E$	نگاشت خطی
$q$ و $p$	دو عدد اول بزرگ به طوری که $p = 2q + 1$	$H(\cdot)$	تابع درهم‌ساز امن
$G$	گروه جمعی دوری	$Z_p^*$	گروه ضربی $p$
$G_1, G_2$	گروه ضربی دوری	$\parallel$	عملیات الحاق
$F_p$	میدان منتهای عدد اول $p$	$X \pmod{p}$	باقیمانده $X$ تقسیم بر $p$
$AK$	کلید احراز اصالت شده	$SK$	کلید جلسه
$P_{pub}$	کلید عمومی	$ECC$	رمزنگاری خم بیضوی
$DLP$	مسئله‌ی لگاریتم گسسته	$CDH$	فرض دفی-هلمن

کلید بین دو هویت وجود دارد؛ در یکی از روش‌ها هویتی یک کلید جلسه ایجاد کرده و به طور امن آن را به هویت دیگری برای هم‌پوشانی انتقال می‌دهد؛ ضمناً به منظور تأمین احراز اصالت پروتکل توافق کلید، تصدیق کلید عمومی اغلب در محیط کلید عمومی سنتی با تصدیق گواهی‌نامه بکاربرده می‌شود. [۴] Adi Shamir در ۱۹۸۴ رمزنگاری براساس شناسه هویت را معرفی کرد. ایده او به تمامی بخش‌ها اجازه می‌داد شناسه‌های هویت‌شان را به عنوان کلید عمومی بکار گرفته و به کمک مؤلّد کلید خصوصی (PKG)، کاربرها کلیدهای خصوصی‌شان را تولید کرده و براساس پروتکل‌های رمزنگاری اجرا شوند. احراز اصالت بدون تصدیق کلید عمومی مزیت اصلی رمزنگاری براساس شناسه هویت است. پروتکل توافق کلید احراز اصالت شده دو بخشی (AK) علاوه بر این که به بخش‌ها اجازه می‌دهد کلید جلسه‌ای که فقط به آن‌ها شناخته شده را محاسبه کنند بلکه اعتبار قسمت‌ها را نیز تضمین کنند. همچنین کلید جلسه محرمانه می‌تواند یکپارچگی و استقلال داده را در طول جلسات متوالی فراهم کند. پروتکل توافق کلیدی که احراز اصالت متقابل کلید ضمنی (از باب به آلیس) را فراهم می‌کند؛ پروتکل توافق کلید احراز اصالت شده AK نامیده می‌شود در این پروتکل توافق کلید، زمانی تصدیق کلید (از باب به آلیس) فراهم می‌شود که آلیس مطمئن شده باشد فقط باب کلید محرمانه را در تصرف دارد. پروتکلی که احراز اصالت کلید متقابل و همچنین تأییدیه کلید متقابل را فراهم می‌کند تحت عنوان یک توافق کلید احراز اصالت شده با پروتکل تصدیق کلید (یا یک پروتکل AKC) نامیده می‌شود. در این مقاله، یک پروتکل توافق کلید احراز اصالت شده امن و مؤثر (AK) بر اساس یک روش تابع درهم‌ساز امن و مسئله لگاریتم گسسته پیشنهاد می‌شود. همچنین در بخش بعدی با مقایسه الگوریتم پیشنهادی نسبت به الگوریتم‌های مرتبط دیگر به این نتیجه می‌رسیم که الگوریتم پیشنهادی ما در مدت زمان کمتری اجرا شده و علاوه بر این در هزینه محاسباتی، ارتباطی و نحوه ذخیره‌سازی مؤثر ظاهر می‌شود و همچنین بررسی خواهیم کرد که توابع درهم‌ساز از بُعد محاسباتی با عملگر معکوس اجراء نشدنی بوده و لذا الگوریتم پیشنهادی با پیروی از این ویژگی در برابر بیشتر حمله‌های شناخته شده پایداری خواهد کرد.

## ۲ تحلیل مؤلفه‌های سیستم رمزنگاری طرح پیشنهادی

### ۱.۲ مفاهیم اساسی

طرح پیشنهادی از برخی سیستم‌های رمزنگاری، از قبیل: تابع درهم‌ساز (SHA-512)، MD5، مسئله لگاریتم گسسته، و پروتکل توافق کلید دفی هلمن و الگوریتم خم بیضوی بهره می‌گیرد. در الگوریتم SHA-1، مانند MD5 طول چکیده پیام آن ۱۶۰ بیت (معادل ۲۰ بایت) می‌باشد. هر چند طول چکیده پیام SHA-2 بیش از ۱۶۰ بیت است. اما اغلب در سیستم‌های رمزنگاری از SHA-256 و SHA-512 استفاده می‌شود. بنابراین برای هر پروتکل توافق کلید احراز اصالت شده شامل کردن مشخصه‌های امن زیر لازم می‌باشد:

۱. امنیت کلید معلوم: افشای یک کلید جلسه محرمانه نباید باعث کشف رمز کلیدهای جلسه دیگر شود. بنابراین توافق کلید می‌تواند از کشف رمز کلیدهای جلسه و حملات شخص در وسط، انعکاس، جلسه موازی، تکرار و حمله خودی جلوگیری کند.

۲. امنیت پیشرو: اگر طول کلید خصوصی یک هویت یا چند هویت کشف رمز شود؛ آن‌گاه نباید امنیت کلیدهای جلسه مرتبط دیگر تحت تأثیر قرار گیرند. سیستمی امنیت پیشرو جزئی خواهد داشت که اگر طول کلید یک هویت کشف رمز شود آن‌گاه امنیت سیستم بدون کشف رمزکردن کلیدهای جلسه قبلی تحریف خواهد شد. پس به منظور پایداری در برابر حمله جستجوی جامع برای بازیابی عدد تصادفی محرمانه، اگر اندازه عدد تصادفی بزرگتر از کلید جلسه محرمانه باشد بهتر است. لذا برای نگهداری اطلاعات محرمانه (کلید جلسه) به عدد تصادفی نیاز است؛ چون اگر کلید محرمانه فاش شود آن‌گاه کلیدهای جلسه خطر کشف رمز دارند.

۳. محرمانگی پیشرو PKG: کلید اصلی PKG ممکن است بدون خطر کشف رمزکردن کلیدهای جلسه برقرار شده امن قبلی توسط هرکاربر تحریف شود.

۴. خطرکشف رمزکلید قابلیت ارتجاع برای جعل هویت: برای هر هویتی مانند آلیس، خطرکشف رمزکردن طول کلید خصوصی آلیس، اخلاص گر را به جعل هویت آلیس قادر خواهد کرد اما این روش جعل هویت آلیس نباید اخلاص گر را قادر به جعل هویت کردن اشخاص مرتبط به آلیس کند.

۵. قابلیت ارتجاع تسهیم کلید نامعلوم: یعنی هویتی مانند آلیس نباید به تسهیم یک کلید با هر هویت هم جنس دیگری به جای باب قادر باشد. یعنی آلیس نباید تصور کند که او با هر هویت دیگر مبدل شده به جای باب تسهیم کلید می‌کند.

۶. امنیت اطلاعات موقتی - ثابت جلسه معلوم: برخی اطلاعات خصوصی به صورت تصادفی به عنوان یک ورودی تابع تولید کلید جلسه بکار برده می‌شوند؛ فاش کردن این اطلاعات موقتی خصوصی نباید امنیت کلید جلسه‌های دیگر را به خطر بیندازد.

امنیت اطلاعات موقتی - ثابت جلسه معلوم ابتدا توسط Canetti-Krawczyk [۶] در ۲۰۰۱ بررسی شد و او به این نتیجه رسید که این مشخصه امن اساسی نیاز می‌باشد و اگر امنیت زودگذر جلسات به صورت تصادفی برای اخلاص گر فاش شده باشد آن گاه امنیت کلید جلسه معین نباید تحت تأثیر قرارگیرد. هرچند در طرف مقابل فاش‌سازی اطلاعات خصوصی هم قابل چشم‌پوشی نبوده و ممکن است در برخی طرح‌های عملی این اتفاق افتاده باشد.

در ۲۰۰۹ و ۲۰۱۰، Cao etc. [۷]، [۸] دو طرح مستقل توافق کلید احراز اصالت شده براساس شناسه هویت (ID) دو سویه با دو یا سه مرحله انتقال پیشنهاد کرد که همه مشخصه‌های امن اساسی را بانجام رسانده و به عملگرهای جفتی هم نیاز نبود. اما می‌دانیم این پروتکل‌ها یک ویژگی امن اساسی با تحت عنوان امنیت اطلاعات موقتی - ثابت جلسه معلوم را پشتیبانی نمی‌کنند که یکی از مشخصه‌های امن زودگذر بوده که برامنیت کلید جلسه اثر می‌گذارد.

۷. بدون کنترل کلید: هیچکدام از هویت‌ها قادر به استفاده مجدد کلید جلسه برای مقادیر پیش فرض نمی‌باشند. قابلیت اجرای بدون اعتبارکلید تحت رویدادهای معین به خصوص درکاربردهای گروهی معین از قبیل ارتباطات امن در حرفه مراقبت سلامتی (بهداشت) مطلوب است. چون قابلیت اعتماد جزء نیازمندی‌های مجاز می‌باشد.

تاکنون برخی پروتکل‌های توافق کلید احراز اصالت شده براساس شناسه هویت با قابلیت اجرا در طرح‌های [۱۰]، [۱۲]، [۱۳]، [۱۴] و [۱۷] پیشنهاد شده‌اند. اما با بررسی و تحلیل ساختار و عملکردشان متوجه می‌شویم که اکثر آن‌ها مشخصه امن پیشرو کامل را فراهم نمی‌کنند. علی‌رغم این که Shim [۱۵] در ۲۰۰۳ مدعی بود که پروتکلی پیشنهادی‌اش همه مشخصه‌های امن را فراهم می‌کند اما در همان سال Sun and Hsieh [۱۶] آسیب‌پذیری پروتکل Shim [۱۵] را به حمله شخص در وسط اثبات کردند. در ۲۰۰۶، Gentry [۱۱] یک سیستم رمزنگاری براساس شناسه هویت پیشنهاد کرد که امنیت را در مدل استاندارد کامل کرده و مزیت‌هایی هم نسبت به سیستم‌های قبلی داشت.

باقیمانده مقاله سازمان‌دهی می‌شود به عنوان زیر:

در بخش ۳ پس‌زمینه‌های تکنیکی ضروری پروتکل بیان می‌شود و همچنین طرح رمزنگاری براساس شناسه هویت Gentry و طرح Cao بازبینی خواهند شد و دربخش ۴ طرح پیشنهادی جدید را ارائه می‌دهیم دربخش ۵ تحلیل امنیتی و پروتکل‌های پیشنهادی کارآمد و همچنین مقایسه پروتکل‌های قابل مقایسه را ارائه خواهیم داد.

## ۳ پس‌زمینه‌های تخصصی

### ۱.۳ گراف‌های خطی (دوسویه)

به فرض  $G_1$  و  $G_2$  دو گروه دوری ضربی از مرتبه اول  $p$  و  $g$  یک مولد  $G_1$  باشد و از آن‌جایی که حل مسئله لگاریتم گسسته در هر دو گروه  $G_1$  و  $G_2$  مشکل می‌باشد گراف خطی (دوسویه)  $e: G_1 \times G_1 \rightarrow G_2$  را

در نظر بگیرید که سه ویژگی زیر را ایفا می‌کند:

- خطی بودن (دوسویه): برای همه  $u, v \in G_1$  و  $a, b \in Z_p^*$  داریم  $e(u^a, v^b) = e(u, v)^{ab}$ .
- بدون تبهگنی (بدون هم‌ارزی):  $e(g, g) \neq 1$ .
- قابل مقایسه: اگر  $u, v \in G_1$  آن‌گاه می‌توان به صورت بهینه در زمان چندجمله‌ای  $G_2$   $e(u, v)$  را محاسبه کرد.

## ۲.۳ گروه‌های خم بیضوی

رمزنگاری خم بیضوی برای تأمین امنیت در سیستم رمزنگاری RSA یا DSA با مسئله لگاریتم گسسته (DLP) مرسوم می‌باشد. رمزنگاری خم بیضوی کمترین سربار محاسباتی و اندازه کلید کوچکتر و امنیت و کارآمدی بالایی دارد. گروه خم بیضوی از بُعد محاسباتی، گروهی با متغیر و ضرایب خم بیضوی محدود شده به عناصر میدان متناهی می‌باشد. سمبل  $E/Fp$  نشانگر یک خم بیضوی  $E$  روی میدان متناهی  $Fp$  اول بوده که به کمک یک معادله  $y^2 = (x^3 + ax + b) \pmod p$  با فرض  $a, b \in Z_p$  و  $4a^3 + 27b^2 \pmod p \neq 0$  تعریف می‌شود. البته نقاط روی  $E/Fp$  با یک نقطه اضافی  $o$  به فرم  $G = \{(x, y) \in F_p, E(x, y) = 0\} \cup o$  یک گروه جمعی دوری تحت عمل جمع نقاط "+" به صورت زیر تعریف می‌شود: فرض  $l, p, q \in G$  خطی شامل نقاط  $p, q$  (خط مماس به  $E/Fp$  اگر  $p = q$  باشد) و  $R$  فصل مشترک نقطه سوّم  $l$  با  $E/Fp$  است. فرض خط  $l'$  نقاط  $R$  و را مرتبط می‌کند. سپس  $p + q$  نقطه‌ای است به طوری که  $l', o$  را در  $E/Fp$  قطع می‌کند. همچنین ضرب اسکالر روی  $E/Fp$  با یک عدد صحیح با فرض تکراری کردن جمع یعنی  $kp = p + p + \dots + p$  ( $k$  times) تعریف می‌شود.

## ۳.۳ فرضیات پیچیدگی محاسبات

مسائل تعریف شده زیر بر روی گروه خم بیضوی در زمان چندجمله‌ای رامنشده (غیرعملی) فرض شده‌اند.

**تعریف ۱:** فرض محاسباتی دفی-هلمن (CDH): مولد گروه خم بیضوی  $G$  و بازاء  $a, b \in Z_p^*$  با تعیین  $aP$  و  $bP$ ، محاسبه کردن  $abP$  مشکل است.

**تعریف ۲:** فرض قطعی دفی-هلمن (DDH): مولد گروه خم بیضوی  $G$  و بازاء  $a, b, c \in Z_p^*$  با معین کردن  $aP$  و  $bP$  و  $cP$ ، تعیین این که آیا  $cP = abP$  مشکل می‌باشد.

**تعریف ۳:** شکاف فرض دفی-هلمن (Gap-DH): با معین کردن سه تایی  $\{P, aP, bP\} \in G$  جایی که بازاء  $a, b, c \in Z_p^*$  محاسبه  $abP$  به کمک اوراکل (غیب‌گو) DDH مشکل می‌باشد (پاسخ‌دهی به طوری که یک چهارگانه معین یک چهارگانه DH است یا خیر).

## ۴ طرح پیشنهادی جدید

در این بخش، ما یک پروتکل توافق کلید کارآمد و احراز اصالت شده یک طرفه امن براساس شناسه هویت پیشنهاد می‌کنیم که تقریباً همه مشخصه‌های امن شناخته شده، مخصوصاً امنیت داده موقتی-ثابت جلسه معلوم را بانجام می‌رساند. امنیت پروتکل پیشنهادی می‌تواند فرض محاسباتی دفی هلمن CDH را در مدل اوراکل تصادفی کاهش دهد. پروتکل شامل ۴ مرحله راه‌اندازی، تولید کلید، توافق کلید و تصدیق صحیح می‌باشد؛ که ۳ مرحله اول تقریباً با اندکی اصلاحات با طرح Cao [۶] یکسان بوده اما در تولید کلید جلسه متفاوت است. ما تمایل داریم یک پروتکل توافق کلید براساس یک شناسه هویت قابل اجرا را طوری پیشنهاد کنیم که کلید جلسه کاربر بتواند توسط PKG بازیابی شود در حالی که در طرح‌های مرتبط دیگر اشخاص می‌توانند کلیدهای جلسه گذشته کاربر را بازیابی کنند حتی اگر طول کلید بزرگ باشد. پروتکل شامل ۳ هویت می‌باشد: دو کاربر به نام آلیس و باب به برقراری یک کلید جلسه محرمانه تسهیم شده تمایل دارند و PKG مرکز تولید و توزیع کلیدهای خصوصی کاربر با کاربرد کلید اصلی آنها مسئول می‌باشد.

ما به منظور حفظ تشریح یکپارچگی مراحل، پروتکل را به صورت زیر ارائه می‌دهیم:

۱. **راه‌اندازی:** مولد کلید خصوصی PKG ابتدا پارامترهای سیستم و سپس جفت کلید خصوصی/عمومی را تولید می‌کند به عنوان زیر:

مولد کلید خصوصی PKG با تعیین یک پارامتر امن سیستم به عنوان  $K$ ، گانه  $\{E/Fp, G, p\}$  و کلید خصوصی اصلی  $x \in Z_p^*$  را انتخاب می‌کند و کلید عمومی را به عنوان  $P_{pub} = kp^x$  محاسبه کرده و سپس  $G$  و  $G_T$  دو گروه از مرتبه اول  $p$ ، سه تابع درهم‌سازی رمزنگاری امن و یک نگاشت خطی انتخاب می‌کند و خواهیم داشت:

$$\begin{aligned} e &: G \times G \rightarrow G_T \quad (\text{نگاشت خطی}) \\ H_1 &: \{0, 1\}^* \times G \rightarrow Z_p^* \\ H_2 &: \{0, 1\}^* \times \{0, 1\}^* \times G \times G \times G \rightarrow \{0, 1\}^k, \\ H_3 &: \{0, 1\}^* \times \{0, 1\}^* \times G \times G \times G \times G \rightarrow \{0, 1\}^k \end{aligned}$$

$$\text{Let } g, p, t \in G, t = g^x \text{ mod } p, g_T = e(g, t) \in G_T.$$

سپس PKG پارامترهای عمومی سیستم را به عنوان  $\langle E/Fp, G, P_{pub}, t, g_T, H_1, H_2, H_3 \rangle$  منتشر می‌کند. در ضمن کلید خصوصی اصلی PKG، متغیر  $x$  می‌باشد.

۲. **تولید کلید:** مرکز تولید کلید به منظور احراز هویت کاربر در  $Z_p^*$ ، یک کلید خصوصی طولانی ایجاد کرده و همچنین برای یک کاربر با شناسه هویت  $ID \in Z_p^*$ ،  $ID \neq x$ ، یک عدد تصادفی  $r_{ID} \in Z_p^*$  متناسب با شناسه هویت معین  $ID$  نسبت داده و معادله  $R_{ID} = (kp^{-r_{ID}})^{(x-ID)}$ ،  $h_{ID} =$



می دهد جایی که  $s_{ID} = r_{ID} + h_{ID}x$  و  $H_1(ID||R_{ID})$  را محاسبه کرده و کلید خصوصی  $d_{ID} = \langle R_{ID}, s_{ID} \rangle$  را به عنوان خروجی

سپس کلید خصوصی طولانی کاربر به همراه شناسه هویت کاربری از طریق کانال امن به کاربر منتقل شده و کاربر با شناسه هویت  $ID$  می تواند کلید خصوصی طولانی اش را با بررسی کردن معادله  $s_{ID}P = R_{ID} + H_1(ID||R_{ID})P_{pub}$  تصدیق کند.

کلید خصوصی طولانی معتبر است اگر معادله صحیح نگه داشته شود و بالعکس. فرض کنید دو هویت به نام آلیس (عمل کننده آغازگر) و باب (به عنوان پاسخ دهنده) وجود داشته باشند که می خواهند کلید جلسه برقرار شود.

۳. **توافق کلید:**  $ID_B$  و  $ID_A$  شناسه تعیین هویت آلیس و باب بوده که یک کلید جلسه تسهیم شده را با احراز اصالت در پروتکل زیر اجرا خواهند کرد.

#### Scheme 1.

(1)  $A \rightarrow B : ID_A, R_A$ .  $B$  chooses  $b \in Z_p^*$  and computes the message

$$T_B = g_B^{b(R_A + H_1(ID_A||R_A)P_{pub})} \text{ mod } p$$

(2)  $B \rightarrow A : ID_B, R_B, T_B$ .  $A$  chooses  $a \in Z_p^*$  and computes the message

$$T_A = g_A^{a(R_B + H_1(ID_B||R_B)P_{pub})} \text{ mod } p$$

(3)  $A \rightarrow B : T_A$ .  $B$  computes  $K_{BA} = (b+1)s_B^{-1}T_A + H_1((ID_A||R_A)P_{pub}) + bp$  and

$$SK_{BA} = H_2(ID_A||ID_B||T_A||T_B||K_{BA}); \text{ Finally } A \text{ computes}$$

$$K_{AB} = (a+1)s_A^{-1}T_B + H_1((ID_B||R_B)P_{pub}) + aP \text{ and}$$

$$SK_{BA} = H_2(ID_A||ID_B||T_A||T_B||K_{BA}).$$

۴. **صحت تصدیق:** در پایان اجرای پروتکل، آلیس و باب روی کلید جلسه یکسان توافق می کنند. ما می توانیم به آسانی تصدیق کنیم که  $sk = SK_{BA} = SK_{AB}$  همچنین از فرم معادله  $SK_{AB}$  و  $SK_{BA}$  می توان تشخیص داد که اگر اخلاص گر  $a$  و  $b$  جلسات محرمانه موقت-معین را بشناسند آن ها نمی توانند کلید جلسه ی  $SK_{BA}$  یا  $SK_{AB}$  را بگیرند؛ برای این که اخلاص گر نمی تواند  $T_B, T_A, H_1((ID_B||R_B)P_{pub})$  و همچنین  $s_A^{-1}$  و  $s_B^{-1}$  را محاسبه کند، زیرا به طور محاسباتی معکوس تابع درهم ساز بدون شناختن کلید محرمانه سرور غیر عملی است و همچنین طرح مشخصه



امن اضافی، امنیت داده موقتی / ثابت (معین) جلسه معلوم را به آسانی پشتیبانی می کند زیرا:

$$\begin{aligned} K_{AB} &= (a + 1)s_A^{-1}T_B + H_1((ID_B||R_B)P_{pub}) + ap \\ &= as_A^{-1}T_B + s_A^{-1}T_B + H_1((ID_B||R_B)P_{pub}) + ap \\ &= abp + ap + bp + s_Bp \\ &= bap + bp + ap + s_AP \\ &= bs_B^{-1}T_A + s_B^{-1}T_A + H_1((ID_A||R_A)P_{pub}) + bp \\ &= (b + 1)s_B^{-1}T_A + H_1((ID_A||R_A)P_{pub}) + bp = K_{BA} \end{aligned}$$

بنابراین ما کلید جلسه توافق شده یکسان را به دست می آوریم به صورت  $sk = SK_{BA} = SK_{AB}$

## Scheme 2.

- (1)  $A \rightarrow B : ID_A, R_A, T_A$ . The initiator  $A$  chooses a random ephemeral key  $a \in Z_p^*$ , and compute the message  $T_A = aP$
- (2)  $B \rightarrow A : ID_B, R_B, T_B$  On receiving the message from  $A$ , The responder  $B$  chooses a random ephemeral key and compute the message  $T_B = bP$ ;

Finally,  $A$  computes  $K_{AB} = (T_B + R_B + H_1(ID_B||R_B)P_{pub})(a + s_A)$ ;  
 $B$  computes  $K_{BA} = (T_A + R_A + H_1(ID_A||R_A)P_{pub})(b + s_B)$ ;  
 It is easy to validate that  $K_{AB} = (T_B + R_B + H_1(ID_B||R_B)P_{pub})(a + s_A)$ ;  
 $= (bP + s_BP)(a + s_A) = (aP + s_AP)(b + s_B)$   
 $= (T_B + R_B + H_1(ID_B||R_B)P_{pub})(b + s_B) = K_{BA}$   
 $= (a + s_A)(b + s_B)P = abP + as_BP + bs_AP + s_As_BP$

ما می توانیم بررسی کنیم که آیا  $sk = SK_{BA} = SK_{AB}$

## ۵ تحلیل امنیتی و کارآمدی

در این بخش، تحلیل امنیتی جامع، راندمان طرح پیشنهادی و مقایسه کارآمدی پروتکل های کاربردی را ارائه می دهیم.

### ۱.۵ تحلیل امنیتی

حال اثبات خواهیم کرد که پروتکل پیشنهادی تعدادی مشخصه امن مطلوب از قبیل: امنیت کلید معلوم، امنیت پیشرو PKG، قابلیت ارتجاع جعل هویت در برابر خطرکشف رمزکلید، قابلیت ارتجاع تسهیم کلید نامعلوم، کنترل نکردن کلید پشتیبانی کرده و همچنین به طور خاص امنیت پیشرو کامل را بانجام می رساند.

### ۱.۱.۵ امنیت کلید معلوم

اگر یک کلید جلسه کشف رمز شود به معنای این نیست که هر کلید جلسه دیگری کشف رمز خواهد شد در حقیقت هر اجرای پروتکل یک کلید جلسه متفاوت را محاسبه می کند که به کلیدهای خصوصی موقت  $x$  و  $y$  وابسته است. تا جایی که  $x$  و  $y$  به طور تصادفی توسط آلیس و باب به طور مستقل انتخاب می شوند.

### ۲.۱.۵ قابلیت ارتجاع جعل هویت در برابر خطرکشف رمزکلید

فرض یک اخلاص گر از جنس مؤنث کلید طولانی خصوصی را شناسایی کرده و تمایل داشته باشد به عنوان باب به آلیس مبدل شود. علی رغم این که جنس مؤنث می تواند با شناسه هویت باب خودش را بشناساند و  $T_B$  را به آلیس ارسال کند. اما او نمی تواند بدون شناختن کلید خصوصی باب،  $K_{BA}$  را برای محاسبه کلید جلسه یکسان همانند آلیس بکار گیرد.

### ۳.۱.۵ قابلیت ارتجاع تسهیم کلید نامعلوم

اخلاص گر برای حمله کردن به پروتکل پیشنهادی، به یادگیری کلید خصوصی هویت یکسان نیاز دارد. هر چند می دانیم که مشخصه قابلیت ارتجاع تسهیم کلید نامعلوم با احراز اصالت کلید ضمنی دلالت داشته و از این رو اخلاص گر به آسانی نمی تواند به کلید خصوصی دسترسی یابد.

### ۴.۱.۵ بدون کنترل کلید

در این پروتکل،  $x$  و  $y$  توسط آلیس و باب به طور تصادفی انتخاب می شوند و هویت دیگری قادر به مجبورکردن کلید جلسه به منظور انتخاب مقدار پیش فرض نمی باشد. حال اگر اخلاص گری از جنس مؤنث پیام معاوضه شده با چنین فرضی را اصلاح کند آن - گاه آلیس و باب می توانند به سختی کلید جلسه یکسان را محاسبه کنند.

### ۵.۱.۵ امنیت توافق کلید

کشف یک کلید جلسه امن نباید باعث خطر کشف رمز کلیدهای جلسه دیگر شود. بنابراین توافق کلید می تواند از کشف رمز کلیدهای جلسه و حملات شخص در وسط، انعکاس، جلسه موازی، تکرار و حمله خودی جلوگیری نماید و همچنین به منظور پایداری در برابر حمله جستجوی جامع برای بازیابی عدد تصادفی محرمانه، اگر اندازه عدد تصادفی بزرگتر از کلید جلسه محرمانه باشد بهتر است. بنابراین به منظور نگهداری اطلاعات محرمانه (کلید جلسه محرمانه) به عدد تصادفی نیاز است چون اگر کلید محرمانه فاش شود آن گاه کلیدهای جلسه خطر کشف رمز دارند.

### ۶.۱.۵ امنیت پیشرو کامل

اگر کلیدهای طولانی دو بخشی کشف رمز شوند یک شخص (به جز PKG) می تواند  $K_{AB_1}$ ،  $K_{BA_1}$  و  $<$   $asBP$ ،  $bsAP$ ،  $sasBP$ ،  $T_A$ ،  $T_B$ ،  $s_A^{-1}$ ،  $s_B^{-1}$ ،  $H_1((ID_B || R_B)P_{pub}) >$  اما او نمی تواند

$K_{BA_r}$  و  $K_{AB_r}$  را بدون شناختن کلید جلسه یکسان توافق شده با  $SK_{BA} = SK_{AB}$  محاسبه  $sk = SK_{BA}$  محاسبه کند؛ چون به منظور محاسبه‌ی  $K_{BA_r}$ ،  $K_{AB_r}$ ،  $K_{BA_l}$ ،  $K_{AB_l}$  در دو طرح پیشنهادی فوق، باید مسئله‌ی سخت محاسبه‌ی دفی-هلمن و معکوس تابع درهم‌ساز حل شود.

### ۷.۱.۵ امنیت پیشرو PKG

اگر اخلاص کلید اصلی سیستم را PKG به دست آورد به این معناست که اخلاص گر می‌تواند کلید خصوصی هر دوی آلیس و باب را به دست آورد. اما هنوز قادر نیست کلید خصوصی را محاسبه کند زیرا حل مسئله‌ی محاسباتی دفی-هلمن و معکوس تابع درهم‌ساز غیرعملی است.

### ۸.۱.۵ امنیت داده موقت - معین (ثابت) جلسه معلوم

اگر اخلاص گر پارامتر  $a$  و  $b$  محرمانه‌ی جلسه‌ی موقت را شناسایی کند آن‌گاه او می‌تواند فقط  $< abP, asBP, bsAP, RID >$  محاسبه کند اما نه هر دو کلید طولانی  $sASBP, sID$ . برای محاسبه‌ی  $sASBP$ ، نیاز است حداقل یکی از کلیدهای خصوصی طولانی آلیس و باب به دست آید که هنوز یک مسئله‌ی سخت محاسباتی دفی-هلمن می‌باشد در این طرح محاسبه‌ی  $K_{BA}$  یا  $K_{AB}$  فقط به دو عملگر اسکالر جمع و دو عملگر اسکالر ضرب نیاز دارد. اگر ما پیش پردازش محاسبه‌ی  $RID + H_1(IDID || RID)P_{pub}$  را در نظر بگیریم آن‌گاه فقط هزینه‌ی محاسباتی یک عملگر اسکالر جمع و یک عملگر اسکالر ضرب نیاز می‌باشد. پس طرح پیشنهادی خیلی کارآمدتر از طرح Cao خواهد بود.

### ۹.۱.۵ پایداری به حمله‌ی اصلاح (تحریف و دستکاری)

در پروتکل پیشنهادی هر پیام احراز هویت با عدد تصادفی محرمانه‌ی جدید و مهر زمانی به همراه تابع درهم‌ساز پشتیبانی می‌شود و بدون عدد تصادفی، مهاجم قادر نبوده مقدار درهم‌ساز صحیحی برای پیام احراز هویت محاسبه نماید. بنابراین ایجاد یک پیام تحریف شده موفق از پیام معتبر بسیار دشوار خواهد بود.

### ۱۰.۱.۵ پایداری به حمله‌ی فاش کلید محرمانه سرور

اگر کلید محرمانه سرور  $x$  فاش شود، با این حال اخلاص گر نمی‌تواند  $IDID$  و  $hID$  را از  $RID + H_1(IDID || RID)P_{pub}$  بازیابی نماید. چون به دلیل کاربرد یک روش تابع درهم‌ساز  $h(\cdot)$  سرور می‌تواند به آسانی کلید محرمانه‌ی  $x$  را تغییر و اصلاح کرده و دوباره بازگرداند. یادآوری می‌کنیم فاش شدن کلید محرمانه‌ی سرور خطر کشف رمز کلیدهای جلسه را در پی خواهد داشت.

### ۱۱.۱.۵ پایداری به حمله‌ی فریب سرور

در حمله‌ی فریب سرور، یک اخلاص گر نمی‌تواند به عنوان یک سرور مجاز مبدل شود برای این که نمی‌تواند  $sASBP, sID, RID$  را بدون شناسایی  $IDID, rID$  و  $x$  محاسبه نماید. بنابراین سرور نمی‌تواند  $sk = SK_{BA} = SK_{AB}$  را بدون شناسایی  $IDID$  محاسبه نماید و همچنین کلید جلسه برای کاربر یکسان در جلسه ورود مختلف متفاوت است. پس طرح در برابر حمله‌ی فریب سرور امن است.

### ۱۲.۱.۵ پایداری به حمله جلسه موازی

اگر فرض کنیم اخلاص گر بتواند به عنوان کاربر مجاز  $U_i$  با تکرار مجدد پیام درخواست ورود به سیستم  $\{ID_A, R_A\}, \{ID_B, R_B, T_B\}$ ، در چارچوب زمان معتبر مبدل شود اما در مرحله بعد اخلاص گر نمی تواند پیام تصدیق  $sk = SK_{BA} = SK_{AB}$  را محاسبه نماید؛ زیرا پیام تصدیق شامل هر داده ای برای ایجاد مراحل بعدی نمی باشد و علاوه بر این امنیت پیام احراز اصالت طرح پیشنهادی در برابر حمله جلسه موازی به پیچیدگی محاسباتی لگاریتم گسسته، روش تابع درهم ساز، خم بیضوی و پروتکل توافق کلید دفی-هلمن وابسته است.

### ۱۳.۱.۵ پایداری به حمله خودی

اگر یک خودی مصون سرور، اطلاعات محرمانه سرور از قبیل  $\langle abP, as_{BP}, bs_{AP}, R_{ID} \rangle$  به دست آورد. او نمی تواند اطلاعات حساس مشابه مانند  $s_{ASBP}, s_{SID}$  و  $R_{ID} + H_1(ID_{ID} || R_{ID})P_{pub}$  استخراج نماید برای این که از نظر محاسباتی معکوس یک روش تابع درهم ساز غیر عملی است و علاوه بر این، حل کردن مسئله لگاریتم گسسته مشکل است و نیز توافق کلید جلسه می تواند از حمله خودی جلوگیری نماید.

### ۱۴.۱.۵ پایداری به حمله تکرار (اجرای مجدد)

فرض کنیم اخلاص گر پیام تقاضای ورود به سیستم  $\{ID_A, R_A\}, \{ID_B, R_B, T_B\}$  از کاربر  $U_i$  جعل هویت کند و بتواند پیام یکسانی را به سرور تکرار نماید. (البته این کار به ندرت اتفاق می افتد) هر چند او نمی تواند یک حمله اجرای مجدد روی پروتکل احراز اصالت جدید ایجاد نماید زیرا پیام احراز هویت سرور با اعداد تصادفی و تمبر زمانی ترکیب شده است؛ در این مورد اگر مهاجم یک پیام قدیمی را از طرف سرور اجرای مجدد کند آن گاه سرور می تواند به آسانی حمله اجرای مجدد را با بررسی پیام ورود به سیستم با عدد تصادفی فعلی و مهر زمان کشف نماید زیرا در هر مرحله عدد تصادفی جدیدی برای هر تقاضای ورود به سیستم جدید انتخاب می کند. از این رو طرح پیشنهادی در برابر حمله تکرار پایدار است.

### ۲.۵ مقایسه پروتکل با پروتکل های موجود

یک مثال از پروتکل توافق کلید احراز اصالت شده براساس یک شناسه در سبک قابل اجرا، پروتکل پیشنهادی توسط Kudla and Chen [۱۴] می باشد. یک بازخورد این پروتکل (و همچنین پروتکل توافق کلید احراز اصالت شده براساس شناسه هوشمند [۱۰]) این می باشد که هر دوی آنها مشخصه امنیت کامل پیشرو را فراهم نمی کنند. علی رغم اینکه Shim [۱۵] در پروتکل پیشنهادی اش ادعا می کند چنین مشخصه ای را فراهم می کند. اما او بعداً در طرح [۱۶] یافت که طرحش به حمله شخص در وسط آسیب پذیر است. در سال ۲۰۰۵، Wang [۱۷] یک پروتکل توافق کلید احراز اصالت شده براساس یک شناسه هویت پیشنهاد کرد که امنیت پیشرو کامل را در سبک قابل اجرا بانجام می رساند اما طرح او برای اجرا به ۳ عملگر توان در  $G$ ، یک ضرب در  $G$  و یک جفت کننده نیاز داشت. علی رغم این که پروتکل ما نیاز دارد که یک عملگر توان در  $G$ ، ۴ عملگر توان در  $G_T$ ، و یک جفت کننده را اجرا کند. بازدهی محاسباتی دو طرح فوق تقریباً یکسان بوده

و همچنین خیلی کارآمدتر از طرح Cao می باشد برای این که می تواند از کشف رمز کلیدهای جلسه و حملات شخص در وسط، انعکاس، جلسه موازی، تکرار، فریب سرور و حمله خودی جلوگیری کند.

### ۳.۵ تحلیل هزینه و عملکرد

در طرح پیشنهادی، کلید محرمانه سرور، ID (شناسه هویت) و خروجی تابع درهم ساز همگی به طول ۱۶۰ بیت هستند. تابع درهم ساز امن (SHA-1) مقدارهایی به طول ۱۶۰ بیت اجرا می کند. همچنین مهر زمانی به طول ۴۰ بیت و شناسه به طول ۳۲ بیت است.

### ۶ نتیجه گیری

امنیت کامل داده موقت - ثابت (معین) جلسه یک ویژگی امن اساسی برای پروتکل های توافق کلید احراز اصالت شده به حساب می -آید (در هر دو سبک قابل اجرا و بدون اجرا). ما یک پروتکل توافق کلید احراز اصالت شده براساس یک شناسه ارائه دادیم که در سبک قابل اجرا امن می باشد و همچنین نشان دادیم که پروتکل پیشنهادی تقریباً همه مشخصه های امن شناخته شده، مخصوصاً مشخصه امنیت کامل داده موقت - ثابت (معین) جلسه را با بهره وری محاسباتی خوب فراهم می کند و نیز در برابر اکثر حملات شناخته شده مقاوم است.

### مراجع

- [1] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, "Universal designated verifier signatures," in *Asiacrypt'03*, vol. LNCS 2894, pp. 523-542, 2003.
- [2] F. Laguillaumie and D. Vergnaud, "Designated verifier signatures: anonymity and efficient construction from any bilinear map," IACR eprint.
- [3] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology: Proc. Crypto '84*, Lecture Notes in Computer Science vol. 196, (Berlin), pp. 47-53, Springer-Verlag, 1985.
- [4] A. Shamir, Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS Vol. 196, Springer, Heidelberg. pp. 47-53.
- [5] Mandt TK, Tan CH. Certificateless authenticated two-party key agreement protocols. In: Okada M, Satoh I, eds. Proc. of the 11th Annual Asian Computing Science Conference (ASIAN'06), Secure Software and Related Issues, LNCS 4435, Berlin/Heidelberg: Springer-Verlag, pp. 37-44, 2008.
- [6] Canetti R, Krawczyk H. Analysis of key exchange protocols and their use for building secure channels. In: Pfitzmann B, ed. Proc. of the Advances in Cryptology (EUROCRYPT'01), LNCS 2045, Berlin/Heidelberg: Springer-Verlag, 2001. pp. 453-474.

- [7] Cao Xue-fei, Kou Wei-dong, Fan Kai, Zhang Jun, "An Identity-Based Authenticated Key Agreement Protocol without Bilinear Pairing," Chinese Journal of Electronics & Information Technology 31(5), 2009, pp.1241-1244.
- [8] X.F. Cao, W.D. Kou, X.N. Du, "A Pairing-free Identity-Based Authenticated Key Agreement Protocol with minimal Message Exchanges," Information Sciences 180(15), 2010, pp. 2895-2903.
- [9] A. Cilardo, L. Coppolino, N. Mazzocca, L. Romano, Elliptic curve cryptography engineering, Proceedings of the IEEE, 94(2), 2006, pp. 395-406.
- [10] N.P. Smart, "An identity based authenticated key agreement protocol based on the Weil pairing," Electronics Letters, 38(13), pp. 630-632, 2002.
- [11] C. Gentry, "Practical identity-based encryption without random oracles," Proc. of the EUROCRYPT'06, Lecture Notes in Computer Science 4004, Berlin: Springer-Verlag, pp 445-464, 2006.
- [12] S.B. Wang, Z.F. Cao, and X.L. Dong, "Provably secure identity-based authenticated key agreement protocols in the standard model," Chinese Journal of Computers 30(1), pp. 1842-1854, 2007.
- [13] N. McCullagh, and P.S.L.M. Barreto. "A new two-party identity-based authenticated key agreement," Proc. of CT-RSA 2005, LNCS vol. 3376, Springer-Verlag, New York, pp. 262-274, 2005.
- [14] L. Chen, and C. Kudla, "Identity based key agreement protocols from pairings," Proc. of the 16th IEEE Computer Security Foundations Workshop, IEEE Computer Society, pp. 219-213, 2002. See also Cryptology ePrint Archive, Report 2002/184.
- [15] K. Shim, "Efficient ID-based authenticated key agreement protocol based on the Weil pairing," Electronics Letters 9(8), pp. 653-654, 2003.
- [16] H. Sun, and B. Hsieh. "Security analysis of Shim's authenticated key agreement protocols from pairings," Cryptology ePrint Archive, Report 2003/113, 2003. Available at <http://eprint.iacr.org/2003/113>.
- [17] Y. Wang, "Efficient identity-based and authenticated key agreement protocol," Cryptology ePrint Archive, Report 2005/108, 2005. Available at <http://eprint.iacr.or>
- [18] Boyd, C., Choo, K.-K.R.: Security of Two-Party Identity-Based Key Agreement. In: Dawson, E., Vaudenay, S. (eds.) Mycrypt 2005. LNCS Vol. 3715, Springer, Heidelberg. pp. 229-243.
- [19] L. Chen, and C. Kudla, "Identity based key agreement protocols from pairings," Proc. of the 16th IEEE Computer Security Foundations Workshop, IEEE Computer Society, 2002, pp. 219-213.
- [20] Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: Symposium on Cryptography and Information Security, Okinawa, Japan, 2000.

- [21] Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis. In: Darnell M, ed. Proc. of the 6th IMA International Conference on Cryptography and Coding, LNCS 1355, Berlin/Heidelberg: Springer-Verlag, 1997, pp. 30–45.



# تصدیق دیجیتال کلید عمومی برای احراز اصالت کاربر و برقراری کلید جلسه برای ارتباطات شبکه‌ای امن

امیرحسین رحیمی<sup>۱</sup>

<sup>۱</sup> کارشناس ارشد رمز و مربی دانشگاه آزاد اسلامی، واحد قم، گروه ریاضی، قم  
amir.rahimi361@gmail.com

## چکیده

تصدیق دیجیتال کلید عمومی به تنهایی نمی‌تواند به عنوان عاملی امن برای احراز اصالت کاربر به کار رود؛ اما در ساختار کلید عمومی (PKI) می‌تواند به منظور تأمین احراز اصالت کلید عمومی کاربر و توافق کلید بکار رود. تصدیق دیجیتال تعمیم یافته‌ی (GDC) شامل اطلاعات عمومی کاربر از قبیل: اطلاعات تصدیق‌کننده‌ی دیجیتال کاربر، اطلاعات تصدیق تولد دیجیتال و اطلاعات عمومی تصدیق اعتبار (گواهینامه) امضای دیجیتال (CA) و غیره می‌باشد؛ یک GDC شامل هر کلید عمومی کاربر نبوده برای این که کاربر هر جفت کلید خصوصی و عمومی را در اختیار ندارد. مدیریت کلید در بکارگیری GDC خیلی آسان‌تر از کاربرد تصدیق دیجیتال کلید عمومی بوده و درحقیقت امضای دیجیتال GDC به عنوان یک توکن محرمانه هر کاربر به کار برده می‌شود که به هر تصدیق‌کننده‌ای فاش نمی‌شود؛ در عوض مالک امضای دیجیتال، تصدیق امضایش را با پاسخ‌دهی به چالش تصدیق‌کننده اثبات می‌کند. لذا بر اساس این مفهوم، ما دو پروتکل بر اساس عامل‌یابی عدد صحیح (IF) و لگاریتم گسسته (DL) پیشنهاد می‌کنیم که می‌تواند احراز اصالت کاربر و برقراری کلید محرمانه را به انجام رساند.

**کلمات کلیدی:** توافق کلید، احراز اصالت کاربر، مولد کلید خصوصی (PKG)، گواهی دیجیتال، تابع درهم‌ساز، لگاریتم گسسته، کلید جلسه محرمانه.

## ۱ مقدمه

از گذشته تا حال احراز اصالت کاربر و برقراری کلید جلسه دو سرویس اساسی در ارتباطات امن بوده است و همواره تصدیق دیجیتال کلید عمومی برای احراز اصالت کاربر و برقراری کلید بکار رفته است. یک تصدیق دیجیتال ترکیبی از یک عبارت (شامل کلید عمومی و بعضی اطلاعات عمومی مرتبط به کاربر) و یک امضای دیجیتال عبارت می‌باشد.

هرچند تصدیق دیجیتال کلید عمومی فقط شامل اطلاعات عمومی بوده که می‌تواند به آسانی ثبت شده و یکبار دیگر برگشت داده شود؛ اما برای احراز اصالت یک کاربر توصیه نمی‌شود. از تصدیق‌های دیجیتال

شناخته شده می‌توان تصدیق دیجیتال کلید عمومی X.509 را نام برد که در بسیاری از موارد در ساختار کلید عمومی (PKI) برای تأمین احراز اصالت کلید عمومی کاربر به کار می‌رود. ما در طرح پیشنهادی شیوه جدیدی معرفی خواهیم کرد که قادر است یک کاربر را احراز اصالت کرده و همچنین یک کلید جلسه تسهیم شده محرمانه با شریک ارتباطی کاربر را با استفاده از کاربرد تصدیق‌های دیجیتال، از قبیل: یک تصدیق کننده دیجیتال (برنامه راه انداز)، یک تصدیق تولد دیجیتال یا یک ID دیجیتال و غیره برقرار کند. این نوع تصدیق دیجیتال به عنوان یک تصدیق دیجیتال تعمیم یافته (GDC) شناخته می‌شود و همچنین توصیه کاربرد این نوع تصدیق دیجیتال برای مدیریت تصدیق‌های دیجیتال کلید عمومی X.509 خیلی آسان تر می‌باشد.

تصدیق دیجیتال تعمیم یافته (GDC) به عنوان عاملی امن برای تأمین احراز اصالت کاربر می‌باشد که شامل اطلاعات عمومی کاربر (کاربر هر جفت کلید خصوصی و کلید عمومی را در دسترس ندارد) و یک امضای دیجیتال اطلاعات عمومی بوده که توسط مرکز صدور گواهینامه مورد اعتماد CA امضا می‌شود. علاوه بر این مالک GDC نمی‌تواند متن اصلی امضای GDC را به هر تصدیق کننده‌ای فاش کند در عوض می‌تواند با یک کلید جلسه محرمانه پاسخ به چالش تصدیق کننده را برآورد کند زیرا او تصدیق امضای دیجیتال را در دسترس دارد. پس به طور کلی امضای دیجیتال GDC به عنوان یک توکن محرمانه هرکاربر برای احراز اصالت امن کاربر بکاربرده می‌شود.

تفاوت بین تصدیق دیجیتال تعمیم یافته (GDC) و تصدیق دیجیتال کلید عمومی این است که در یک GDC اطلاعات عمومی شامل هر کلید عمومی کاربر نمی‌باشد.

### سه هویت اساسی و کاربردی تصدیق دیجیتال عبارتند از:

۱. اعتبار تصدیق مرکز صدور گواهینامه (CA): CA شخص مورد اعتماد یا سازمان صلاحیت دار که به صورت دیجیتال یک دستور (عبارت) را با کلید خصوصی مالکش امضاء می‌کند.

۲. مالکیت یک تصدیق دیجیتال تعمیم یافته (GDC): مالکیت (GDC) شخصی است که (GDC) را از یک مرکز صدور گواهی مورد اعتماد روی CA یک کانال امن دریافت می‌کند و همچنین به محاسبه یک «جواب» معتبر در پاسخ به چالش «سؤال» تصدیق گر به منظور احراز اصالت و برقراری یک کلید جلسه محرمانه نیاز دارد.

۳. تصدیق کننده: تصدیق کننده شخصی است که مالک GDC را به چالش می‌کشد و پاسخ را با به کار بردن اطلاعات عمومی مالک و کلید عمومی CA تأیید اعتبار می‌نماید.

در اکثر تحقیقات ثبت شده در زمینه کاربردهای احراز هویت کاربر، یک مقام صلاحیت دار مورد اعتماد برای صدور کارت تعیین هویت با اطلاعات کاربری، از قبیل نام کاربری و یک عکس شخصی روی کارت، برای هرکاربر مسئول بوده و هر کاربر می‌تواند بر اساس این اطلاعات کاربری با موفقیت تعیین هویت شود اگر همواره مالک مجاز کارت باشد.

جدول ۱: نمادگذاریها

نماد	تعریف	نماد	تعریف
$ID$	شناسه‌ی هویت کاربر	$\oplus$	عملگر XOR
$Z_p^*$	گروه ضربی $p$	$Z_q$	حلقه صحیح به پیمانۀ $q$
$R_A$	عدد تصادفی تولیدشده توسط $A$	$T_A$	مهر زمان کاربر $A$
$DVS$	امضای تصدیق‌کننده طراحی شده	$H(\cdot)$	تابع درهم‌ساز امن
$GDC$	تصدیق دیجیتال تعمیم‌یافته	$\parallel$	عملیات الحاق
$DHA$	فرض دفی-هلمن	$GDHA$	فرض دفی-هلمن تعمیم‌یافته
$q$ و $p$	دو عدد اول بزرگ به طوری که $p = 2q + 1$	$H(\cdot)$	تابع درهم‌ساز امن
$PKI$	ساختار کلید عمومی	$PKG$	مولد کلید خصوصی
$CA$	مرکز صدور گواهینامه	$m_A$	چکیده پیام
$DL$	لگاریتم گسسته	$IF$	پروتکل برقراری کلید و عامل‌یابی عدد صحیح
$x_A$	کلید خصوصی	$y_A$	کلید عمومی

در بخش بعدی، ما محاسن و معایب طرح‌های مرتبط گذشته را بررسی خواهیم کرد. در بخش ۳ بعضی مقدمات در زمینه تصدیق دیجیتال را معرفی خواهیم کرد و همچنین احراز اصالت کاربر مبتنی بر لگاریتم گسسته (DL) و پروتکل برقراری کلید را با کاربرد GDC تشریح خواهیم کرد. در بخش ۴ احراز اصالت کاربر را بر اساس عامل‌یابی عدد صحیح و پروتکل برقراری کلید (IF) بیان خواهیم کرد و در نهایت نتیجه‌گیری را در بخش ۵ خواهیم داشت.

## ۲ کارهای مرتبط

در گذشته یک امضای دیجیتال سنتی به منظور احراز اصالت یک پیام معین برای دریافت‌کننده امضا به کار می‌رفت. هرچند در این روش گاهی اوقات کلید خصوصی امضاءکننده مختل می‌شد چون گاهی اوقات یک دریافت‌کننده معاند می‌توانست به راحتی امضای دیجیتال ارسال‌کننده را به هر بخش سوئی بدون موافقت ارسال‌کننده فاش کند و به دنبال آن هر شخصی می‌توانست به کلید عمومی امضاءکننده و امضای دیجیتال معتبر دسترسی یابد.

در سال ۱۹۸۹، Chaum و Antwerpen [۵] نظریه امضای انکارناپذیر را معرفی کردند؛ نظریه آن‌ها امضاءکننده را به دستیابی کنترل کامل روی امضایش قادر ساخته و علاوه بر این برای تصدیق یک امضای انکارناپذیر به تسهیم امضای پیام نیاز داشت. هرچند این روند می‌توانست تصدیق‌کننده‌های نامطلوب را از اعتبار دادن امضاء جلوگیری نماید اما مسئله واقعی انکارناپذیری امضا این بود که امضاءکننده به اعتباردهی تصدیق‌کننده نیاز داشت قبل از این که تصدیق‌کننده برای تأیید اعتبار امضای انکارناپذیر کمک کند.

امضاهای تصدیق‌کننده طراحی شده (Designated Verifier Signature (DVS) به‌طور مستقل ابتدا توسط K. Sako, M. Jakobsson, و R. Impagliazzo [۶] و بعداً توسط D. Chaum [۷] هر دو در ۱۹۹۶ معرفی شدند. همواره یک DVS، احراز اصالت یک پیام معین را به یک تصدیق‌کننده معین فراهم کرده و ویژگی بارز DVS این است که یک DVS معتبر می‌تواند توسط امضاءکننده «واقعی» یا توسط تصدیق‌کننده طراحی شده ایجاد شود با این ویژگی منحصر به فرد، یک DVS از یک امضای دیجیتال سنتی در دو جنبه متمایز است: (۱) تصدیق‌کننده طراحی شده متقاعد است که DVS توسط امضاءکننده واقعی ایجاد می‌شود نه توسط خود تصدیق‌کننده. هر چند امضای دیجیتال سنتی می‌تواند توسط هر تصدیق‌کننده‌ای برای DVS تصدیق شود بدون کمک بخش سوومی که همواره می‌تواند امضاکننده واقعی DVS را حتی با شناسایی کلید خصوصی تعیین کند. (۲) یک DVS احراز اصالت یک پیام معین را بدون هیچ ویژگی انکارامضای دیجیتال سنتی فراهم می‌کند. البته یک DVS می‌تواند امضای دیجیتال سنتی را در اکثر کاربردهای اساسی جایگزین کرده و خدماتی با توانایی انکارپذیری فراهم نماید.

در طرح K. Sako, M. Jakobsson, و R. Impagliazzo [۶] یک DVS بر اساس یک طرح امضای انکارناپذیر نامتقابل با یک الزام محدود پیشنهاد شده است اما این طرح به‌طور محاسباتی کامل نمی‌باشد. در ۲۰۰۳، S. Kremer, S. Saeednia, و O. Markowitch [۸] یک طرح DVS بر اساس لگاریتم گسسته مبتنی ترکیب امضای اچنور (Schnorr [۹]) و امضای Zheng [۱۰] پیشنهاد کردند. البته اخیراً طرح‌های DVS بر اساس هر دو رویه پیشنهاد می‌شوند. UDVS (DVS جامع) یک امضای دیجیتال متداول با عاملیت اضافی بوده که اجازه می‌دهد یک امضای دیجیتال به انتخاب امضاء درون DVS هر تصدیق‌کننده میسر شود. ساختار یک طرح UDVS، (DVSBM) بر اساس یک طرح دو سویه است. سه ساختار جدید UDVS بر اساس امضای Schnorr [۹] و RSA [۲] در طرح J. Pieprzyk و H. Wang, R. Steinfeld, و [۱۱] پیشنهاد شده است. همچنین UDVS بر اساس امضای الجمال در طرح D. و F. Laguillaumie و Vergnaud [۱۲] پیشنهاد گردید.

سه هویت مستقل در هر کاربرد UDVS وجود دارد: (۱) مرکز صدور گواهی CA، (۲) مالک امضای دیجیتال، (۳) تصدیق‌کننده طراحی شده. در یک UDVS، مالک به تبدیل کردن امضای دیجیتال درون یک DVS نامتقابل (بدون فعل و انفعال) به منظور اعتبار دهی یک پیام نیاز دارد. همچنین یک گواهی‌نامه دیجیتال به همراه یک تصدیق‌کننده به منظور اثبات کردن تصدیق گواهی‌نامه دیجیتال نیاز بوده که توسط تصدیق‌کننده احراز اصالت می‌شوند.

طرح پیشنهادی ما بر اساس طرح پیشنهادی A. Shamir [۲۳] مبتنی بر ID و با کاربرد مسئله لگاریتم گسسته (DL) و فرض دفی-هلمن (DHA) پایه‌ریزی شده است؛ در الگوریتم‌های رمزنگاری بر اساس ID هر کاربرد به ثبت در یک مولد کلید خصوصی (PKG) و تشخیص هویت خودش قبل از پیوستن به شبکه نیاز دارد به همین منظور یک کلید خصوصی برای کاربر ایجاد کرده و شناسه هویت کاربر (به‌طور مثال نام کاربری یا آدرس ایمیل) متناظر کلید عمومی خواهد بود. همچنین در این روش یک کاربر فقط به شناخت «شناسه هویت» شریک ارتباطی‌اش و کلید عمومی (PKG) نیاز دارد. هر چند در یک الگوریتم رمزنگاری بر اساس ID فرض می‌شود که هر کاربر شناسه هویت شریک ارتباطی‌اش را بشناسد؛ اما بر اساس این فرض

هیچ یک از روش‌های عملی به اعتباردهی شناسه هویت نیازی ندارند. این یکی از مزیت‌های اصلی رمزنگاری بر اساس ID می‌باشد. اطلاعات عمومی GDC از قبیل شناسه هویت کاربر می‌تواند منتقل شود و توسط هر هویت ارتباطی بررسی شود همچنین از این اطلاعات برای اعتباردهی یکدیگر نیز استفاده می‌شود؛ از کاربردهای دیگر طرح پیشنهادی مبتنی PKI به کارگیری در حوزه اینترنت و تجارت الکترونیک می‌باشد که در آن هویت‌های ارتباطی به شناختن ارتباطات قبلی یکدیگر نیاز ندارند که راه‌حل پیشنهادی ما در این حوزه مبتنی امنیت پیشرو، ترکیب طرح امضای دیجیتال متداول و طرح تعمیم‌یافته فرض دفی-هلمن می‌باشد که علاوه بر این می‌توان در طرح پیشنهادی از سیستم رمزنگاری نامتقارن به همراه سیستم DVS و گواهی دیجیتال نیز بهره برد.

### ۳ پروتکل پیشنهادی بر اساس لگاریتم گسسته (DL)

#### ۱.۳ مقدمه

یک تصدیق (گواهی‌نامه) کاغذی می‌تواند به عنوان یک عملگر احراز اصالت کاربر به کار برده شود. اما یک تصدیق دیجیتال کلید عمومی نمی‌تواند به عنوان یک عملگر احراز اصالت در کاربردهای شبکه به کار برده شود؛ برای این که یک تصدیق چاپی نمی‌تواند به آسانی جعل یا کپی شود. اما یک تصدیق دیجیتال کلید عمومی می‌تواند به آسانی ثبت شده و شروع مجدد گردد.

در طرح پیشنهادی مالک تصدیق دیجیتال تعمیم‌یافته GDC اصلاً به آشکارسازی متن اصلی امضای دیجیتال GDC برای تصدیق‌کننده نیاز ندارد؛ در عوض مالک GDC فقط برای تصدیق امضای دیجیتال به احراز اصالت بر اساس چالش / پاسخ نیاز دارد و تصدیق امضای دیجیتال روی GDC می‌تواند احراز اصالت کاربر را نیز فراهم کند. پروتکل پیشنهادی برای تصدیق امضای دیجیتال بر اساس مسئله لگاریتم گسسته (DL) و فرض دفی-هلمن (DHA) پایه‌ریزی شده و همچنین باید برای احراز اصالت کاربر نیازمندی‌های امن زیر را ایفا نماید.

(۱) Unforgeability (غیرقابل جعل بودن): یک پاسخ معتبر می‌تواند فقط توسط مالکیت تصدیق ایجاد شود. (کسی که امضای دیجیتال GDC می‌شناسد).

(۲) One-Wayness (روش مرسوم تابع درهم‌ساز و الحاق): هیچ شخص سوومی نمی‌تواند تصدیق امضای دیجیتال را بر اساس روش فعل و انفعال (برهم‌کنش) به دست آورد؛ زیرا معکوس تابع درهم‌ساز غیرعملی است.

(۳) Nontransferrability (غیرقابل انتقال‌پذیری): در احراز اصالت بر اساس (چالش/پاسخ) یک پاسخ به چالش تصدیق‌کننده را نمی‌توان در پاسخ انتقال یافته دیگری به چالش دیگر تصدیق‌کننده به کار برد؛ چون در غیر این صورت زمینه جعل هویت کاربر ایجاد می‌شود.

### ۲.۳ بررسی امضای دیجیتال الجمال

در طرح الجمال [۳] یک عدد اول بزرگ  $p$  و یک مولد  $g$  از مرتبه  $p - 1$  برای تسهیم همه کاربرها فرض می‌شود و امضاءکننده یک کلید خصوصی تصادفی  $x \in [1, p-2]$  انتخاب کرده و کلید عمومی متناظر  $y = g^x \bmod p$  را محاسبه می‌کند. پس از آن امضاءکننده به طور تصادفی یک پارامتر محرمانه  $k \in [1, p-1]$  را با فرض  $\gcd(k, p-1) = 1$  انتخاب کرده و  $r = g^k \bmod p$  محاسبه می‌کند، سپس با شناسایی امضای محرمانه  $s$ ، کلید خصوصی  $x$  و پارامتر  $k$  چکیده پیام  $m = ks + rx \bmod p - 1$  محاسبه می‌شود و به دنبال آن پیام  $m'$  نیز محاسبه می‌شود. سپس  $(r, s)$  به عنوان امضای دیجیتال پیام  $m'$  تعریف شده و امضای  $(r, s)$  می‌تواند تصدیق شود با بررسی این که آیا معادله  $g^m = y^r r^s \bmod p$  (۲) صحیح می‌باشد. در یک طرح امضای الجمال، پارامتر  $r$  امضاء می‌تواند آفلاین به صورت  $r = g^k \bmod p$  محاسبه شده و همچنین مؤلفه  $s$  امضاء به صورت آفلاین محاسبه می‌شود در نتیجه برای همه طرح‌های امضاء بر اساس مسئله لگاریتم گسسته DL معادله تعمیم یافته امضاءکننده را می‌توان به عنوان  $ax = bk + c \bmod p - 1$  محاسبه کرد جایی که  $(a, b, c)$  سه پارامتر از مجموعه مقادیر  $(m, r, s)$  بوده و به طور واضح هر پارامتر می‌تواند یک ترکیب ریاضیاتی  $(m, r, s)$  باشد. برای مثال پارامتر  $a$  می‌تواند با  $m, r, s$  جایگزین شود در نتیجه معادله تصدیق به صورت  $y^a = r^b g^c \bmod p$  تعیین خواهد شد.

### ۳.۳ فرض دفی-هلمن (DHA) Diffie-Hellman Assumption

به فرض دو شخص A و B به ترتیب کلید خصوصی  $x_A$  و  $x_B$  و متناظر آن‌ها کلیدهای عمومی  $y_A = g^{x_A} \bmod p$  و  $y_B = g^{x_B} \bmod p$  را در اختیار داشته باشند؛ جایی که  $p$  یک عدد اول صحیح بزرگ و  $g$  یک عضو اول گروه جمعی به پیمانه  $p$  باشد. آن‌گاه فقط شخص A و B می‌توانند یک تسهیم محرمانه  $K_{A,B} = y_B^{x_A} = y_A^{x_B} = K_{B,A} \bmod p$  را محاسبه کنند. فرض دفی-هلمن [۱] DHA به فرضی رجوع می‌کند که به طور محاسباتی برای تعیین  $K_{A,B}$  بدون شناختن کلید خصوصی  $x_A$  یا  $x_B$  غیر عملی خواهد بود. زیرا سختی حل کردن مسئله کلید خصوصی  $x_A$  یا  $x_B$  از کلید عمومی متناظر  $y_A$  یا  $y_B$  به سختی حل مسئله لگاریتم گسسته وابسته می‌باشد.

#### ۱.۳.۳ پروتکل برقراری کلید و احراز اصالت کاربر

(۱) ثبت در CA: به فرض A مالک تصدیق و B تصدیق‌کننده باشد. شخص A به ثبت شدن در یک مرکز صدورگواهینامه CA برای بدست آوردن یک GDC نیاز دارد. CA یک امضای الجمال  $(r_A, s_A)$  را برای دستور A کاربر  $m'_A$  بر اساس معادله (۱) ایجاد کرده و  $m_A$  چکیده پیام عبارت (دستور)  $m'_A$  می‌باشد. از آن جایی که مؤلفه  $r_A$  امضاء یک عدد صحیح تصادفی بوده و به  $m_A$  وابسته نمی‌باشد پس به نگهداری محرمانه نیاز ندارد. هر چند مؤلفه  $s_A$  امضاء یک تابع دستوری بوده و هر مالک به نگهداری محرمانه آن از تصدیق‌کننده در فرآیند احراز اصالت نیاز دارد. احراز اصالت کاربر و پروتکل برقراری کلید در شکل ۱ نشان داده می‌شود.



۲) پروتکل: پروتکل احراز اصالت و برقراری کلید شامل ۴ مرحله است:

۱. کاربر A اطلاعات کاربریش  $m'_A$  و پارامترهای  $(r_A, S_A)$  را به تصدیق کننده B انتقال می‌دهد  
جائی که  $S_A = r_A^{s_A} \bmod p$ .

۲. تصدیق کننده بعد از دریافت  $m'_A$  و  $(r_A, S_A)$  بررسی می‌کند که آیا  $g^{m'_A} = y^{r_A} S_A \bmod p$  صحیح می‌باشد. جائی که  $y$  کلید عمومی CA می‌باشد. اگر این برابری، صحیح حفظ شود ابتدا تصدیق کننده B به‌طور تصادفی یک عدد صحیح  $v_B \in [1, p-2]$  انتخاب می‌کند، سپس یک چالش  $c_B = r_A^{v_B} \bmod p$  محاسبه کرده و  $c_B$  را به کاربر A ارسال می‌کند؛ در غیر این صورت احراز اصالت کاربر شکست خورده و پروتکل متوقف می‌شود.

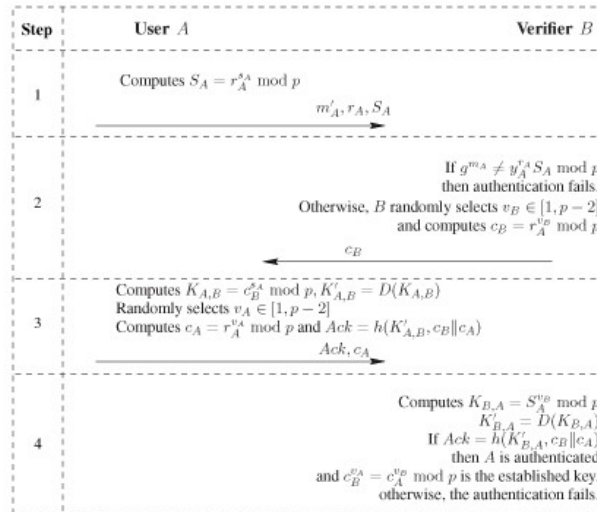
۳. کاربر A ابتدا  $s_A$  محرمانه‌اش را برای محاسبه کلید محرمانه دفی-هلمن  $K_{A,B} = c_B^{s_A} \bmod p$  و  $p$  و  $K'_{A,B} = D(K_{A,B})$  به کار می‌گیرد جائی که  $D(K_{A,B})$  یک روند استخراج کلید با  $K_{A,B}$  به‌عنوان یک ورودی ارائه می‌دهد. سپس کاربر A به‌طور تصادفی یک عدد صحیح  $v_A \in [1, p-2]$  انتخاب می‌کند و  $c_A = r_A^{v_A} \bmod p$  محاسبه کرده و  $Ack = h(K'_{A,B}, c_B || c_A)$  پاسخ می‌دهد جائی که  $h(K'_{A,B}, c_B || c_A)$  یک روش تابع کلید هش شده تحت کلید  $K'_{A,B}$  ارائه می‌دهد. کاربر A،  $Ack$  و  $c_A$  را در برگشت به B ارسال می‌کند.

۴. تصدیق کننده B بعد از دریافت کردن  $Ack$  و  $c_A$  از کاربر A،  $v_B$  محرمانه‌اش را برای محاسبه کلید محرمانه تسهیم شده دفی-هلمن  $K_{B,A} = S_A^{v_B} \bmod p$  و  $K'_{B,A} = D(K_{B,A})$  به کار گرفته و بررسی می‌کند که آیا  $Ack = h(K'_{B,A}, c_B || c_A)$  صحیح است. اگر این تصدیق موفق باشد، مالک تصدیق A، توسط تصدیق کننده B احراز اصالت شده و یک کلید جلسه محرمانه یکبار مصرف  $c_B^{v_A} = r_A^{v_A v_B} = c_A^{v_B} \bmod p$  بین کاربر A و B تسهیم می‌شود. این کلید تسهیم شده می‌تواند امنیت پیشروی کامل را فراهم کند.

در پروتکل پیشنهادی مالک تصدیق، به منظور احراز اصالت موفق با تصدیق کننده به محاسبه و ارسال یک جفت معتبر  $(r_A, S_A)$  و  $Ack$  به تصدیق کننده درگام ۱ و ۳ نیاز دارد. پارامترهای  $(r_A, S_A)$  به تصدیق کردن  $g^{m'_A} = y^{r_A} S_A \bmod p$  نیاز دارند. این جفت عدد صحیح می‌تواند به آسانی توسط هرکسی محاسبه شود. هرچند نشان خواهیم داد که فقط مالک تصدیق A، مؤلفه محرمانه  $S_A$  را برای محاسبه یک معتبر  $Ack$  می‌شناسد؛ برای این که تصدیق کننده B می‌تواند کلید محرمانه یکبار مصرف  $K_{B,A}$  را به‌عنوان  $K_{B,A} = S_A^{v_B} \bmod p$  محاسبه کرده تا برای ایجاد  $Ack$  بکارگیرد.

بر اساس فرض دفی-هلمن DHA، مالک تصدیق A کسی است که مؤلفه محرمانه  $S_A$  را می‌شناسد و همچنین می‌تواند  $K_{A,B}$  را به عنوان  $K_{A,B} = c_B^{s_A} = r_A^{s_A v_B} = K_{B,A} \bmod p$  محاسبه کند بنابراین مالک تصدیق می‌تواند فعل و انفعال با تصدیق کننده داشته و با موفقیت احراز اصالت شود.





شکل ۱: پروتکل توافق کلید و احراز اصالت بر اساس DL

## ۴ طرح پیشنهادی

از آن جایی که احراز اصالت کاربر و برقراری کلید دو سرویس اساسی در ارتباطات امن می‌باشد از این‌رو ما طرحی بر اساس تصدیق دیجیتال کلید عمومی ID با پروتکل برقراری کلید با کاربرد GDC (تصدیق دیجیتال تعمیم‌یافته) را به همراه سیستم احراز اصالت کاربر مبتنی لگاریتم گسسته DL (با فرض دفی-هلمن) و پروتکل عامل‌یابی عدد صحیح (IF) برای برقراری و تسهیم کلید جلسه محرمانه پیشنهاد می‌کنیم که ویژگی‌های زیر را ایفا می‌کند:

۱. غیر قابل انکارپذیری (Non-Repudiation)
۲. غیر قابل انتقال‌پذیر (Nontransferrability)
۳. غیر قابل جعل‌پذیری (Unforgeability)
۴. استفاده از چکیده پیام و خروجی تابع درهم‌ساز برای امضاء: در تابع درهم‌ساز با ورودی معین  $a$  محاسبه  $h(a) = b$  آسان می‌باشد ولی با  $b$  معین، به آسانی نمی‌توان  $h^{-1}(b) = a$  را محاسبه کرد (معکوس تابع درهم‌ساز با عملگر معکوس اجراء نشدنی است).
۵. داده‌ها در فرم متن اصلی روی شبکه منتقل نمی‌شوند «گمنامی کاربر و پایداری در برابر حمله تحریف و دستکاری».

۶. پایداری در برابر تصادم و مقاوم به خطر کشف رمز اطلاعات ذخیره شده در کارت هوشمند توسط اخلال گر «مقاوم به حملات کانال جانبی».
۷. جدول تصدیق امضا درون سرور ذخیره نمی شود «سربرار سرور برای احراز اصالت کاهش می یابد». چون سرور فقط کلید محرمانه را نگهداری می کند.
۸. پشتیبانی از سیستم احراز اصالت متقابل (کاربر/ سرور) با توافق کلید جلسه تصدیق شده. توافق کلید می تواند از حمله خودی، حمله تکرار، حمله جلسه موازی، انعکاس، حمله شخص در وسط جلوگیری نماید؛ برای پایداری در برابر برخی حملات، اگر اندازه عدد تصادفی بزرگتر از کلید محرمانه باشد؛ بهتر است. پس به منظور نگهداری اطلاعات (کلید) محرمانه به عدد تصادفی نیاز است. اگر کلید محرمانه فاش شود آن گاه کلیدهای جلسه خطرکشف رمز دارند. حفظ گمنامی کاربر از ویژگی های بارز احراز اصالت متقابل به شمار می رود. در پروتکل پیشنهادی ترکیب یک عدد تصادفی "Nonce" با مهر زمانی و مقدار درهم ساز، از پیام احراز اصالت در برابر حمله موازی محافظت می نماید از کلید جلسه به منظور نگهداری اطلاعات محرمانه استفاده می شود. بنابراین طرح پیشنهادی در برابر حمله جلسه موازی امن است. فاش کلید محرمانه سرور خطر کشف رمز کلیدهای جلسه را در پی خواهد داشت. بکارگیری یک عدد تصادفی یا مسئله همزمانی (مهر زمانی)  $T' - T \leq \Delta T$  باعث می شود طرح در برابر حمله جعل و حمله تکرار مقاوم کند.
۹. به عنوان سامانه ای امن با ثبات عملیاتی بالا با کاربرد تصدیق گواهی نامه دیجیتال برای تبادل داده در تراکنش های بانکی، سیستم های پرداخت الکترونیکی، هویت الکترونیکی، سیستم های دفاعی و الکترونیکی، سیستم اتوماسیون اداری، در کارت های هوشمند و تراشه های الکترونیکی به کار می رود.
۱۰. هزینه محاسباتی و ارتباطی معقول و نحوه ذخیره سازی مؤثر «به دلیل کاربرد توابع درهم ساز و کارت هوشمند» هر چند کاربرد الگوریتم کلید نامتقارن سرعت بالایی ندارد برای این که در هر زمان محاسبات توان پیمانهای که جز عملگر پیچیدگی می باشد را شامل می کند.
۱۱. طرح پیشنهادی مبتنی هر دو مشخصه لگاریتم گسسته «روی میدان متناهی» و تابع درهم ساز امن می تواند بیشتر حملات آنلاین و آفلاین شناخته شده از قبیل: حمله تکرار، حمله کانال جانبی، حمله خارجی، حمله جعل امضاء، حمله حدس، حمله خودی، حمله تحریف و دستکاری پیامها و داده ها (حمله مبتنی بر پیام آشکار)، حمله جعل هویت، حمله جلسه موازی، حملات اخلال در سرویس، حمله فریب سرور و حمله فریب مرکز ثبت، حمله کارت هوشمند مسروقه، حمله کاربر مبدل شده، حمله سرور، حمله کلید معلوم، حمله لغت نامه ای، حمله یافتن کلید در نواحی آنتروپی بالا، حمله آزمایش و خطا روی سیستم های رمزنگاری، حمله بازیابی متن اصلی و حمله معکوس XOR را با هزینه محاسباتی معقول محدود نماید.

## ۱.۴ تحلیل امنیتی طرح پیشنهادی

تمام مکانیزم‌های رمزنگاری و گواهینامه دیجیتال و روش‌های قدرتمند احراز هویت، برای پیشگیری از دسترسی متجاوزین به حریم منابع سیستم و بهره‌برداری غیرمجاز از داده‌ها ابداع شده‌اند. اغلب این مکانیزم‌ها از لحاظ عملی غیرقابل نفوذ و مطمئن هستند ولی آیا این مکانیزم‌ها، امنیت صددرصد داده‌ها را تضمین می‌کنند؟ چگونه ممکن است که از پنجاه سال قبل تاکنون هنوز یک مورد ضعیف بنیادی در روش رمزنگاری [۲] RSA گزارش نشده ولی در هر روز ده‌ها مورد از نفوذ در شبکه و وب سایت‌ها به گوش می‌رسد! شاید از خود پرسیم که پس این مکانیزم‌ها به چه کار می‌آیند؟ جواب بدیهی است: این مکانیزم‌ها لازمند ولی کافی نیستند! از این رو امنیت پروتکل پیشنهادی ما بر اساس ترکیب امن امضای RSA، به‌سختی محاسبه لگاریتم گسسته، پایداری تصادم یک روش تابع درهم‌ساز (برای نگهداری کلید محرمانه) و GDHA تکیه می‌کند. همچنین مسئله لگاریتم گسسته هنوز یک مسئله باز است و خیلی امن‌تر از روش تابع درهم‌ساز پیشنهاد می‌شود؛ هر چند به دست آوردن معکوس تابع درهم‌ساز هم غیرعملی بوده و می‌توان از آن به عنوان ابزاری برای نگهداری کلید محرمانه (در سرور) در برابر حمله‌های شناخته شده استفاده نمود. البته می‌توان استفاده از توافق کلید دفی-هلمن [۱] را نیز در شبکه‌های ناامن توصیه کرد؛ از این رو سیستم رمزنگاری طرح پیشنهادی ما مبتنی بر دو مشخصه مسئله لگاریتم گسسته «روی میدان متناهی» و امنیت یک روش تابع درهم‌ساز، می‌تواند اکثر حمله‌های شناخته شده از قبیل: حمله تکرار، حمله کانال جانبی، حمله خارجی، حمله جعل امضاء، حمله حدس، حمله خودی، حمله تحریف و دستکاری پیام‌ها و داده‌ها (حمله مبتنی بر پیام آشکار)، حمله جعل هویت، حمله جلسه موازی، حملات اخلاص در سرور، حمله فریب سرور و حمله فریب مرکز ثبت، حمله کارت هوشمند مسروقه، حمله کاربر مبدل شده، حمله سرور، حمله کلید معلوم، حمله لغت‌نامه‌ای، حمله یافتن کلید در نواحی آنتروپی بالا، حمله آزمایش و خطا روی سیستم‌های رمزنگاری، حمله بازیابی متن اصلی و حمله معکوس XOR را با هزینه محاسباتی معقول محدود نماید. البته حمله‌های حدس آنلاین را نیز می‌توان به آسانی با محدود کردن تعداد ورود به سیستم مردود شده، جلوگیری کرد. از این رو با توجه به تحلیل و مقایسه عملکرد طرح‌های مرتبط و بررسی حفره‌های آسیب‌پذیری آن‌ها، می‌توان امنیت بالا، هزینه ارتباطی پایین و پایداری به انواع حمله‌های آسیب‌پذیر را برای این طرح پیشنهادی وعده داد.

### ۱.۱.۴ حملات به امضای الکترونیک

رایوست، حملات ممکن در مورد امضای الکترونیک را بر اساس اطلاعاتی که مهاجم در اختیار دارد؛ به دو دسته کلی تقسیم نموده است.

۱. حملات کلید (Key-Only Attack): حملاتی که در آن‌ها مهاجم تنها از کلید عمومی صاحب امضا با خبر است و در واقع تنها می‌تواند صحت یک امضای الکترونیک را کنترل کند.
۲. حملات مبتنی بر پیام (Message Attack): حملاتی که در آن‌ها مهاجم علاوه بر کلید عمومی صاحب امضا، نمونه‌هایی از متن‌های عادی و معادل امضاء شده آن را نیز در اختیار دارد.

هریک از این قسم حملات ممکن است به شکست سیستم امضای الکترونیک منتهی شود؛ شکست یک سیستم امضای الکترونیک دارای تعابیر مختلفی است.

۱. شکست کامل (Total Break): شکست کامل به معنای آن است که کلید خصوصی امضاء کننده کاملاً فاش شود.

۲. جعل عمومی (Universal Forgery): جعل عمومی از طریقی محقق می‌گردد که در آن مهاجم از کلید خصوصی بی‌خبر است اما می‌تواند هر پیام دلخواه را بصورت معتبر از سوی صاحب اصلی امضاء کند.

۳. جعل انتخابی (Selective Forgery): جعل انتخابی به معنای آن است که مهاجم می‌تواند تنها مجموعه محدودی از پیام‌ها که از پیش تعیین شده را امضا کند.

۴. جعل وجودی (Existential Forgery): جعل وجودی بدین معنا است که مهاجم می‌تواند دست کم یک پیام را که از قبل قابل تعیین نیست به طور مؤققت آمیز و معتبر از طرف صاحب اصلی امضاء کند، از آن جاییکه در این روش مهاجم چندان کنترلی بر روی پیام‌های امضاء شده معتبر ندارد؛ احتمال آن که پیام امضاء شده‌ای که تولید می‌کند پیامی با مفهوم و معنادار باشد بسیار اندک است بنابراین این نوع از شکست‌ها عملاً دشواری به بار نمی‌آورند و چندان با اهمیت نیستند.

#### ۲.۱.۴ تحلیل امنیتی پروتکل استقرار کلید و احراز اصالت کاربر

در این بخش، ما امنیت پیشنهادی پروتکل استقرار کلید و احراز اصالت کاربر را به منظور توانایی غیرقابل جعل به همراه غیرقابل انتقال پذیری بر اساس یک روش تابع درهم‌ساز، مسئله لگاریتم گسسته و فرض دفی-هلمن تحلیل خواهیم کرد.

**توانایی غیرقابل جعل:** اخلاص گر به منظور اجرای یک حمله خارجی، به ارائه دادن یک جفت معتبر  $(r_A, S_A)$  درگام ۱ پروتکل و متناظر Ack درگام ۳ پروتکل برای جعل هویت موفق مالک تصدیق نیاز دارد. یک جفت معتبر  $(r_A, S_A)$  به‌تنهایی درگام ۱ نمی‌تواند برای احراز اصالت کردن مالکیت تصدیق بکاربرده شود؛ لذا این جفت پارامتر می‌تواند به آسانی توسط اخلاص گر از معادله ۳ به دست آید. اما به طور محاسباتی حل لگاریتم گسسته  $S_A$  توسط اخلاص گر غیر عملی بوده و همچنین طرح امضای الجمال امن می‌باشد. بنابراین از بُعد محاسباتی به‌دست آوردن جفت  $(r_A, S_A)$  توسط اخلاص گر برای تصدیق کردن در معادله مؤلفه محرمانه  $S_A$ ، توسط اخلاص گر محاسبه  $K(A, B)$  و جعل کردن یک Ack معتبر در مرحله ۳ غیر عملی خواهد بود؛ از طرفی دیگر مالک تصدیق، مؤلفه محرمانه  $S_A$  را از  $C_A$  در طول مرحله ثبت به دست آورده و می‌تواند با مؤققت در مرحله ۳ احراز اصالت شود. بنابراین امنیت توانایی غیرقابل جعل پروتکل پیشنهادی از طریق ترکیب امنیت طرح امضای الجمال و فرض دفی-هلمن [۱] DHA تأمین می‌شود. پس احراز اصالت پیشنهادی کاربر و پروتکل برقراری کلید در مقابل حملات خارجی امن خواهد بود.

**One-Wayness (روش الحاق (فشرده‌گی)):** درگام ۱ مالک تصدیق،  $S_A$  را به تصدیق‌کننده ارائه می‌دهد. محاسبه  $S_A$  محرمانه از  $S_A$  غیرعملی است زیرا نیاز به حل مسئله لگاریتم گسسته دارد. همچنین مالک تصدیق در مرحله ۳،  $S_A$  محرمانه را برای محاسبه کلید دفی-هلمن  $K(A, B)$  به کار می‌گیرد و علی‌رغم این که تصدیق‌کننده کلید دفی-هلمن  $K(A, B)$  را می‌شناسد؛ اما این روند به فرض دفی-هلمن DHA ختم می‌شود و تصدیق‌کننده نمی‌تواند  $S_A$  محرمانه را به دست آورد.

**غیرقابل انتقال‌پذیری:** با توجه به فرض دفی-هلمن [۱] DHA، یک پاسخ معتبر Ack فقط می‌تواند توسط یک مالک تصدیق ایجاد شود که او مؤلفه محرمانه  $S_A$  امضای دیجیتال از قبیل  $r_A^{S_A} = S_A \bmod p$  و یا عدد تصادفی محرمانه یک چالش تصادفی انتخابی توسط تصدیق‌کننده را می‌شناسد. نظر باینکه هربار تصدیق‌کننده یک چالش تصادفی انتخاب می‌کند؛ پاسخ فقط برای احراز اصالت یکبار مصرف معتبر خواهد بود.

از آن جایی که اصلاً امضای دیجیتال GDC به تصدیق‌کننده صادر (انتقال) نمی‌شود؛ لذا تصدیق‌کننده نمی‌تواند GDC کامل را به هر قسمت سوومی انتقال دهد؛ از این‌رو نگرانی به دستیابی کلید خصوصی در پروتکل پیشنهادی وجود ندارد. پس یک پاسخ معتبر Ack نمی‌تواند درون یک پاسخ چالش تصدیق‌کننده دیگر انتقال یافته شود. پروتکل پیشنهادی قادر است یک مالک تصدیق را احراز اصالت کرده و همچنین دو کلید محرمانه تسهیم شده یکبار مصرف  $K(A, B)$  و  $C_B^{vA} = r_A^{vAvB} = C_A^{vB} \bmod p$  را بین کاربر A و مالک تصدیق برقرار کند. شخصی که  $S_A$  و به دنبال آن  $r_A^{S_A} = S_A \bmod p$  و تصدیق‌کننده B را از طریق پروتکل احراز اصالت بشناسد می‌تواند طی مراحل کلید محرمانه تسهیم شده بین A و B برقرار نماید و علاوه بر این می‌تواند مالکیت را به ارسال یک تصدیق Ack به تصدیق‌کننده قادر سازد؛ از آن جایی که کلید تسهیم شده محرمانه دفی-هلمن می‌تواند توسط هر یک از کاربرهای A یا B ایجاد شود از این‌رو مالک تصدیق A می‌تواند تسهیم‌کننده در پروتکل را انکار کند.

**نکته ۱:** در فرض دفی-هلمن DHA، فرض کردیم که مولد  $g$  یک عضو اول گروه ضربی به پیمانه  $p$  است تا زمانی که پارامتر  $r_A = g^k \bmod p$  در قضیه ۱ لزوماً یک مولد نباشد. هر چند ما می‌توانیم مطمئن شویم که  $r_A$  یک عضو اول گروه ضربی به پیمانه  $p$  توسط استلزام  $\gcd(k, p-1) = 1$  بوده؛ به خصوص وقتی  $p = 2p' + 1$  یک عدد اول امن باشد درجایی که  $p'$  هم یک عدد اول است ما می‌توانیم مطمئن شویم  $r_A$  یک عضو اول گروه ضربی به پیمانه  $p$  است اگر  $K$  یک عدد فرد باشد.

**نکته ۲:** به‌طور مشابه بر اساس الگوریتم‌های رمزنگاری مبتنی بر ID، پروتکل پیشنهادی مشکل ابطال کلید دارد؛ البته CA کلید جلسه محرمانه یکبار مصرف تسهیم شده بین کاربرها را می‌شناسد. بعضی الگوریتم‌های رمزنگاری برای حل کردن مسئله ابطال کلید، امضاء بر اساس ID، (IBS) پیشنهاد کرده‌اند از قبیل امضای دیجیتال با تصدیق کمتر (CDS).

## ۵ پروتکل بر اساس IF (عدد صحیح)

در این بخش، ما یک پروتکل استقرار کلید و احراز اصالت کاربر بر اساس IF پیشنهاد می‌کنیم که ترکیبی از یک امضای دیجیتال آفلاین / آنلاین بوده و فرض دفی-هلمن (GDHA) را ایجاد می‌کند.

### ۱.۵ بررسی امضای دیجیتال آفلاین / آنلاین

در این قسمت خانواده تابع درهم‌ساز درجه و طرح امضای آفلاین / آنلاین را بررسی خواهیم کرد. یک خانواده درهم‌ساز درجه شامل یک جفت  $(L, H)$  است؛ جایی که  $L$  یک الگوریتم مولد کلید زمان چند جمله‌ای احتمالی و  $H$  یک خانواده درهم‌ساز تصادفی بوده که  $L$  یک جفت کلید  $(HK, TK)$  ایجاد می‌کند، به طوری که  $HK$  یک کلید درهم‌ساز (عمومی) و  $TK$  کلید درجه (خصوصی) وابسته به آن می‌باشد. یک تابع درهم‌ساز درجه تحت عنوان  $h_{HK}(m, s)$  با محرمانگی کلید خصوصی فرض می‌شود جایی که  $m$  یک پیام و  $s$  یک عدد تصادفی معین خواهد بود. یک تابع درهم‌ساز درجه باید سه نیازمندی زیر را ایفا کند:

- **بهره‌وری (راندمان):** تعیین یک کلید درهم‌ساز  $HK$  و یک جفت  $(m, s)$ ،  $h_{HK}(m, s)$  که در زمان چند جمله‌ای قابل محاسبه است.
- **پایداری در برابر تصادم:** الگوریتم زمان چند جمله‌ای احتمالی  $A$ ، در ورودی کلید درهم‌ساز (عمومی)  $HK$  وجود ندارد که بتواند دو جفت  $(m_1, s_1)$  و  $(m_2, s_2)$  را ایجاد کند به طوری که بدون چشم پوشی  $m_1 \neq m_2$  و  $h_{HK}(m_1, s_1) = h_{HK}(m_2, s_2)$ .
- **تصادم درجه:** تعیین جفت‌های  $(HK, TK)$  و  $(m_1, s_1)$  و یک پیام اضافی  $m_2$ ، با احتمال الگوریتم زمان چند جمله‌ای  $s_2$  ایجاد می‌شود به طوری که  $h_{HK}(m_1, s_1) = h_{HK}(m_2, s_2)$ . اگر  $s_1$  به طور یکنواخت در  $S$  توزیع شود آن گاه توزیع  $s_2$  به طور محاسباتی غیر قابل تشخیص از توزیع یکنواخت در  $S$  می‌باشد.

### ۲.۵ تابع درهم‌ساز درجه بر اساس عامل‌یابی

با انتخاب تصادفی دو عدد اول امن  $p$  و  $q$  (به طوری که  $q' = \frac{q-1}{2}$  و  $p' = \frac{p-1}{2}$  عددهای اول باشند)  $n = pq$  محاسبه می‌شود و همچنین با انتخاب تصادفی یک عضو  $g$  از مرتبه  $\lambda(n)$ ، جایی که  $\lambda(n) = \text{lcm}(p-1, q-1)$  محاسبه شده و کلید درهم‌ساز عمومی  $HK$  برابر  $(n, g)$  و کلید درجه خصوصی  $TK$  برابر  $(p, q)$  خواهد بود. تابع درهم‌ساز درجه  $h_{HK}(m, s)$  تعریف می‌شود به عنوان:  $h_{HK}(m, s) = g^{m||s} \pmod{n}$  که عملگر الحاق را نشان می‌دهد.

لذا برای این که نشان دهیم  $h_{HK}(m, s)$  یک تابع درهم‌ساز درجه تحت فرض عامل‌یابی می‌باشد نیاز داریم نشان دهیم که آن سه مشخصه اصلی یک تابع درهم‌ساز درجه را تکمیل کرده و همچنین برای محاسبه یک تصادم درجه به جفت‌های معین  $(HK, TK)$ ،  $(m_1, s_1)$  و یک پیام اضافی  $m_2$ ، نیاز داریم، در ادامه  $s_2$  محاسبه می‌شود به طوری که  $h_{HK}(m_1, s_1) = h_{HK}(m_2, s_2)$ . بر اساس معادله ۴ باید  $g^{m_1||s_1} =$



$2^K m_1 + s_1 = 2^K m_2 + s_2 \pmod{n}$  به دست آید و  $s_2$  ای یافت شود چنان که در معادله  $\lambda(n)$  صدق کند جایی که  $K$  اندازه پارامتر معین  $s$  می باشد. کلید درجه معین  $TK = (p, q)$  و  $\lambda(n)$  می تواند با تابع زمان چند جمله ای محاسبه شوند و همچنین  $s_2$  می تواند در زمان چند جمله ای با حل کردن معادله خطی  $s_2 = 2^K(m_1 - m_2) + s_1 \pmod{\lambda(n)}$  محاسبه شود.

### ۳.۵ طرح امضاء

به طور اساسی هر طرح امضای دیجیتال معین با یک خانواده درهم ساز درجه  $(L, H)$  می تواند در یک طرح امضای آنلاین / آفلاین تعریف شود و در مرحله امضای آفلاین، یک امضاء کننده مقدار درهم سازی را به قصد انجام یک پیام انتخاب شده دلخواه تولید می کند. اما در مرحله آنلاین، امضاء کننده برای یک پیام معین، یک تصادم درهم ساز درجه را با مقدار درهم سازی محاسبه شده قبلی می یابد. نقطه تصادم و امضای ایجاد شده در مرحله آفلاین می تواند به عنوان امضاء برای پیام ایجاد شده در مرحله آنلاین ارائه شود با فرض این که  $h_{HK}(m, s)$  به عنوان تابع درهم ساز درجه،  $HK$  کلید درهم ساز،  $TK$  کلید درجه،  $VK$  کلید تصدیق و  $SK$  کلید امضاء کننده برای هر طرح امضای دیجیتال معین نشان داده می شود؛ در بخش زیر طرح امضای آفلاین / آنلاین تشریح می کنیم:

- الگوریتم ایجاد کلید GEN: یک جفت  $(SK, VK)$  با بکار بردن الگوریتم ایجاد کلید عمومی و یک جفت  $(HK, TK)$  با بکار بردن الگوریتم  $L$  ایجاد می شوند. کلید امضاء کننده  $(SK, HK, TK)$  و کلید تصدیق  $(VK, HK)$  می باشد.
- الگوریتم امضاء کننده SIGN: یک کلید امضاء کننده  $(SK, HK, TK)$  تعیین می شود. الگوریتم امضاء کننده عمل می کند به عنوان زیر:

- مرحله آفلاین: امضاء کننده به طور تصادفی  $(m, s)$  انتخاب کرده و  $h_{HK}(m, s)$  محاسبه می کند. سپس کلید محرمانه  $SK$  را برای امضای  $h_{HK}(m, s)$  به کار گرفته و  $S_{SK}(h_{HK}(m, s)) < s, m$  امضاء کننده می آورد. امضاء کننده  $S_{SK}(h_{HK}(m, s))$  را به طور اختیاری از  $h_{HK}(m, s)$  برای محاسبه مجدد در طول مرحله آنلاین اجتناب می کند.

- مرحله آنلاین: با فرض یک پیام معین  $m'$ ، امضاء کننده یک تصادم درهم ساز درجه را برای  $(m, s)$  می یابد چنان که  $h_{HK}(m', s') = h_{HK}(m, s)$  امضای پیام  $m'$  به عنوان  $< S_{SK}(h_{HK}(m, s)), s', h_{HK}(m, s) >$  تعریف می شود.

الگوریتم تصدیق VERF: ابتدا  $< S_{SK}(h_{HK}(m, s)) >$  را با به کارگیری  $VK$  و  $h_{HK}(m, s)$  بررسی کرده و سپس  $h_{HK}(m', s')$  محاسبه کرده برای بررسی این که  $h_{HK}(m, s) = h_{HK}(m', s')$



## ۴.۵ فرض دفی-هلمن تعمیم یافته (GDHA)

فرض کنید کاربر A و B کلیدهای خصوصی  $x_A$  و  $x_B$  و متناظر آنها به ترتیب کلیدهای عمومی  $y_A = g^{x_A} \bmod n$  و  $y_B = g^{x_B} \bmod n$  را در اختیار دارند. حال اگر  $n = pq$ ، جایی که  $p$  و  $q$  دو عدد اول بزرگ باشند، آن گاه فرض می‌کنیم که فقط A و B می‌توانند یک محرمانگی تسهیم شده  $K_{A,B} = y_A^{x_B} = y_B^{x_A} \bmod n$  را محاسبه کنند.

در حقیقت GDHA رجوع می‌کند به فرضیه‌ای که به طور محاسباتی برای تعیین کردن  $K(A, B)$  بدون شناختن کلید خصوصی  $x_A$  یا  $x_B$  غیر عملی خواهد بود.

## ۵.۵ پروتکل احراز اصالت کاربر و برقراری کلید

(۱) ثبت در CA: به فرض A مالکیت تصدیق و B تصدیق کننده باشد. A به ثبت کردن در CA برای به دست آوردن یک GDC نیاز دارد. CA یک امضای دیجیتال آنلاین/ آفلاین  $(S_{SK}(h_{HK}(m', s')), S_A, h_{HK}(m', s'))$ ، برای دستور A کاربر  $m_A$  ایجاد می‌کند؛ در پروتکل احراز اصالت هر مالکیت به نگهداری امضای محرمانه  $s_A$  از تصدیق کننده نیاز دارد تا زمانی که تصدیق مؤلفه محرمانه به تصدیق کننده اثبات شود. مالکیت، مؤلفه محرمانه را به تصدیق کننده در طول مرحله احراز اصالت مطابق فرضیه GDHA پنهان می‌کند. احراز اصالت کاربر و پروتکل برقراری کلید در شکل ۲ نشان داده می‌شود.

(۲) پروتکل: پروتکل برقراری کلید و احراز اصالت شامل ۴ مرحله زیر می‌باشد:

۱. کاربر A اطلاعات کاربری اش  $m_A$  و پارامترهای  $(S_{SK}(h_{HK}(m', s')), S_A, h_{HK}(m', s'))$  را به تصدیق کننده B، تحت رابطه  $S_A = g^{s_A} \bmod n$  انتقال می‌دهد.

۲. بعد از دریافت  $m_A$  و  $(S_{SK}(h_{HK}(m', s')), S_A, h_{HK}(m', s'))$ ، تصدیق کننده B ابتدا بررسی می‌کند که آیا  $(S_{SK}(h_{HK}(m', s')), S_A, h_{HK}(m', s'))$  امضای  $h(m', s')$  با کاربرد  $VK$  است. سپس  $h_{HK}(m_A, S_A) = g^{K m_A} S_A \bmod n$  را محاسبه کرده و بررسی می‌کند که آیا رابطه  $h_{HK}(m_A, S_A) = h_H K(m', s')$  برقرار است، جایی که  $K$  مؤلفه محرمانه  $s_A$  می‌باشد. اگر این برابری صحیح نگه داشته شود؛ تصدیق کننده B ابتدا به طور تصادفی یک عدد صحیح  $v_B \in [1, n-1]$  انتخاب می‌کند، سپس  $c_B = g^{v_B} \bmod n$  محاسبه کرده و  $c_B$  را به کاربر A ارسال می‌کند؛ در غیر این صورت، احراز اصالت کاربر شکست خورده و پروتکل متوقف می‌شود.

۳. ابتدا کاربر A،  $s_A$  محرمانه اش را برای محاسبه کلید محرمانه دفی-هلمن  $k(A, B) = C_B^{s_A} \bmod n$  و  $K'_{A,B} = D(K_{A,B})$  به کار می‌گیرد. سپس کاربر A به طور تصادفی عدد صحیح  $v_A \in [1, n-1]$  انتخاب می‌کند و  $c_A = g^{v_A} \bmod n$  محاسبه کرده و

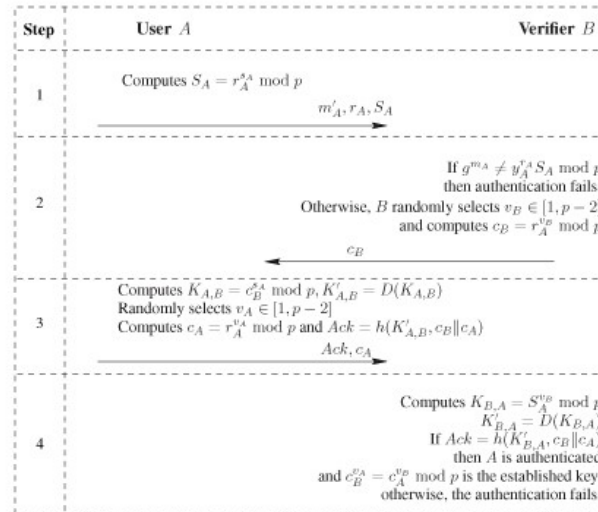
$Ack = h(K'_{A,B}, c_B || c_A)$  پاسخ می‌دهد جایی که  $D(K_{A,B})$  یک روند استخراج کلید تحت  $K_{A,B}$  را به عنوان یک ورودی و  $h(K_{A,B}', c_B || c_A)$  و یک روش تابع درهم‌ساز کلید شده تحت کلید  $K'_{A,B}$  ارائه می‌دهد. کاربر  $A$ ،  $Ack$  و  $c_A$  را در برگشت به  $B$  ارسال می‌کند.

۴. بعد از دریافت  $Ack$  و  $c_A$  از کاربر  $A$ ، تصدیق‌کننده  $B$ ،  $v_B$  محرمانه‌اش را برای محاسبه کلید محرمانه تسهیم شده دخی-هلمن  $n$   $K_{B,A} = S_A^{v_B} \text{ mod } n$  و  $K'_{B,A} = D(K_{A,B})$  به کار گرفته و بررسی می‌کند که آیا  $Ack = h(K'_{A,B}, c_B || c_A)$  صحیح است. اگر این تصدیق موفق باشد مالکیت تصدیق  $A$  توسط تصدیق‌کننده  $B$  احراز اصالت شده و یک کلید جلسه محرمانه یکبار مصرف  $n$   $c_B^{v_A} = g^{v_A v_B} = c_A^{v_B} \text{ mod } n$  بین  $A$  و  $B$  تسهیم خواهد شد. این کلید می‌تواند امنیت کامل پیشرو را فراهم نماید؛ به منظور احراز اصالت موفق توسط تصدیق‌کننده در پروتکل پیشنهادی، مالکیت تصدیق به محاسبه و ارسال پارامترهای معتبر  $(S_{SK}(h_{HK}(m', s')), S_A, h_{HK}(m', s'))$  و  $Ack$  به تصدیق‌کننده درگام ۱ و ۳ نیاز دارد. پارامتر  $S_A$  به تصدیق  $S_A \text{ mod } n = g^{(2^K m_A)} S_A \text{ mod } n$  نیاز دارد. این پارامتر می‌تواند به آسانی توسط هرکسی حل شده باشد یا به طور عمومی قابل دسترس باشد. هر چند ما نشان خواهیم داد که فقط مالکیت تصدیق  $A$  شخصی است که مؤلفه محرمانه  $S_A$  را می‌شناسد و می‌تواند یک  $Ack$  معتبر محاسبه کند. این به خاطر آن است که تصدیق‌کننده  $B$  می‌تواند کلید محرمانه یکبار مصرف  $K_{B,A}$  بکار برده شده را در ایجادکردن  $Ack$  به عنوان  $K_{B,A} = S_A^{v_B} = g^{S_A v_B} \text{ mod } n$  محاسبه کند، بر اساس فرضیه GDHA، مالکیت تصدیق  $A$  کسی است که برای شناخت مؤلفه محرمانه  $S_A$  می‌تواند  $K(A, B)$  را به عنوان  $K_{A,B} = c_B^{S_A} = g^{S_A v_B} = K_{B,A} \text{ mod } n$  محاسبه کند. بنابراین مالکیت تصدیق می‌تواند با تصدیق‌کننده فعل و انفعال داشته باشد و با موفقیت احراز اصالت شود.

**نکته ۳:** در پروتکل پیشنهادی  $CA$  یک امضای دیجیتال آفلاین/آنلاین را برای هرکاربر ثبت شده ایجاد می‌کند.  $CA$  واقعاً نیازمند ویژگی درجه یک روش تابع درهم‌ساز نبوده و درحقیقت  $CA$  به کلید درجه یک نیاز ندارد. بلکه فقط برای بکاربردن یک ویژگی روش تابع درهم‌ساز برای محاسبه یک مقدار درهم‌ساز  $S_A$  نیاز دارد. همچنین به منظور ایجاد یک پروتکل بر اساس  $IF$ ،  $CA$  به کارگیری امضای  $RSA$  [۲] را برای مقدار درهم‌ساز امضای دیجیتالی  $h(m', s')$  نیاز دارد.

## ۶.۵ تحلیل امنیتی

امنیت این پروتکل مبتنی ترکیب امن امضای  $RSA$  [۲]، پایداری تصادم یک روش تابع درهم‌ساز و فرضیه GDHA تکیه می‌کند. امضای دیجیتال آفلاین/آنلاین در مقابل حملات پیام انتخاب شده توافقی امن خواهد بود به شرط آن که طرح اصلی در مقابل حملات انتخاب شده پیام امن باشد. همچنین به درستی اثبات کردیم که تابع درهم‌ساز درجه یک، در برابر تصادم پایدار است. امنیت پروتکل پیشنهادی بر اساس مسئله لگاریتم گسسته DL، برقراری کلید  $IF$ ، ویژگی توانایی غیرقابل جعل و توانایی غیر درجه یک و همچنین توانایی غیرعملی بودن



شکل ۲: پروتکل توافق کلید و احراز اصالت بر اساس IF

معکوس تابع درهم‌ساز پایدار می‌باشد. علاوه بر این پروتکل ویژگی احراز اصالت انکارپذیر را فراهم کرده و نیز تصدیق دیجیتال کلید خصوصی را هم پشتیبانی می‌کند؛ از این رو طرح ما از بعضی مفاهیم اساسی، از قبیل یک روش تابع درهم‌ساز، به طور مثال MD5 (توابع استخراج چکیده پیام برای نگهداری داده‌های محرمانه در محیط کلید عمومی) یا SHA-1 (مرسوم‌تر ولی SHA-2 قوی‌تر و امن‌تر)، مسئله لگاریتم گسسته، و پروتکل توافق کلید دفی-هلمن به منظور پایداری در برابر حملات شناخته شده بهره گرفته است.

## ۶ نتیجه‌گیری

ما یک طراحی جدید در به کارگیری GDC برای احراز اصالت کاربر و برقراری کلید پیشنهاد کردیم که در این طرح یک GDC، کلید عمومی کاربر را در اختیار نداشته و از آن جایی که کاربر هر جفت کلید خصوصی و کلید عمومی را ندارد این نوع تصدیق دیجیتال برای مدیریت تصدیق‌های دیجیتال کلید عمومی X.509 خیلی آسان‌تر به نظر می‌رسد. این شیوه پیشنهادی می‌تواند هر دو سیستم رمزنگاری کلید عمومی بر اساس IF و DL پشتیبانی نماید.

## مراجع

- [1] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. 22, pp. 644-654, 1976. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

- [2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.
- [3] T. A. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469-472, 1985.
- [4] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM J. Comput.*, vol. 17, no. 2, pp. 281–308, 1988.
- [5] D. Chaum and H. van Antwerpen, "Undeniable signatures," *Advances in Cryptology - Crypto'89, Lecture Notes in Computer Science*, vol. 435, pp. 212-217, 1989.
- [6] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," *Advances in Cryptology - EUROCRYPT*, pp. 143-154, 1996. LNCS Vol 1070.
- [7] D. Chaum, "Private signature and proof systems," 1996.
- [8] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme," *ICISC 2003*, vol. 2836 of Springer Lecture Notes in Computer Science, pp. 40-54, 2003.
- [9] C. Schnorr, "Efficient signature generation by smart cards," *J. Cryptology*, vol. 4, no. 3, pp. 161-174, 1991.
- [10] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption « cost (signature) + cost (encryption))," *Advances in Cryptology - Crypto'97, Lecture Notes in Computer Science* vol. 1294, pp. 165-179, 1997.
- [11] R. Steinfeld, L. Bull, H. Wang, and J. Pieprzyk, "Universal designated verifier signatures," in *Asiacrypt'03*, vol. LNCS 2894, pp. 523-542, 2003.
- [12] F. Laguillaumie and D. Vergnaud, "Designated verifier signatures: anonymity and efficient construction from any bilinear map." *IACR eprint*.
- [13] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology: Proc. Crypto'84, Lecture Notes in Computer Science* vol. 196, (Berlin), pp. 47-53, Springer-Verlag, 1985.
- [14] Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) *CRYPTO 1984*. LNCS Vol. 196, Springer, Heidelberg. pp. 47–53.
- [15] Mandt TK, Tan CH. Certificateless authenticated two-party key agreement protocols. In: Okada M, Satoh I, eds. *Proc. of the 11th Annual Asian Computing Science Conference (ASIAN'06), Secure Software and Related Issues*, LNCS 4435, Berlin/Heidelberg: Springer-Verlag, 2008, pp. 37-44.
- [16] Canetti R, Krawczyk H. Analysis of key exchange protocols and their use for building secure channels. In: Pfitzmann B, ed. *Proc. of the Advances in Cryptology (EUROCRYPT'01)*, LNCS 2045, Berlin/Heidelberg: Springer-Verlag, 2001. pp. 453-474.
- [17] Cao Xue-fei, Kou Wei-dong, Fan Kai, Zhang Jun, "An Identity-Based Authenticated Key Agreement Protocol without Bilinear Pairing," *Chinese Journal of Electronics & Information Technology* 31(5), 2009. pp.1241-1244.

- [18] X.F. Cao, W.D. Kou, X.N. Du, "A Pairing-free Identity-Based Authenticated Key Agreement Protocol with minimal Message Exchanges," *Information Sciences* 180(15), 2010. pp. 2895-2903.
- [19] A. Cilardo, L. Coppolino, N. Mazzocca, L. Romano, Elliptic curve cryptography engineering, *Proceedings of the IEEE*, 94(2), 2006. pp. 395-406.
- [20] N.P. Smart, "An identity based authenticated key agreement protocol based on the Weil pairing," *Electronics Letters*, 38(13), pp. 630-632, 2002.
- [21] C. Gentry, "Practical identity-based encryption without random oracles," *Proc. of the EUROCRYPT'06, Lecture Notes in Computer Science 4004*, Berlin: Springer-Verlag, pp 445-464, 2006.
- [22] S.B. Wang, Z.F. Cao, and X.L. Dong, "Provably secure identity-based authenticated key agreement protocols in the standard model," *Chinese Journal of Computers* 30(10), pp. 1842-1854, 2007.
- [23] N. McCullagh, and P.S.L.M. Barreto. "A new two-party identity-based authenticated key agreement," *Proc. of CT-RSA 2005, LNCS vol. 3376*, Springer-Verlag, New York, pp. 262-274, 2005.
- [24] L. Chen, and C. Kudla, "Identity based key agreement protocols from pairings," *Proc. of the 16th IEEE Computer Security Foundations Workshop, IEEE Computer Society*, pp. 219-213, 2002. See also *Cryptology ePrint Archive, Report 2002/184*.
- [25] K. Shim, "Efficient ID-based authenticated key agreement protocol based on the Weil pairing," *Electronics Letters* 9(8), pp. 653-654, 2003.
- [26] H. Sun, and B. Hsieh. "Security analysis of Shim's authenticated key agreement protocols from pairings," *Cryptology ePrint Archive, Report 2003/113*, 2003. Available at <http://eprint.iacr.org/2003/113>.





# ارائه تعریف فضای سایبری و فضای مجازی بر پایه‌ی مبانی علم سایبرنتیک

احسان خوشحال‌پور<sup>۱</sup>

<sup>۱</sup> کارشناس ارشد مهندسی فناوری اطلاعات-امنیت اطلاعات، دانشگاه صنعتی مالک اشتر، تهران  
khoshhalpour@chmail.ir

## چکیده

فضای سایبری به عنوان یکی از مهم‌ترین پدیده‌های فناورانه‌ی عصر حاضر، تحولات شگرفی را در جوانب مختلف زندگی بشر موجب شده است. حجم، تنوع و سرعت تحولات ناشی از این پدیده، لزوم تدبیر و چاره‌اندیشی برای مواجهه‌ی مؤثر با این پدیده را به امری اجتناب‌ناپذیر بدل نموده است؛ این در حالی است که مواجهه صحیح با این پدیده، نیازمند داشتن شناخت و تعریف صحیح از آن است. علیرغم آنکه تعاریف متعددی از سوی کشورها، نهادها و افراد مختلف برای فضای سایبری ارائه شده است، اما به دلیل عدم توجه به مبانی علمی پیدایش این پدیده، هیچکدام از تعاریف شناخت و درک دقیق و کاملی از آن حاصل نمی‌کنند. در این پژوهش با مراجعه علم سایبرنتیک به عنوان مبنای علمی پیدایش این پدیده‌ی فناورانه، تعریف علمی و دقیقی از فضای سایبری ارائه می‌گردد. همچنین با تمایز قائل شدن میان مفاهیم فضای سایبری و فضای مجازی، تعریف فضای مجازی به عنوان زیرمجموعه و بخشی از فضای سایبری ارائه می‌گردد. تعاریف ارائه شده، تعاریف پایه‌ای بوده و شناخت کلی و صحیح از این مفاهیم حاصل می‌کنند، البته مبتنی و در انطباق با این تعاریف پایه، می‌توان تعاریف کاربردی متناسب با حوزه‌های مختلف کاربرد ارائه داد.

**کلمات کلیدی:** فضای سایبری، فضای مجازی، سایبرنتیک، سیستم پیچیده، ارتباطات و کنترل، محاسبات مصنوعی.

## ۱ مقدمه

فضای سایبری به عنوان پدیده‌ای فناورانه، تحولات گسترده و شگرفی را در زندگی بشر موجب گردیده است، به گونه‌ای که پسوند «سایبری» با الحاق به مفاهیم مختلف، مفاهیمی نظیر «جامعه‌ی سایبری»، «امنیت ملی سایبری»، «جنگ سایبری» و «قدرت سایبری» را موجب شده که سبب تغییر معنای این مفاهیم نسبت به معنای اولیه‌ی آنها شده است؛ این در حالی است که هنوز درک صحیحی از مفهوم فضای سایبری وجود ندارد و همین امر سبب عدم درک صحیح از مفاهیم منتج از ادغام این مفهوم با سایر مفاهیم می‌گردد. در این بین

واژگان فضای سایبری و فضای مجازی که مفاهیمی مرتبط اما متمایز هستند نیز گاهی هم‌معنا با هم و به جای هم به کار برده می‌شوند که این امر بر ابهام در حوزه مفاهیم این حوزه افزوده است. با وجود اینکه تعاریف مختلفی برای فضای سایبری ارائه شده است، اما به دلیل اینکه تعاریف موجود بر مبنای شناخت صحیح از پدیده حاصل نشده‌اند، هیچکدام از آنها تعریف کامل و دقیقی نبوده و کارآمدی لازم برای پاسخگویی به نیاز حوزه‌های کاربردی مختلف را ندارند. در مقاله حاضر ضمن ارائه شناخت صحیح از فضای سایبری با مراجعه به مبنای عملی آن یعنی سایبرنتیک، تعریف کامل و دقیقی از این فضا ارائه می‌گردد. مهم‌ترین نوآوری‌های این مقاله عبارت است از:

- مراجعه به علم سایبرنتیک به عنوان مبنای پیدایش فناوری فضای سایبری و ارائه تعریف فضای سایبری مبتنی بر آن؛
- تفکیک قائل شدن میان مفاهیم فضای سایبری و فضای مجازی و ارائه تعاریف مجزا و مرزبندی مشخص برای این مفاهیم؛
- ارزیابی کامل بودن تعریف فضای سایبری با نگاهی سه‌وجهی شامل مولفه‌ها، کارکردها و ماهیت این فضا.

ساختار مقاله حاضر بدین شرح است: در ابتدا در بخش ۲ ضمن ریشه‌یابی چگونگی پیدایش فضای سایبری، به تعاریف مختلف موجود از این فضا اشاره گردیده و نقدهای مطرح نسبت به هر تعریف به طور اجمالی بیان می‌گردد. پس از آن ضمن ارائه شناخت صحیح از مفاهیم پایه‌ای فضای سایبری و تبیین مرزبندی میان دو مفهوم فضای سایبری و فضای مجازی در بخش ۳، در بخش ۴ تعاریف پیشنهادی برای فضای سایبری و فضای مجازی ارائه می‌گردد. در نهایت در بخش ۵ به دلایل ارجحیت تعریف پیشنهادی بر تعاریف موجود اشاره می‌گردد.

## ۲ مروری بر کارهای دیگران

واژه سایبر در ابتدا از کار مبتکرانه‌ی ریاضیدان آمریکایی نوربرت وینر نشأت می‌گیرد، جایی که او واژه سایبرنتیک را جعل نموده و آن را در کتاب خود به عنوان علم «ارتباطات و کنترل در حیوان و ماشین» تعریف نمود [۱]. هر چند وینر خود از عبارت «فضای سایبری» استفاده نمود، اما تعریف وینر از سایبرنتیک، بیانگر وجوه انسانی و تکنولوژیکی مفهوم سایبر در کنار کارکردهای ارتباطی و کنترلی نهفته در آن است. اولین استفاده از عبارت فضای سایبری به تابلوهای هنری یک هنرمند و معمار دانمارکی به نام سوسانه اوسینگ و شریک او کارستن هاف در خلال سال‌های ۱۹۶۸ تا ۱۹۷۰ میلادی که آن عبارت را برای توصیف تابلوهای هنری شامل اشکال انسان‌هایی که در یک فضای ساخته شده از اشکال هندسی و اندامی قرار گرفته‌اند به کار بردند [۲]. البته کاربرد آنها از این واژه جنبه تکنولوژیکی و رایانه‌ای نداشت و عمدتاً بر تصویرسازی یک چشم‌انداز معماری مستقل از چگونگی امکان‌پذیر بودن تحقق آن تمرکز داشت.

با این حال گسترش عمومی و شهرت این عبارت به دومین کاربرد آن در حدود یک دهه بعد در آثار یک نویسنده‌ی آمریکایی به نام ویلیام گیپسون در داستان کوتاه «صفحه‌ی کرومی سوزان» در سال ۱۹۸۲ و سپس در رمان «نیورمنسر» در سال ۱۹۸۴ - با تعریف فضای سایبری به عنوان «یک توهم توافق‌شده‌ی انبوه میان میلیاردها اپراتور با کمک شبکه‌های رایانه‌ای» - برمی‌گردد [۳]. همانطور که مشخص است در این تعریف ضمن اشاره به عنصر انسانی مشابه توصیف هنرمندان دانمارکی، بر جنبه رایانه‌ای این فضا و ایجاد یک محیط جایگزین برای ارتباطات انسان توسط آن تاکید شده است.

طی سال‌های پس از آن، تعاریف متعددی از سوی کشورها، نهادها، فرهنگ لغات و افراد مختلف برای این فضا ارائه شده است. وزارت دفاع آمریکا (DOD)<sup>۱</sup> فضای سایبری را این‌طور تعریف کرده است: «فضای سایبری، یک دامنه‌ی جهانی درون محیط اطلاعاتی است که از شبکه‌ای به‌هم‌پیوسته از زیرساخت‌های فناوری اطلاعات و داده‌های مقیم که شامل اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و نیز پردازشگرها و کنترل‌کننده‌های تعبیه شده می‌باشد، تشکیل شده است» [۴]. این تعریف صرفاً بر مولفه‌های تکنولوژیکی این فضا تاکید دارد و هیچ اشاره‌ای به مولفه‌ی انسانی فضا و نیز کارکرد کنترلی آن ندارد. ناتو نیز در تعریفی متفاوت فضای سایبری را اینگونه تعریف کرده است: «محیطی متشکل از مولفه‌های فیزیکی و غیرفیزیکی که با استفاده از رایانه‌ها و طیف الکترومغناطیسی توصیف می‌شود و برای ذخیره‌سازی، اصلاح و تبادل داده با استفاده از شبکه‌های رایانه‌ای بکار گرفته می‌شود» [۵]. در این تعریف بدون اشاره‌ی صریح به مولفه‌های انسانی و تکنولوژیکی و نیز کارکردهای ارتباطی و کنترلی فضا، صرفاً بر ماهیت اطلاعاتی این فضا که کارکردهای این فضا را موجب می‌شود تاکید شده است. آژانس امنیت سایبری و امنیت زیرساخت (CISA)<sup>۲</sup> که واحدی عملیاتی ذیل وزارت امنیت داخلی آمریکا (DHS)<sup>۳</sup> می‌باشد، فضای سایبری را این‌طور تعریف کرده است: «فضای سایبری، سیستم عصبی زیرساخت‌های حیاتی ملی یعنی سیستم کنترلی کشور ماست. فضای سایبری از صدها هزار از رایانه‌ها، سرورها، مسیرهای، سوئیچ‌ها و کابل‌های فیبر نوری متصل به هم است که به زیرساخت‌های حیاتی ما اجازه‌ی کار می‌دهند» [۶]. در این تعریف، ضمن اشاره به مولفه‌های انسانی و تکنولوژیکی، بر کارکرد کنترلی این فضا تاکید شده است، اما کارکرد ارتباطی این فضا مغفول واقع شده است. علیرغم تعاریف متعدد ارائه شده برای فضای سایبری، هیچکدام از تعاریف پیشین تعریف کاملی از این فضا ارائه نمی‌دهند. تعریف کامل از این فضا تعریفی است که تمام مولفه‌ها و کارکردهای فضای سایبری را منعکس نموده و همچنین ماهیت این فضا را روشن نماید. در کنار لزوم کامل بودن، تعریف باید دقیق هم باشد و ضمن پرهیز از استفاده از واژگان اضافه، با استفاده از واژگان علمی و صریح ارائه گردد. لازمه‌ی دستیابی به چنین تعریفی مراجعه به مبانی عملی پیدایش این پدیده‌ی فناورانه یعنی سایبرنتیک است. در این مقاله بر پایه‌ی مبانی علم سایبرنتیک، تعریفی کامل، علمی و دقیق از این فضا ارائه می‌گردد. همچنین بر همین اساس با تفکیک قائل شدن میان دو مفهوم فضای سایبری و فضای مجازی، تعریفی مجزا برای فضای مجازی ارائه می‌گردد.

<sup>1</sup>Department of Defense

<sup>2</sup>Cybersecurity and Infrastructure Security Agency

<sup>3</sup>Department of Homeland Security

## ۳ تشریح مفاهیم پایه‌ای فضای سایبری

با ریشه‌یابی چگونگی شکل‌گیری معادل لاتین فضای سایبری یعنی عبارت Cyberspace، ریشه‌های پیدایش این عبارت در تحولات دهه‌ی ۱۹۴۰ و ۱۹۵۰ میلادی پس از جنگ جهانی دوم و ابداع علم «سایبرنتیک» توسط ریاضیدان نابغه «نوربرت وینر» یافته می‌شود. به بیان دیگر وجود واژه‌ی «Cyber» در دو عبارت «Cybernetics» و «Cyberspace»، تصادفی و صرفاً یک تشابه اسمی نیست و ریشه‌ی تمامی تحولات فعلی فضای سایبری و روندهای آینده‌ی این تحولات را باید در سایبرنتیک جستجو نمود. برای درک و شناخت درست از فضای سایبری لازم است تا ابتدا دو مفهوم پایه درک گردد:

- سیستم پیچیده
- سایبرنتیک

### ۱.۳ سیستم پیچیده

یک سیستم عبارت است از مجموعه‌ای از موجودیت‌ها (مانند افراد و ماشین‌ها) که در طول زمان برای دستیابی به یک یا چند هدف با هم تعامل دارند [۷]. سیستم‌ها از نظر سطح پیچیدگی به ۴ دسته‌ی ساده، دشوار، پیچیده و آشوبناک<sup>۴</sup> تقسیم می‌شوند [۸] که البته با تمرکز صرف بر نوع روابط میان اجزا، این ۴ دسته سیستم در نگاهی کلی‌تر در قالب ۲ دسته‌ی سیستم‌های ساده و پیچیده قابل دسته‌بندی هستند. در سیستم ساده روابط بین اجزا خطی است و رفتار کلی سیستم در نتیجه‌ی رابطه‌ای خطی میان رفتار اجزای سیستم بدست می‌آید. در سیستم پیچیده برخلاف سیستم ساده روابط بین اجزا غیرخطی است و رفتار سیستم از رابطه‌ی خطی میان رفتار مجزای تک تک اجزا قابل فهم و تعیین دقیق نیست [۹]، بلکه صرفاً در یک فضای احتمالی قابل پیش‌بینی است؛ در واقع بر خلاف سیستم ساده که رفتار اجزا مستقل از یکدیگر و محیط بوده و رفتار کلی سیستم از رابطه‌ی خطی میان این رفتارهای مجزا حاصل می‌شود، رفتار اجزا در سیستم پیچیده متاثر از یکدیگر و از محیط بوده و رفتار کلی سیستم نیز در نتیجه‌ی رفتار متقابل اجزا در تاثیر و تاثر از یکدیگر و محیط شکل می‌گیرد. در نتیجه در سیستم‌های ساده با مشاهده شرایط اولیه، امکان تعیین وضعیت آتی سیستم در زمان‌های مورد نظر وجود دارد، اما در سیستم‌های پیچیده، وضعیت آتی سیستم نه صرفاً به شرایط اولیه که به شرایط زمان اجرا - شامل رفتار متقابل اجزا و محیط - نیز بستگی دارد.

### ۲.۳ سایبرنتیک

همانطور که گفته شد در سیستم پیچیده، وضعیت آینده‌ی سیستم به طور دقیق قابل تعیین نیست، بلکه در یک فضای احتمال می‌توان حالات احتمالی آینده‌ی آن را پیش‌بینی نمود؛ همچنین گفته شد که وضعیت آتی

<sup>4</sup>Simple, Complicated, Complex and Chaotic

سیستم پیچیده در نتیجه‌ی روابط میان اجزا با هم و با محیط شکل می‌گیرد. سایبرنتیک تشریح‌کننده‌ی چگونگی این ارتباطات و خودکنترلی کلی موجود در سیستم پیچیده ناشی از این ارتباطات است [۱۰]. یک سیستم پیچیده برای تحقق وضعیت مطلوب در میان وضعیت‌های احتمالی آتی نیازمند روابط میان اجزا با هم و با محیط و اعمال کنترل ناشی از آن است. تشریح چگونگی تحقق این ارتباط و کنترل بر پایه‌ی اطلاعات و محاسبات، در کتاب وینر با عنوان «سایبرنتیک: کنترل و ارتباطات در حیوان و ماشین» [۱] صورت پذیرفته است.

سیستم سایبرنتیکی سیستمی است منطبق‌شونده با تغییرات درونی و محیطی برای حفظ حیات تا رسیدن به غایت مطلوب. کنترل در یک سیستم سایبرنتیکی به معنای درون‌آگاهی و محیط‌آگاهی از طریق بازخوردگیری همراه با اقدام به‌موقع اصلاحی به منظور حفظ تعادل و بقا و حرکت در جهت صحیح تا رسیدن به هدف است، یعنی همان کاری که سکاندار در کنترل کشتی در حرکت به سمت فانوس دریایی در شرایط مختلف انجام می‌دهد.

### ۳.۳ فضای سایبری

همانگونه که بیان شد یک سیستم برای برخورداری از کنترل، نیازمند ارتباطات میان اجزای خود و ارتباط با محیط است. وینر در کتاب خود بیان می‌کند که ساز و کار کنترل در انسان و ماشین محاسبه‌گر، ساز و کاری مشابه است و آن را در قالب علم سایبرنتیک تشریح می‌کند [۱].

در واقع سایبرنتیک را می‌توان «شریان کنترلی مبتنی بر مبادله و پردازش اطلاعات روی بستر محاسباتی» دانست، حال چنین شریانی هم در بدن وجود دارد که با بستر محاسباتی بیولوژیکی یا همان سیستم عصبی فراهم می‌آید و هم برای ماشین ایجاد شده که از طریق بستر محاسباتی مصنوعی یا همان فضای سایبری تامین می‌گردد.

پس فضای سایبری فناوری و ابزاری برای تحقق ارتباطات و کنترل سایبرنتیکی روی بستر محاسباتی الکترونیکی و راهکاری مصنوعی برای معادل‌سازی سازوکار ارتباطات و کنترل موجود در پدیده‌های پیچیده‌ی طبیعی است؛ در نتیجه فضای سایبری را می‌توان سایبرنتیک مصنوعی دانست.

### ۴.۳ فضای مجازی

گفته شد که یک سیستم برای برخورداری از کنترل، نیازمند ارتباطات میان اجزای خود و ارتباط با محیط است؛ اما فضای سایبری که یک فضای محاسباتی ماشینی است، برای ارتباط با اجزای زنده، نیازمند تبدیل و ترجمه از زبان ماشین به زبان حسی موجودات زنده و بالعکس است که این امر از طریق شبیه‌سازی رایانه‌ای میسر می‌گردد و اساساً مجاز عبارت است از محتوای ادراک‌پذیر و اقدام‌پذیر شبیه‌سازی شده توسط پردازش رایانه‌ای.

در واقع فضای مجازی یک لایه‌ی اجباری برای ارتباط فضای سایبری با گیرنده‌های حسی و عملگرهای حرکتی اجزای زنده سیستم و ترجمه از زبان ماشین به زبان حسی - حرکتی آنها و بالعکس است؛ بنابراین فضای مجازی نه معادل فضای سایبری بلکه بخشی از آن است، بخش موجود زنده فهم و حسی - حرکتی و

شبیه‌سازی شده‌ی فضای سایبری است که در قالب حسگرها و عملگرهای مورد نیاز برای اجزای زنده سیستم نمود پیدا می‌کند.

## ۴ تعاریف پیشنهادی

با توجه به آنچه گفته شد، روشن گردید که هرگونه تعریف از فضای سایبری و فضای مجازی در صورتی که ردی از سایبرنتیک در آن نباشد، تعریفی سطحی، تک‌بعدی و ناقص خواهد بود؛ بر این اساس و با شناختی که از فضای سایبری در بخش قبل حاصل شد، در ادامه تعاریف پیشنهادی برای فضای سایبری و فضای مجازی ارائه می‌گردد.

### ۱.۴ تعریف فضای سایبری

همانگونه که در بخش قبل گفته شد فضای سایبری همان سایبرنتیک مصنوعی است و تعریف فضای سایبری باید بر این اساس ارائه گردد. تعریف فضای سایبری عبارت است از: «بستر محاسباتی مصنوعی فراهم‌کننده ارتباطات و کنترل در سیستم‌های پیچیده‌ی زنده یا ماشینی.» بخش ابتدایی این تعریف یعنی «بستر محاسباتی مصنوعی» به «مصنوعی بودن» و بخش پایانی تعریف یعنی «ارتباطات و کنترل در سیستم‌های پیچیده‌ی زنده یا ماشینی» به «سایبرنتیکی بودن» این فضا اشاره دارد. لازم به ذکر است که بستر محاسبات مصنوعی، انواع بسترهای محاسباتی ساخت بشر از جمله محاسبات الکترونیکی و محاسبات کوانتومی را در بر می‌گیرد. در تشریح تعریف مذکور باید گفت که فضای سایبری بستر محاسباتی مصنوعی است که امکان پردازش، ذخیره‌سازی و انتقال اطلاعات میان اجزای یک سیستم یا میان سیستم و محیطش را برای کنترل رفتار سیستم به منظور حفظ تعادل و بقا و تکامل در مواجهه با شرایط از پیش تعیین نشده‌ی درونی یا بیرونی در مسیر دستیابی به اهداف تعریف شده فراهم می‌آورد؛ به بیان دیگر فضای سایبری بستر محاسباتی مصنوعی است که ارتباطات و کنترل لازم میان یک مجموعه از موجودیت‌ها برای هماهنگی آنها در قالب یک سیستم واحد هدفمند جهت حفظ تعادل و پایداری سیستم را تأمین می‌کند.

### ۲.۴ تعریف فضای مجازی

گفته شد که فضای مجازی، نمودی موجود زنده فهم از فضای سایبری است؛ بر این اساس تعریف فضای مجازی عبارت است از: «لایه‌ی ارتباطی حسی - حرکتی برای ارتباط فضای سایبری با اجزای هوشمند». مراد از اجزای هوشمند هر آن چیزی است که می‌تواند امور حادث‌شونده در محیط را ادراک نموده و نسبت به آن کنش هدفمند نشان دهد. بر این اساس تمامی موجودات زنده اعم از انسانی، حیوانی و نباتی و نیز ماشین‌های هوشمند، به عنوان اجزای هوشمند سیستم سایبرنتیکی محسوب می‌شوند و فضای مجازی تسهیل‌گر ارتباط آنها با فضای سایبری است.



## ۵ بررسی

تعاریف پیشنهادی در مقایسه با تعاریف موجود، تعاریفی علمی، کامل و دقیق است؛ علمی است چرا که مبتنی بر مبانی علمی پیدایش پدیده یعنی مبتنی بر علم سایبرنتیک ارائه شده است؛ کامل است چرا که تمامی مولفه‌های این فضا شامل مولفه‌های انسانی و رایانه‌ای، تمامی کارکردهای آن شامل کارکردهای ارتباطی و کنترلی را در کنار ماهیت آن شامل ماهیت فیزیکی، محاسباتی و اطلاعاتی منعکس می‌کند؛ همچنین دقیق است چرا که تمامی واژگان تعریف به دقت انتخاب شده است و از کاربرد واژگان اضافه و یا تفسیرپذیر اجتناب شده است.

گفتنی است که تعاریف پیشنهاد شده برای فضای سایبری و فضای مجازی، تعاریف پایه‌ای بوده و شناخت صحیح از این مفاهیم حاصل می‌کنند و می‌توان مبتنی و در انطباق با این تعاریف پایه، تعاریف کاربردی متناسب با حوزه‌های مختلف کاربردی ارائه داد.

## ۶ نتیجه‌گیری

در این سند ضمن معرفی سیستم پیچیده، مفاهیم مطرح در زمینه‌ی علم سایبرنتیک بیان گردید. همچنین فضای سایبری به عنوان بستری فناورانه برای تحقق ارتباطات و کنترل سایبرنتیکی و فضای مجازی به عنوان نمود موجود زنده فهم از فضای سایبری معرفی گردیده و بر این اساس تعریف فضای سایبری و فضای مجازی ارائه گردید. با توجه به اتکای تعاریف و مطالب ارائه شده بر مبانی علمی شکل‌گیری پدیده‌ی فناورانه‌ی فضای سایبری، تعاریف ارائه شده برای این فضا دارای بیشترین انطباق و کاربردپذیری برای پاسخگویی به نیازمندی‌های مختلف در حوزه‌ی فضای سایبری ارزیابی می‌گردد.

## مراجع

- [1] N. Wiener. *Cybernetics: Or Control and Communication in the Animal and the Machine*. John Wiley, 1948.
- [2] J. Lillemose, "The (re)invention of cyberspace," <https://kunstkritikk.com/the-reinvention-of-cyberspace>, Aug. 2015.
- [3] "Who invented the word cyberspace? what does it mean?," <https://herebeanswers.com/who-invented-cyberspace-means.html>
- [4] US Army, *Joint Publication 1-02, Department of Defense Dictionary of Military & Associated Terms*, [http://www.dtic.mil/doctrine/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf), 2016.
- [5] T. I. G. of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, New York, <http://csef.ru/media/articles/3990/3990.pdf>, 2013.

- [6] CISA, *The National Strategy to Secure Cyberspace*. Cybersecurity & Infrastructure Security Agency, [https://www.cisa.gov/uscert/sites/default/files/publications/cyberspace\\_strategy.pdf](https://www.cisa.gov/uscert/sites/default/files/publications/cyberspace_strategy.pdf), Feb. 2003.
- [7] B. J., J. S. Carson II, B. L. Nelson, and D. M. Nicol. *Discrete-Event System Simulation*. Pearson, 2005.
- [8] J. Appelo, "Simple vs. complicated vs. complex vs. chaotic," <https://noop.nl/2008/08/simple-vs-complicated-vs-complex-vs-chaotic.html>, Aug. 2008.
- [9] H. KoorehDavoudi and P. Bogdan, "A statistical physics characterization of the complex systems dynamics: Quantifying complexity from spatio-temporal interactions," *nature*, vol.6, no.1, pp.1-13, 2016.
- [10] S. Morlidge and S. Player. *Future Ready: How to Master Business Forecasting, Appendix 2: Important Concepts in Systems and Cybernetics*. John wiley and sons, 2010.

## ارائه یک مکانیزم تشویقی برای شبکه‌های حسگر جمعی بر پایه ارتباطات گوشی به گوشی

رسول اسماعیلی فرد<sup>۱</sup>، ستاره قره چاهی<sup>۲</sup>

<sup>۱</sup> استادیار، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی شیراز، فارس، ایران  
esmaeily@sutech.ac.ir

<sup>۲</sup> دانشجوی کارشناسی ارشد، دانشکده مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه صنعتی شیراز، فارس،  
ایران  
st.gharechahi@gmail.com

### چکیده

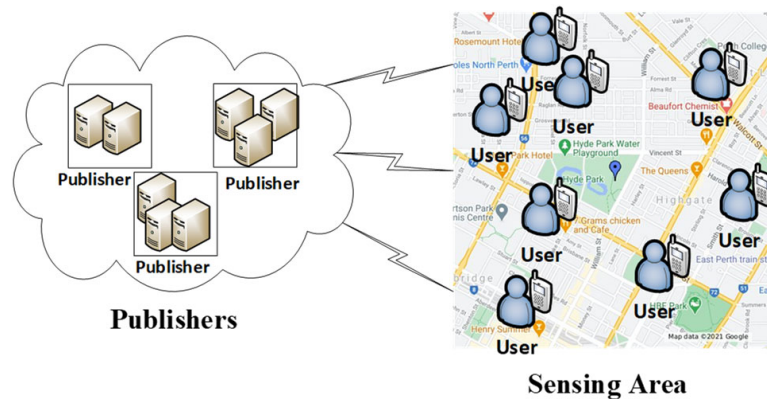
سیستم‌های سایبری موبایل می‌توانند از تلفن‌های هوشمند به‌عنوان یک پلت فرم راحت و اقتصادی استفاده کنند تا حسگری با دستگاه‌های موبایل را که کاربردی پیچیده و فراگیر است را بین انسان‌ها و دنیای فیزیکی اطراف تسهیل کنند. افزایش تعداد کاربران و حجم اطلاعات این شبکه‌ها منجر به افزایش هزینه و انرژی مصرفی کاربران می‌شود. علاوه بر این نیاز است داده‌های تولیدشده توسط کاربران در زمان کوتاه‌تر و با تأخیر کمتری به دست ناشرین برنامه‌های حسگری برسند. در این پژوهش به مسئله انتقال داده‌ها در شبکه‌های حسگری جمعی مبتنی بر ارتباطات گوشی به‌گوشی پرداخته شده است و یک مکانیزم تشویقی برای افزایش مشارکت کاربران ارائه داده شده است. در این مکانیزم کاربران با یکدیگر همکاری داشته و با مبادله داده‌های تولیدشده خود با داده‌های دیگر کاربران آنها را به دست ناشرین می‌رسانند. کاربران در ازاء همکاری که انجام می‌دهند اعتبار دریافت می‌کنند و مفهوم حواله برای انتقال این اعتبار معرفی شده است. ارتباطات بین کاربران به صورت یک بازی همکارانه‌ی دو نفره مدلسازی شده است و راه‌حل آن با یک رویکرد اکتشافی ارائه شده است. علاوه بر این یک مکانیزم حراج آنلاین به منظور سرعت بخشیدن گردش اعتبار و حواله در شبکه ارائه شده است. نتایج شبیه‌سازی نشان می‌دهد این روش باعث بهبود نرخ تحویل در مقایسه با سایر روش‌های رقیب می‌شود.

**کلمات کلیدی:** حسگری جمعی، ارتباطات گوشی به گوشی، مکانیزم تشویقی، نظریه بازی.

### ۱ مقدمه

تلفن‌های هوشمند و شبکه‌های تلفن همراه الگوی جدیدی به نام حسگری جمعی<sup>۱</sup> برای جمع‌آوری و پردازش داده‌ها درباره یک پدیده در مقیاس بزرگ ایجاد کرده‌اند. حسگری جمعی، جمعیت بزرگی از کاربران

<sup>۱</sup> Mobile Crowdsensing



شکل ۱: معماری شبکه حسگر جمعی با چند ناشر

دستگاه‌های موبایل را به کار می‌گیرد تا با استفاده از حسگرهای تعبیه شده در دستگاه‌هایشان به انجام وظایف حسی بپردازند. اخیراً این الگو به دلیل نفوذ دستگاه‌های موبایل در زندگی روزمره‌ی انسان‌ها به روشی موثر برای جمع‌آوری اطلاعات تبدیل شده است [۸]. یک سیستم حسگری جمعی اغلب از تعدادی کاربر و چند ناشر وظایف حسگری تشکیل شده است که کاربران اطلاعات مورد علاقه ناشرین را جمع‌آوری کرده و برای آنها ارسال می‌کنند [۱۵]. ناشرین با جمع‌آوری و پردازش این اطلاعات از آنها بهره‌برداری می‌کنند. معماری کلی این ارتباطات در شکل ۱ نمایش داده شده است. در این شبکه‌ها ممکن است چندین ناشر علاقمند به دریافت داده‌های حس شده یکسانی باشند.

اما از یک طرف داده‌های حس شده می‌توانند به فرمت‌های مولتی‌مدیا نظیر صدا، تصویر و ویدئو باشند و از طرف دیگر تعداد دستگاه‌های درگیر در فرآیند حسگری نظیر تلفن‌های هوشمند، گجت‌های پوشیدنی، ساعت‌های هوشمند و خودروهای هوشمند نیز در حال افزایش است [۴]. این مسئله باعث حجیم شدن داده‌های انتقالی در شبکه‌های حسگری جمعی می‌شود. بیشتر پلتفرم‌های حسگری از شبکه‌های سلولی موبایل برای انتقال اطلاعات خود استفاده می‌کنند اما حجیم بودن اطلاعات می‌تواند تا خروج از تحمل مقیاس‌پذیری شبکه‌های موبایل سلولی پیش برود. علاوه بر این، این مساله می‌تواند منجر به افزایش هزینه‌ها و مصرف انرژی برای کاربران شود و از تمایل کاربران در به انجام رساندن وظایف حسگری می‌کاهد. از سوی دیگر، ارتباطات گوشی به گوشی<sup>۲</sup> یک الگوی ارتباطی بی‌سیم جدید است که در آن دستگاه‌ها می‌توانند بدون استفاده از ایستگاه پایه یا شبکه اصلی با یکدیگر ارتباط برقرار کنند و داده‌های خود را به صورت فرصت‌طلبانه به اشتراک بگذارند [۶]. این الگو در نسل پنجم شبکه‌های سلولی گنجانده شده است و زمینه را برای شکل‌گیری بهتر چنین ارتباطاتی فراهم آورده است [۹]. سیستم‌های حسگری جمعی می‌توانند از آن برای کاهش هزینه کاربران و افزایش تمایل آنها برای مشارکت استفاده کنند [۳].

از سوی دیگر، مشارکت کاربران در شبکه‌های حسگری جمعی نیز به دلیل استفاده از منابع باتری یا قرار

<sup>2</sup>Device-to-Device Communications

دادن خودشان در معرض تهدیدهایی نظیر مسائل حریم خصوصی، اغلب داوطلبانه است [۱۴]. از این جهت، یکی از چالش‌های اصلی شبکه‌های حسگری جمعی داوطلبانه بودن مشارکت کاربران در این شبکه‌ها و نیاز به تشویق آنها به مشارکت است [۵]. از این رو، جلب مشارکت کاربران یک فاکتور حیاتی برای موفقیت انتقال اطلاعات در این نوع شبکه است و ارائه مشوق‌هایی به کاربر جهت افزایش مشارکت آنها می‌تواند در طراحی مکانیزم‌های انتقال بسیار موثر باشد.

در اینجا این سوال مطرح است که بر اساس شرایط سیستم حسگری توضیح داده شده، چگونه می‌توان با بکارگیری ارتباطات گوشی به گوشی و ارائه مشوق به کاربران سرعت انتقال اطلاعات در شبکه‌های حسگری جمعی با چند ناشر را بهبود داد. بر این اساس، تا جایی که مطلع هستیم این اولین مطالعه‌ای است که به بررسی ارائه راهکاری برای افزایش نرخ انتقال اطلاعات به چندین ناشر علاقمند به داده‌های حسگری در یک شبکه حسگری جمعی بر اساس ارتباطات گوشی به گوشی می‌پردازد و مکانیزم مشوقی را به منظور افزایش مشارکت کاربران ارائه می‌کند.

ادامه این مقاله به شرح مقابل سازمان‌دهی شده است. بخش دوم به مروری بر پیشینه تحقیق می‌پردازد. در بخش سوم روش پیشنهادی به تفصیل شرح داده می‌شود. در بخش چهارم روش پیشنهادی مورد ارزیابی قرار می‌گیرد و نتایج ارزیابی عملکرد گزارش می‌شود و مورد تفسیر قرار می‌گیرد. نهایتاً بخش پنجم به نتیجه گیری اختصاص یافته است.

## ۲ پیشینه پژوهش

با توجه به حرکت کاربران که منجر به ارتباط ناپایدار آنها می‌شود، مسئله انتقال داده‌های حس شده را می‌توان مشابه انتقال داده در شبکه‌های فرصت‌طلبانه موبایل دانست. در دیدگاه ارتباطات فرصت‌طلبانه گوشی به گوشی، حرکت کاربران منجر به ارتباط ناپایدار آنها می‌شود. اما با توجه به شرایط خاص داده‌های حسگری و با توجه به وظایف مشخص شده ناشران، برخی از مطالعات انجام شده به بررسی روش‌هایی برای مسیریابی انتقال اطلاعات به علاقمندان داده‌های حس شده در شبکه‌های حسگری جمعی پرداخته‌اند و روش‌هایی را برای آن ارائه داده‌اند. به عنوان مثال، وانگ و همکاران [۱۰] به ارائه راهکاری برای جمع‌آوری داده‌های حسگری جمعی با استفاده از ارتباطات گوشی به گوشی پرداخته‌اند و راهکاری را با در نظر گرفتن شرایط کاربران، زمان و مکان در نظر گرفته‌اند. آنها با تبدیل روند حرکت کاربر به یک گراف وزن‌دار جهت‌دار یک مساله جستجوی مسیر را تشکیل می‌دهند و با یک راهکار بهینه‌سازی حریصانه بازگشتی مساله را حل کرده‌اند. اما راهکار ارائه شده تنها مسیریابی برای یک هدف را مد نظر قرار می‌دهد و بنظر نمی‌رسد راهکار ارائه شده قابل توسعه به مسیریابی برای چند هدف باشد.

یانگ و همکاران [۱۱] به موضوع استفاده از ارتباطات فرصت‌طلبانه با برد کوتاه و ارتباطات شبکه‌های سلولی موبایل به صورت ترکیبی پرداخته‌اند تا هزینه استفاده از شبکه و باتری دستگاه را کاهش دهند و یک راه حل بهینه برای مسئله ارائه دهند. اما راهکار ارائه شده بر ارتباطات کوتاه برد نظیر وای‌فای و بلوتوث متمرکز است و قابلیت توسعه به ارتباطات با برد بلند گوشی به گوشی با تعداد کاربران بالا که مورد هدف این

پژوهش بوده است را ندارد.

اگر چه این مکانیزم‌های معرفی شده می‌توانند راهکار جایگزینی برای انتقال داده به ناشرین ارائه دهند اما فرض اکثر آنها همکاری کاربران در شبکه فرصت طلبانه است. در حالیکه در یک شبکه حسگر جمعی مشارکت کاربران داوطلبانه است و این مسئله موفقیت این راهکارها در محیط حسگر جمعی را کاهش می‌دهد. از این جهت مطالعاتی ارائه مکانیزم‌های تشویقی را بدین منظور مورد نظر قرار داده‌اند. بخشی از این مطالعات به ارائه مشوق برای ارتباطات تک‌هپه و خارج از شبکه سلولی برای کاهش هزینه پرداخته‌اند. در این روش‌ها اگر مقصد اطلاعات مستقیماً با کاربر روبرو شود می‌تواند اطلاعات خود را از آن دریافت کنند و یا حداکثر از تعداد ثابتی گره میانی استفاده شود. به عنوان نمونه، زان و همکاران [۱۳] و [۱۲] به ارائه مکانیزمی تشویقی برای انتقال داده‌های حساس به زمان برای جمع‌آوری داده‌ها در شبکه‌های فرصت طلبانه پرداخته است. این روش نیز از ارتباطات گوسی به گوسی بهره برده است. در این روش، داده‌ها پس از تولید به صورت چندین هپه به سمت مقصد منتقل می‌شوند. انتخاب گره‌های رله میانی با استفاده از راه‌حل چانه‌زنی نش انجام می‌شود. این روش اگر چه مکانیزم مناسبی را برای انتقال در شبکه‌های فرصت طلبانه ارائه می‌دهد، اما موضوع نوع داده‌ها که همان وظایف انجام شده مورد انتظار ناشرین در شبکه‌های حسگر جمعی هستند مورد توجه قرار نگرفته است. از این جهت، تصمیم‌گیری برای هدایت داده‌ها بر اساس نوع آنها و یا چندین مقصد میسر نیست و داده‌ها را می‌توان تنها به سمت یک مقصد خاص هدایت کرد.

### ۳ روش پیشنهادی

در این بخش یک مکانیزم تشویقی برای مدل انتقال داده شرح داده می‌شود تا بوسیله آن بتوان کاربران را به همکاری با یکدیگر تشویق کرد. در این مدل انتقال داده، تولیدکنندگان داده در ازای تحویل داده به ناشرین از آنها پاداش دریافت می‌کنند. این کاربران حاضرند تا به منظور تحویل داده‌هایشان به ناشرین علاقمند از سایر کاربران کمک بگیرند و به آنها پاداش یا اعتبار پرداخت کنند. بنابراین کاربری که داده‌ای را به ناشر تحویل می‌دهد می‌تواند از کاربر تولیدکننده آن داده پاداش دریافت کند. اما این مسئله که چگونه تولیدکننده می‌تواند بفهمد کدام کاربر به تحویل داده کمک کرده است و همچنین چگونه تحویل دهنده می‌تواند پاداش خود را دریافت کند، از چالش‌هایی است که باید در مکانیزم پیشنهادی در نظر گرفته شود. در این مکانیزم، کاربران داده‌های حسگری خود را تولید می‌کنند و آنها را برای ناشرین علاقمند می‌فرستند. در این مکانیزم کاربران خودخواه و با رفتار منطقی فرض می‌شوند که با در نظر گرفتن منافع خود و تنها در صورتی که از آن سود ببرند، انتقال داده را انجام می‌دهند.

بدین منظور، هر داده‌ای که تولید می‌شود، به همراه آن یک حواله نیز تولید می‌شود و به آن یک شناسه خاص غیر قابل تغییر و یک بهای اختصاص می‌یابد. بهای حواله  $d$  با  $d$  نشان داده می‌شود و نشان دهنده مقدار اعتباری است که تولید کننده داده  $d$  در قبال رساندن داده‌اش به دست ناشران پرداخت می‌کند. به هنگام تحویل داده به ناشر، حواله‌ی آن داده توسط ناشر امضا می‌شود و به کاربر تحویل داده می‌شود. حداکثر تحویل داده‌ی  $d$  که با  $h_d$  نمایش داده می‌شود، تعیین کننده حداکثر تعداد ناشرانی است که قرار است داده



را تحویل بگیرند. ناشران علاقمند به جمع‌آوری انواع مختلفی داده هستند. برای هر داده یک نوع در نظر گرفته می‌شود که با  $i$  نمایش داده می‌شود.

برای آنکه مشخص شود هر کاربر با چه احتمالی با ناشرین علاقمند به نوع داده  $i$  به طور مستقیم یا غیرمستقیم ارتباط دارد، از ارتباط نزدیک استفاده می‌شود. ارتباط نزدیک مستقیم در صورتیکه کاربر  $u$  مستقیماً با یکی از ناشرین علاقمند به نوع داده  $i$  برخورد کند، طبق معادله ۱ بروزسانی می‌شود. در صورتی که کاربر بطور غیرمستقیم و از طریق کاربر  $v$  با یکی از ناشرین علاقمند به نوع داده  $i$  برخورد کند، ارتباط نزدیک غیرمستقیم طبق معادله ۲ بروزسانی می‌شود.  $\alpha$  و  $\beta$  عددی ثابت بین صفر و یک هستند که تاریخچه‌ای از ارتباطات نزدیک قبلی کاربر را نگهداری می‌کنند. در صورتیکه طی یک بازه زمانی مشخص کاربر با هیچ ناشر یا کاربر دیگری برخورد نداشته باشد، این ارتباطات بروزسانی می‌شوند. ارتباط نزدیک کلی کاربر  $u$  با یک ناشر با استفاده از ارتباط نزدیک مستقیم و غیرمستقیم طبق معادله ۳ محاسبه می‌شود.

$$Y_u^{(i)} := \begin{cases} (1 - \alpha)Y_u^{(i)} + \alpha & \text{contact} \\ (1 - \alpha)Y_u^{(i)} & \text{Timeout} \end{cases} \quad (1)$$

$$Z_u^{(i)} := \begin{cases} (1 - \beta)Z_u^{(i)} + \beta Y_v^{(i)} & \text{contact} \\ (1 - \beta)Z_u^{(i)} & \text{Timeout} \end{cases} \quad (2)$$

$$X_u^{(i)} = 1 - (1 - Y_u^{(i)})(1 - Z_u^{(i)}) \quad (3)$$

هنگامی که دو کاربر به هم می‌رسند، هر کدام به دنبال آن است که با مبادله داده یا حواله منافع خود را به حداکثر برساند. برای این منظور کاربران باید بتوانند ارزش هر داده یا حواله را تخمین بزنند. ارزش یک داده به دو عامل بستگی دارد. اولین عامل مربوط به احتمال برخورد کاربر با ناشران علاقمند است. هرچه این احتمال بالاتر باشد، داده نیز با ارزشتر می‌شود. دومین عامل مربوط به حداکثر تحویل است. هر چه این عدد بزرگتر باشد، احتمال تحویل داده به تعداد بیشتری ناشر علاقمند وجود دارد و در نتیجه احتمال دریافت پاداش بیشتر است.

بدلیل پیچیدگی بروزسانی حداکثر تحویل برای داده‌ها و به منظور تسهیل در تعیین ارزش داده و مبادله آن، کاربر برای هر داده به اندازه  $h_d$  داده مجازی درست می‌کند. معادله ۴ نشان‌دهنده ارزش بالقوه داده مجازی  $d'$  و پاداش مجازی داده است که با  $R_u^{d'}$  نشان داده شده است و مشخص می‌کند کاربر  $u$  با مبادله داده مجازی  $d'$  چه مقدار اعتبار می‌تواند به دست آورد. در این معادله  $v_{d'}$  بهای حواله مربوط به داده  $d$  است و  $X_u^{(i)}$  نشان‌دهنده ارتباطات کاربر  $u$  با ناشران علاقمند به نوع داده  $i$  است. به شکل مشابه، برای تسهیل در تعیین ارزش یک حواله از پاداش مجازی حواله استفاده می‌شود.

$$R_u^{d'} = v_{d'} \times X_u^{(i)} \quad (4)$$

فرض کنیم کاربر  $u$  با کاربر دیگر ملاقات می‌کند و داده‌هایی در این بین مبادله می‌شود.  $\varphi_u$  و  $\hat{\varphi}_u$  به ترتیب مجموعه‌ای از داده‌های کاربر  $u$  قبل و بعد از مبادله هستند. منفعت شخصی که کاربر  $u$  از مبادله داده‌ها به دست می‌آورد با  $S_u^d$  نشان داده می‌شود و با معادله ۵ محاسبه می‌گردد. منفعت شخصی حاصل از مبادله حواله‌های امضاشده نیز بطور مشابه محاسبه می‌شود.

$$S_u^d = \sum_{d \in \hat{\varphi}_u} R_u^d - \sum_{d \in \varphi_u} R_u^d \quad (5)$$

بدلیل خودخواه بودن کاربران، هر کاربر قصد دارد در صورت تبادل داده منفعت شخصی خود را به حداکثر برساند. برای اینکه کاربر  $u$  بتواند بهترین تصمیم را در خصوص تبادل داده‌ها بگیرد از تابع سودمندی آمده در معادله ۶ استفاده می‌شود که در آن  $P_u$  نشان‌دهنده تابع سودمندی کاربر  $u$  است.  $\varphi_u$  و  $\hat{\varphi}_u$  به ترتیب مجموعه‌ای از داده‌ها قبل و بعد از مبادله داده هستند.

$$\max P_u = \sum_{d \in \hat{\varphi}_u} R_u^d - \sum_{d \in \varphi_u} R_u^d \quad (6)$$

### ۱.۳ مکانیزم تشویقی

بر اساس مدل انتقال داده مطرح شده، مکانیزم تشویقی پیشنهادی در ادامه در پنج مرحله توصیف شده است. لیست  $L_u$  نشان‌دهنده این مجموعه‌ی داده‌های توصیفی برای داده‌های متعلق به کاربر  $u$  است و لیست  $E_u$  ارتباطات نزدیک کاربر  $u$  را نشان می‌دهد.

در اولین مرحله، هر کاربر به صورت متناوب کشف همسایه انجام می‌دهد. بدین منظور، هنگامی که کاربر  $u$  با کاربر یا ناشر همسایه  $v$  که در فاصله نزدیک او قرار دارد ملاقات می‌کند، کاربر  $u$  لیست‌های  $L_u$  و  $E_u$  را برای همسایه  $v$  ارسال می‌کند و همزمان همسایه  $v$  نیز لیست‌های  $L_v$  و  $E_v$  خود را برای کاربر  $u$  می‌فرستد. سپس بر اساس لیست‌های بدست آمده از همسایه  $v$  اطلاعات خود را در مورد داده‌های  $\varphi_v$  و حواله‌های  $\psi_v$  بروزرسانی می‌کند. این اقدام منجر به تشکیل یک لیست کاندید مبادله داده به نام  $K_u$  به صورت  $K_u = \varphi_v - (\varphi_u \cap \varphi_v)$  و  $\hat{K}_u = \psi_v - (\psi_u \cap \psi_v)$  به صورت  $\hat{K}_u = \psi_v - (\psi_u \cap \psi_v)$  می‌شود. این دو لیست در واقع نشان‌دهنده داده‌ها یا حواله‌هایی است که در گره  $v$  موجود هستند اما در گره  $u$  نیستند.

در دومین مرحله اگر کاربر  $u$  یک ناشر باشد و علاقمند به چند نوع داده در لیست  $k_u$  باشد، آن داده‌ها را از همسایه  $v$  خود درخواست می‌کند. بعد از دریافت هر داده، ناشر  $u$  یک کپی از حواله مربوط به آن داده را برای کاربر  $v$  امضا می‌کند و به او تحویل می‌دهد. در سومین مرحله کاربر  $u$  لیست کاندید مبادله حواله  $\hat{k}_u$  را بررسی می‌کند و اگر حواله‌ای در این لیست بنام وی بود باید بهای آن را پرداخت کند. بدین منظور وی باید اعتبار کاربر  $v$  را معادل با بهای داده‌ی آن حواله افزایش دهد. کاربر  $v$  بعد از دریافت اعتبار، آن حواله‌ها را از  $\psi_v$  حذف می‌کند.

در چهارمین مرحله کاربران  $u$  و  $v$  به بررسی اینکه کدام داده‌ها و حواله‌ها باید معامله شوند می‌پردازند و بر سر انتخاب داده‌ها و حواله‌ها چانه‌زنی می‌کنند. این مرحله می‌تواند به صورت یک بازی همکارانه دونفره در نظر گرفته شود و یک رویکرد اکتشافی برای رسیدن به راه‌حل بهینه اعمال شود. در مرحله آخر، دو کاربر  $u$  و  $v$  داده‌های انتخاب شده در لیست‌های  $L'_u$  و  $L'_v$  و همچنین حواله‌های انتخابی در دو لیست  $L''_u$  و  $L''_v$  را با یکدیگر مبادله می‌کنند.

اگر فرض را بر این بگذاریم که کاربران رفتار منطقی دارند، می‌توانیم تعامل بین دو کاربر را به صورت یک بازی همکارانه دونفره مدلسازی کنیم. راه‌حل بهینه برای بازی همکارانه دونفره با به حداکثر رساندن حاصلضرب زیر ارائه می‌شود [۷].

$$\left(\hat{P}_u, \hat{P}_v\right) = \arg \max \left(P_u - D_u\right) \times \left(P_v - D_v\right) \quad (7)$$

در معادله ۷ زوج مرتب  $(D_u, D_v)$  نقطه وضعیت کنونی بر روی تابع را نشان می‌دهد که در کار ما بر روی  $(0,0)$  تنظیم می‌شود.  $\hat{P}_u$  و  $\hat{P}_v$  به ترتیب بازده سودمندی گره‌های  $u$  و  $v$  هستند که باید عددی مثبت باشند تا بتوان به یک راه حل امکان پذیر دست یافت.  $P_u$  و  $P_v$  توسط مجموعه داده‌های مبادله شده تعیین می‌شود که در معادله ۶ نشان داده شده است. راه‌حل بهینه نهایتاً منجر به تولید یک مجموعه از داده‌هایی می‌شود که باید بین کاربر  $u$  و  $v$  مبادله شوند. بررسی تمام ترکیبات ممکن داده‌ها می‌تواند زمان‌نمایی داشته باشد. جهت رفع این مشکل یک رویکرد اکتشافی ساده به کار گرفته می‌شود به این صورت که در هر لحظه فقط یک جفت داده در نظر گرفته می‌شود و حاصلضرب برای آن محاسبه می‌شود.

### ۲.۳ الگوریتم حراج آنلاین توزیعی

حواله اعتبار واقعی نیست و نمی‌توان مستقیماً از آن برای پرداخت پاداش تحویل داده استفاده کرد. چراکه تحویل‌دهنده بایستی مستقیماً با تولیدکننده داده ملاقات داشته باشد تا بتواند حواله امضا شده خود را به اعتبار تبدیل کند. فرایند این تبادل به عنوان یک مدل حراج فرموله شده است تا سود خریدار را به حداکثر برساند. حراج آنلاین یک نوع مزایده از طریق شبکه‌های کامپیوتری است که در آن قیمت کالاها و خدمات در انتهای یک فرجه زمانی به خریداران مشخص می‌شود. خریداران باید بدون اطلاع از قیمت نهایی، قیمتی را پیشنهاد دهند که قابل لغو نیست و بالاترین پیشنهاد به عنوان برنده انتخاب خواهد شد.

در این حراج که برگرفته از مسئله منشی است، یک کاربر به عنوان خریدار و یک کاربر به عنوان فروشنده یک حواله وارد مکانیزم حراج می‌شوند. فروشنده با خریداران یکی پس از دیگری ملاقات می‌کند و در نتیجه از پیشنهادهایی که در آینده توسط سایر خریداران ممکن است دریافت کند خبری ندارد. بنابراین، می‌توانیم هر حواله را به عنوان یک موقعیت منشی‌گری در نظر بگیریم و به دنبال انتخاب بهترین خریدار حواله از بین تمام خریداران باشیم. ما مکانیزم حراج آنلاین را بر اساس مکانیزم معرفی شده در [۱] طراحی می‌کنیم که توسط الگوریتم ۱ نمایش داده شده است. فرض می‌کنیم همه خریداران دارای چگالی زمانی رسیدن مستقل  $a$  بر روی بازه زمانی  $[T, 0]$  هستند و  $A$  نشان‌دهنده تابع توزیع زمان رسیدن مربوطه باشد که به صورت معادله ۸ در زیر نمایش داده می‌شود.

## الگوریتم ۱. الگوریتم حراج آنلاین توزیعی

---

**Input:**  $time, bid, maxBid$   
**Output:**  $Bid\ acceptance$

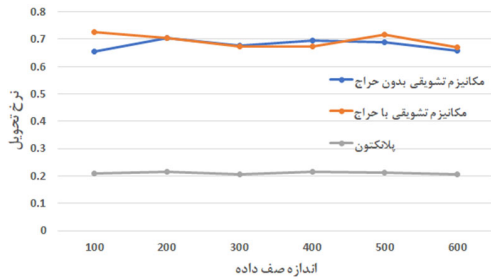
- 1: **if**  $bid \geq highestPrice$  **then**
- 2:     **return**  $true$
- 3: **end if**
- 4:  $waitingTimeLimit \leftarrow \tau$ , where  $A(\tau) = 1 / e$
- 5: **if**  $time < waitingTimeLimit$  **then**
- 6:     **if**  $bid > maxBid$  **then**
- 7:         **return**  $maxBid = bid$
- 8:     **end if**
- 9:     **return**  $false$
- 10: **end if**
- 11: **if**  $bid > maxBid$  **and**  $bid \geq lowestPrice$  **then**
- 12:     **return**  $true$
- 13: **end if**
- 14: **return**  $false$

---

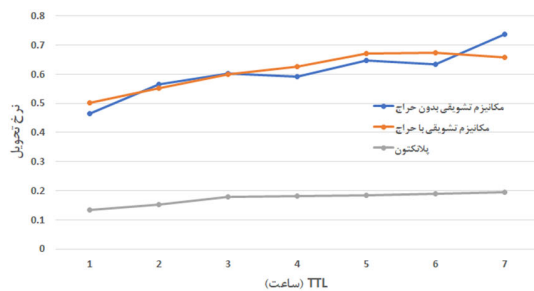
$$A(t) = \int_0^t a(s) ds, 0 \leq t \leq T \quad (8)$$

## ۴ ارزیابی کارایی

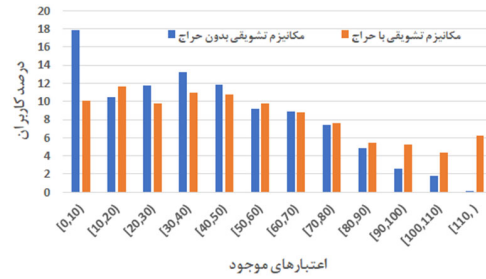
در این بخش نتایج حاصل از شبیه‌سازی ارائه می‌شود و کارایی روش پیشنهادی بررسی می‌شود. جهت ارزیابی، روش پیشنهادی با روش پلانکتون [۲] مقایسه می‌شود. پلانکتون یک الگوریتم مسیریابی است که کاربران همگی خودخواه هستند و مشارکتی در انتقال داده‌ها انجام نمی‌دهند. در این شبیه‌سازی تعداد ناشران ۴، انواع علاقمندی ۱۰، تعداد کاربر ۱۰۰، اندازه صف داده ۱۰۰، نرخ تولید داده ۱ داده در هر ۱۵ دقیقه، تعداد علاقمندی‌های هر ناشر ۵، اعتبار اولیه هر کاربر ۱۰۰ و بهای حواله ۱ در نظر گرفته شده است. در ابتدای شروع فعالیت کاربران در شبکه اعتباری در اختیار آنها قرار می‌گیرد که از طریق آن می‌توانند به انتشار داده‌ها در شبکه اقدام کنند. هرچه یک کاربر اعتبار بیشتری داشته باشد، می‌تواند داده‌های بیشتری را انتشار دهد. هرچه توزیع اعتبار و دریافت وجه حواله‌های حاصل از تحویل داده‌ها در شبکه روانتر انجام گیرد احتمال مواجه شدن کاربران با کمبود اعتبار کمتر است. شکل ۲ توزیع اعتبارهای موجود در خاتمه شبیه‌سازی را برای روش پیشنهادی نشان می‌دهد. نتایج نشان می‌دهد فرایند حراج به کاربران کمک کرده



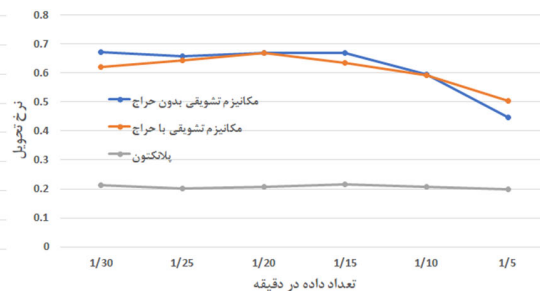
شکل ۳. نرخ تحویل تحت افزایش اندازه صف داده



شکل ۵. نرخ تحویل تحت مختلف TTL های مختلف



شکل ۲. توزیع اعتبارهای موجود



شکل ۴. تاثیر نرخ تولید داده بر روی نرخ تحویل

است تا تعادل خوبی در تولید و مصرف اعتبار داشته باشند و بتوانند به طور مداوم داده‌های خود را منتشر کنند.

شکل‌های ۳ الی ۵ روند کارایی را با تغییر پارامترهای شبکه مانند اندازه صف، بار ترافیک و TTL نشان می‌دهند. همانطور که در شکل ۳ نشان داده شده است، با افزایش یافتن اندازه صف، نرخ تحویل همه روش‌ها کمی افزایش پیدا می‌کند زیرا کاربران با داشتن صف طولانی‌تر می‌توانند داده‌های بیشتری را برای مدت طولانی‌تری نگهداری کنند. اما تاثیر افزایش اندازه صف بر روی دو روش مکانیزم تشویقی بدون حراج و با حراج به صورت جزئی است و نرخ تحویل نسبت به روش پلانکتون بالاتر است. کارایی روش‌های پیشنهادی تحت بار ترافیک مختلف نیز مورد ارزیابی قرار گرفت و نرخ تولید داده از یک داده در هر ۳۰ دقیقه شروع شد و تا یک داده در هر ۵ دقیقه افزایش یافت. نتایج در شکل ۴ نشان می‌دهد که با افزایش بار ترافیک و وارد شدن ترافیک بیشتر به شبکه نرخ تحویل در همه روش‌ها کاهش پیدا کرده است. این موضوع از آنجا ناشی می‌شود که اندازه صف کاربران محدود است و کاربران ناچار به حذف داده‌های قبلی خود در صف پر شدن صف هستند. اما همچنان در روش‌های پیشنهادی، نرخ تحویل بالاتر است. برای مشاهده میزان تاثیر TTL بر نرخ تحویل، این میزان از ۱ ساعت به ۷ ساعت تغییر داده شد. همانطور که در شکل ۵ مشاهده می‌شود، با افزایش TTL روش‌های پیشنهادی می‌توانند داده‌های بیشتری را به ناشران انتقال دهند.

## ۵ نتیجه‌گیری

در این پژوهش، یک مکانیزم تشویقی جهت تشویق کاربران به همکاری در انتقال داده‌های تولید شده در شبکه‌های حسگری جمعی بر پایه ارتباطات گوشی به گوشی ارائه شد. در این مکانیزم تشویقی، کاربران داده‌های تولید شده خود را با دیگر کاربران مبادله می‌کنند و آنها را در شبکه انتقال می‌دهند تا داده‌ها به دست ناشرین علاقمند رسانده شوند. مبادله داده بین کاربران به صورت یک بازی همکارانه دونفره مدلسازی شد و راه‌حل آن با یک رویکرد اکتشافی به دست آمد. در مکانیزم ارائه شده تولیدکنندگان داده به کاربرانی که در انتقال داده‌هایشان همکاری داشته‌اند اعتبار پرداخت می‌کنند و برای هر کاربر یک حواله صادر می‌کنند. علاوه بر این، جهت تسریع گردش اعتبارات در شبکه، یک الگوریتم حراج آنلاین برای حواله‌ها معرفی شد. در آخر نیز جهت ارزیابی و مقایسه عملکرد روش پیشنهادی، شبیه‌سازی صورت گرفت. نتایج شبیه‌سازی راهکار پیشنهادی حکایت از بهبود نرخ تحویل داده و بهبود گردش اعتبار در شبکه دارد.

## مراجع

- [1] D. YANG, G. XUE, X. F., AND TANG, J. "Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing". *Proceedings of the 18th annual international conference on Mobile computing and networking* (2012).
- [2] GUO, X. F., AND CHAN, M. C. "Plankton: An efficient DTN routing algorithm". *2013 IEEE International Conference on Sensing, Communications and Networking (SECON)* (2013), 550–558.
- [3] HOU, H., JIN, H., AND LIAO, X. "Cost Efficient Edge Service Placement for Crowdsensing via Bus Passengers". *IEEE Access* 26, 2 (2021), 899–908.
- [4] KRAFT, R., REICHERT, M., AND PRYSS, R. Towards the Interpretation of Sound Measurements from Smartphones Collected with Mobile Crowdsensing in the Healthcare Domain: An Experiment with Android Devices". *Sensors* 22, 1 (2022).
- [5] LI, Y., LI, F., YANG, S., ZHOU, P., ZHU, L., AND WANG, Y. "Three-stage stackelberg long-term incentive mechanism and monetization for mobile crowdsensing: An online learning approach". *IEEE Transactions on Network Science and Engineering* 8, 2 (2021), 129–153.
- [6] MALIK, P. K., WADHWA, D. S., AND KHINDA, J. S. "A survey of device to device and cooperative communication for the future cellular networks". *International Journal of Wireless Information Networks* 27, 3 (2022), 411–432.
- [7] NASH, J. "Two-Person Cooperative Games". *Econometrica* 21, 1 (1953), 128–140.
- [8] NGUYEN, T. N., AND ZEDADALLY, S. "Mobile crowd-sensing applications: Data redundancies, challenges, and solutions". *ACM Transactions on Internet Technology (TOIT)* 22, 2 (2021), 1–15.



- [9] REE, M. D., MANTAS, G., RADWAN, A., MUMTAZ, S., RODRIGUEZ, J., AND OTUNG, I. E. "Key management for beyond 5G mobile small cells: A survey". *IEEE Access* 7 (2019), 59200–59236.
- [10] WANG, L., YU, Z., YANG, D., KU, T., GUO, B., AND MA, H. "Collaborative mobile crowdsensing in opportunistic D2D networks: A graph-based approach". *ACM Transactions on Sensor Networks* 15, 3 (2019), 1–30.
- [11] YANG, S., ADEEL, U., AND MCCANN, J. "Backpressure meets taxes: Faithful data collection in stochastic mobile phone sensing systems". *2015 IEEE Conference on Computer Communications (INFOCOM)* (2015), 1490–1498.
- [12] ZHAN, Y., XIA, Y., LIU, Y., LI, F., AND WANG, Y. "Incentive-aware time-sensitive data collection in mobile opportunistic crowdsensing". *IEEE Transactions on Vehicular Technology* 66, 9 (2017), 7849–7861.
- [13] ZHAN, Y., XIA, Y., ZHANG, J., AND WANG, Y. "Incentive mechanism design in mobile opportunistic data collection with time sensitivity". *IEEE Internet of Things Journal* 5, 1 (2017), 246–256.
- [14] ZHAO, B., TANG, S., LIU, X., AND ZHANG, X. "PACE: Privacy-preserving and quality-aware incentive mechanism for mobile crowdsensing". *IEEE Transactions on Mobile Computing* 20, 5 (2020), 1924–1939.
- [15] ZHENG, X., YUAN, Q., WANG, B., AND ZHANG, L. "A Homomorphic Encryption Based Location Privacy Preservation Scheme for Crowdsensing Tasks Allocation". *Wireless Personal Communications*, 2022.



## تشخیص طنز در زبان فارسی با رویکرد یادگیری عمیق

فاطمه نجفی لیوندانی<sup>۱</sup>، محمدحسن شیرعلی شهرضا<sup>۱</sup>

<sup>۱</sup> دانشکده ریاضی و علوم کامپیوتر، دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)، تهران، ایران  
{fatemenajafi135,hshirali}@aut.ac.ir

### چکیده

طنز و طعنه روشی خلاقانه برای بیان احساسات است که انسان‌ها با به کار بردن آن در گفتار یا نوشتار، ممکن است هدف و منظوری متفاوت با آنچه بیان می‌شود داشته باشند. با گسترش استفاده از اینترنت، استفاده از شبکه‌های اجتماعی و وبسایت‌های فروش اینترنتی افزایش پیدا کرده است. با مرسوم شدن اعلام دیدگاه‌ها در این شبکه‌ها یا بیان نظرات در مورد کالاهایی که در وبسایت‌ها به فروش گذاشته شده‌اند، بررسی نظرات و احساسات کاربران در این موارد برای شرکت‌ها و سازمان‌ها اهمیت شایانی پیدا می‌کند. چون معمولاً این نظرات با زبان رسمی و به صراحت اعلام نمی‌شوند و گاهی آغشته به شوخی، طعنه و کنایه هستند، کارایی تحلیل احساسات تحت تأثیر قرار می‌گیرد. در سال‌های اخیر، توییت‌ها به منبع بزرگی از ابراز ایده‌ها و دیدگاه‌های کاربران در تقریباً تمامی زمینه‌ها تبدیل شده است. این مسئله باعث جلب توجه شرکت‌ها و پژوهشگرانی به توییت‌ها شده است که در زمینه تحلیل نظرات کاربران فعالیت می‌کنند. درصد بالایی از توییت‌ها شامل طنز هستند و کاربران فارسی‌زبان نیز از این قاعده مستثنی نمی‌شوند. تحلیل‌هایی که به وجود شوخی در متن آگاه باشند، می‌توانند با دقت بهتری احساسات را پیش‌بینی کنند. در این پژوهش مجموعه داده‌ای از توییت‌های فارسی معرفی می‌شود که برچسب نمونه‌ها نشان‌گر وجود طنز و یا عدم وجود آن است. با استفاده از تطبیق دقیق مدل‌های زبانی از پیش آموزش داده شده بر روی مجموعه داده به دست آمده، مدلی برای تشخیص وجود یا عدم وجود طنز در زبان فارسی ارائه می‌دهیم.

**کلمات کلیدی:** تشخیص طنز، تحلیل احساسات، پردازش زبان طبیعی، یادگیری عمیق، ترانسفررها، زبان فارسی.

### ۱ مقدمه

طنز و طعنه روشی خلاقانه برای بیان احساسات است که انسان‌ها با به کار بردن آن در گفتار یا نوشتار، ممکن است هدف و منظوری متفاوت با آنچه بیان می‌شود داشته باشند زیرا این ماهیت خلاقانه مانع از درک صحیح متن می‌شود.

با گسترش استفاده از اینترنت، استفاده از شبکه‌های اجتماعی و وبسایت‌های فروش اینترنتی افزایش پیدا کرده است. با مرسوم شدن اعلام دیدگاه‌ها در این شبکه‌ها یا بیان نظرات در مورد کالاهایی که در

وبسایت‌ها به فروش گذاشته شده‌اند، بررسی نظرات و احساسات کاربران در این موارد برای شرکت‌ها و سازمان‌ها اهمیت شایانی پیدا می‌کند. چون معمولاً این نظرات با زبان رسمی و به صراحت اعلام نمی‌شوند و گاهی آغشته به شوخی، طعنه و کنایه هستند، کارایی تحلیل احساسات تحت تاثیر قرار می‌گیرد. برای مثال جمله «مرسی برای این همه بدبختی، خدایا شکرت!» حاوی طنز است در حالی که جمله «من امروز خیلی خوشحالم. دمت گرم روزم رو ساختی» بدون طنز و جدی است.

در سال‌های اخیر، توییت‌ها به منبع بزرگی از ابراز ایده‌ها و دیدگاه‌های کاربران در تقریباً تمامی زمینه‌ها تبدیل شده است. این مسئله باعث جلب توجه شرکت‌ها و پژوهشگرانی به توییت‌ها است که در زمینه تحلیل نظرات کاربران فعالیت می‌کنند. درصد بالایی از توییت‌ها شامل طنز هستند و کاربران فارسی‌زبان نیز از این قاعده مستثنی نمی‌شوند. تحلیل‌هایی که به وجود شوخی در متن آگاه باشند، ممکن است بتوانند با دقت بهتری احساسات و قطبیت متن را پیش‌بینی کنند. مسئله تشخیص طنز، مسئله‌ی دسته‌بندی است و نمونه‌ها باید با یکی از دو برچسب ۱ و ۰ که به ترتیب نشان‌دهنده متن طنز و متن جدی است دسته‌بندی شوند.

در این پژوهش نوآوری‌هایی برای حل مسئله تشخیص طنز در زبان فارسی ارائه می‌شود:

- معرفی دادگان جدید برای تشخیص طنز در زبان فارسی که به صورت خودکار برچسب‌زده شده‌اند،
- ارائه مدل‌هایی که از تطبیق دقیق<sup>۱</sup> مدل‌های زبانی از پیش آماده‌شده بر روی دادگان به دست آمدند،
- تحلیل و ارزیابی روش‌های پیشنهادی

فصل بعدی، بررسی پیشینه پژوهش مسئله را شامل می‌شود. در فصل سوم راهکارهای پیشنهادی برای حل مسئله معرفی می‌شوند. در فصل چهارم به معرفی دادگان استفاده شده در پژوهش و چگونگی جمع‌آوری آن می‌پردازیم. آزمایش‌های انجام شده و نتایج آن‌ها در فصل پنجم تحلیل شده و نتیجه‌گیری و پیشنهادهایی برای کارهای آینده در فصل ششم قرار گرفته است.

## ۲ مروری بر کارهای دیگران

نظر به این که پژوهش‌های انجام شده برای تشخیص طنز در زبان فارسی محدود است، برای شناخت ایده‌های مشابه ابتدا به بررسی تشخیص طنز در سایر زبان‌ها می‌پردازیم و سپس کارهای انجام شده بر روی زبان فارسی را بررسی می‌کنیم.

پژوهش‌های قدیمی‌تر از مجموعه ویژگی‌های حاصله از متن به کمک الگوریتم‌های یادگیری ماشین برای دسته‌بندی متون به طنز و جدی استفاده کرده‌اند. از این دسته راهکارها می‌توان به [۲۱] و [۲] اشاره کرد که تنها با ۴ و ۷ ویژگی اقدام به تشخیص طنز کرده‌اند. این راهکارها عموماً متن را در نظر نمی‌گیرند.

<sup>1</sup>Fine tuning

بعضی پژوهش‌ها با عنایت به زمینه‌ی متن به تشخیص طنز موجود در متن پرداختند. برای این کار ویژگی‌هایی از نویسنده متن (یا توییت) و یا نوشته‌های پیشین وی استخراج می‌کنند. [۱۹] در کنار این ویژگی‌ها، به تحلیل ویژگی‌های روان‌شناسی و رفتاری نویسنده می‌پردازد. مانند آنچه در [۲] و [۲۲] استفاده شد، این ویژگی‌ها می‌توانند از تعاملی که سایر کاربران با نوشته دارند، باشد. محدودیتی که این روش‌ها ایجاد می‌کنند به دلیل اطلاعات بیشتری است که برای پردازش نیاز دارند و جمع‌آوری دادگانی با این ویژگی‌ها آسان نیست.

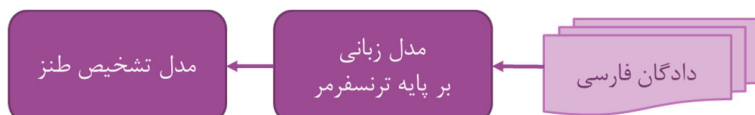
با گسترش استفاده از تکنیک‌های یادگیری عمیق برای حل مسائل پردازش زبان طبیعی، بیشتر پژوهش‌های اخیر از این روش‌ها برای تشخیص طنز در متن استفاده می‌کنند. پژوهش [۱۱] با یادگیری انتقالی از شبکه‌ای عمیق که برای مسئله دسته‌بندی صورتک از پیش آموزش دیده شده بود، به تشخیص طعنه پرداخت. امیر و همکاران [۱] ویژگی‌های نویسنده متن را بر اساس فعالیت‌های قبلی استخراج می‌کرد. در مقاله [۱۲] شبکه‌ای تشکیل شده از CNN و LSTM که در دنبال آن قرار می‌گرفت معرفی شد تا تنها بر اساس متن وجود طنز را تشخیص دهد. ژانگ و همکاران به صورت خودکار با استفاده از شبکه عمیق GRU دو سویه، ویژگی‌های معنایی و محتوایی را استخراج می‌کرد. [۲۳] با در نظر گرفتن ویژگی‌های مربوط به نویسنده توییت و متن توییت، مقاله [۱۴] روشی ترکیبی بر اساس محتوا و زمینه متن به کمک شبکه CNN ارائه کردند. کومار و همکاران در [۱۵] به کمک بازنمایی برداری GloVe [۱۸] و استخراج ویژگی‌هایی چون علائم نگارشی استفاده شده، مدل ترکیبی از BiLSTM بر اساس توجه و CNN معرفی کردند.

بدین جهت که شبکه‌های یاد شده برای عملکرد مناسب از دادگانی در مرتبه میلیون توییت استفاده کرده‌اند، روش پیشنهادی محدودیت‌های این شبکه‌ها را در نظر می‌گیرد. مورد دیگری که در این پژوهش به آن توجه می‌شود، استفاده از مدل‌های زبانی که اخیراً معرفی شده‌اند و مرز دانش هستند، به جای روش‌های تعبیه کلمات قدیمی استفاده شده در پژوهش‌های پیشین است.

SemEval مجموعه کارگزارهای پژوهشی و بین‌المللی در حوزه پردازش زبان طبیعی است که هر ساله به چالش‌های تعدادی از مسئله‌های پردازش زبان طبیعی می‌پردازد. یکی از مسئله‌هایی که تاکنون در این محفل بررسی شده است، مسئله‌ی تشخیص طعنه در زبان انگلیسی و عربی است. بیشتر شرکت‌کنندگان در این پژوهش راهکارهای خود را به کمک مدل‌های از پیش آموزش دیده بر پایه ترنسفرمر ارائه نموده‌اند. [۱۰] ما نیز در این پژوهش از رویکردهای مشابه برای زبان فارسی استفاده می‌کنیم.

تلاش‌های انجام شده بر روی زبان فارسی در پژوهش‌های [۱۷] و [۱۳] دیده می‌شود. بکایی‌نژاد و همکاران در مقاله [۱۷] مدلی بر روی دادگانی از ۲۵۰۰ توییت ارائه دادند. پس از پیش‌پردازش و آماده‌سازی دادگان، ویژگی‌های قطبیت متن، استفاده از علائم نگارشی و ... را استخراج کردند و از آن‌ها برای آموزش مدل‌ها استفاده کردند. در ارزیابی مدل‌های بررسی شده، مدلی بر اساس ماشین بردار پشتیبان با  $F1 = 78\%$  بالاترین مقدار را داشت. در این پژوهش متن به عنوان ویژگی در الگوریتم‌های دسته‌بندی استفاده نمی‌شود و برای دسته‌بندی تنها به چند ویژگی محدودی که از متن استخراج کرده‌اند اکتفا می‌کند اما در این پژوهش قصد داریم از متن توییت در الگوریتم تشخیص استفاده کنیم.

گل‌عزیزیان و همکاران در مقاله [۱۳] با استفاده از دو شبکه عمیق و یادگیری انتقالی، تشخیص شوخی



شکل ۱: راهکار پیشنهادی برای مسئله تشخیص طنز در زبان فارسی؛ تطبیق دقیق مدل زبانی بر پایه ترنسفرمر بر دادگان تشخیص طنز به زبان فارسی مدلی برای تشخیص طنز زبان فارسی ارائه می‌دهد.

در زبان فارسی را انجام دادند که نتیجه آن  $F1 = 83\%$  بود. شبکه اول برای مسئله‌ی پیش‌بینی صورتک و شبکه دوم برای تشخیص طنز ارائه شده بود. در این پژوهش از فست‌تکست [۴] برای تعبیه جملات استفاده شده است. با توجه به این که شبکه اول شخصی‌سازی شده است، در این پژوهش سعی داریم با راهکار عمومی‌تری مسئله را بررسی کنیم همچنین به عنوان جایگزینی برای روش فست‌تکست از تکنیکی با کارایی بیشتر برای تبدیل متن به بردار استفاده کنیم.

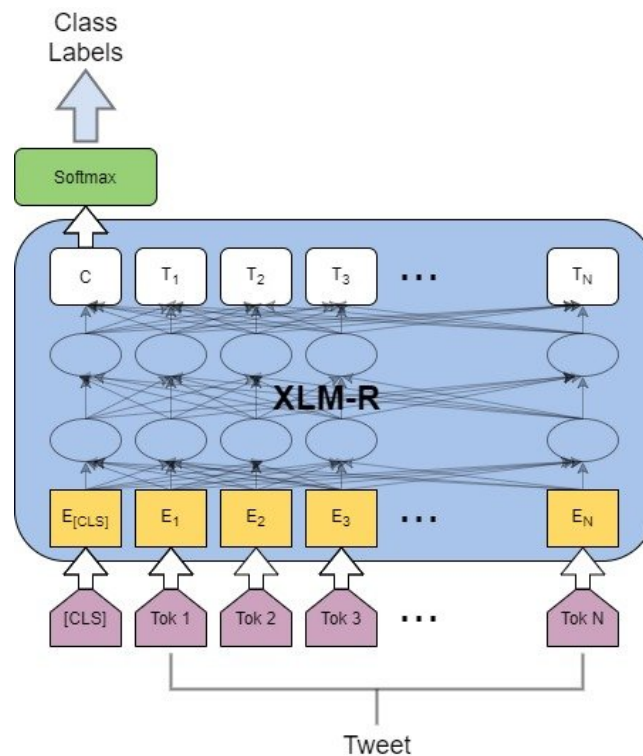
### ۳ راهکار پیشنهادی

پس از معرفی مکانیزم توجه و معماری ترنسفرمر [۷] و مدل زبانی برت [۵] که بر پایه ترنسفرمر بود، مدل‌های زبانی دیگری با معماری مشابهی نسبت به برت توسعه داده شدند که در بسیاری از مسائل پردازش زبان طبیعی عملکرد بهتری از خود نشان می‌دادند. پژوهش‌های انجام شده برای تشخیص طنز و طعنه در زبان‌های دیگر [۱۰] نشان از کارایی مدل‌های زبانی بر اساس ترنسفرمرها دارد به همین دلیل در ادامه راهکارهایی را با استفاده از مدل‌های زبانی مختلفی که بر پایه ترنسفرمر هستند برای حل مسئله تشخیص طنز و طعنه در زبان فارسی بررسی می‌کنیم.

به عنوان راهکار اول، تطبیق دقیق مدل‌های زبانی مختلف را برای مسئله‌ی دسته‌بندی بررسی می‌کنیم. از میان مدل‌های موجود، به بررسی مدل زبانی پارس‌برت [۹] که تنها بر روی پیکره‌ای از متن رسمی زبان فارسی و با معماری مدل BERTBase [۵] از پیش آموزش دیده شده است و دو مدل زبانی -XLM-RoBERTaBase و XLM-RoBERTaLarge که چندزبانه هستند می‌پردازیم. این دو مدل به ترتیب با معماری BERTBase و BERTLarge بر روی پیکره‌ای متشکل از ۱۰۰ زبان که هر کدام شامل متون‌هایی به زبان رسمی و محاوره بودند، پیش‌آموزش دیده شده است [۶] [۱۶]. در شکل ۱ شمایی از راهکار پیشنهادی دیده می‌شود که نشان می‌دهد برای استفاده از مدل‌های زبانی بر پایه ترنسفرمر مدل از پیش‌آموزش دیده شده را با دادگان توییت‌های فارسی تطبیق دقیق می‌دهیم تا مدلی برای تشخیص طنز در زبان فارسی حاصل شود. در شکل ۲ معماری دسته‌بندی برای مسئله تشخیص طنز به کمک مدل زبانی بر پایه ترنسفرمر مشاهده می‌شود.

مقاله [۸] نشان می‌دهد، تطبیق دقیق مدل‌های زبانی بر پایه ترنسفرمرها بر روی مسئله‌های متفاوت، عملکردی یادگیری بدون نمونه را افزایش می‌دهد. به عنوان راهکار دوم برای تشخیص متن حاوی طنز، تاثیر دادگان با نمونه‌هایی از زبان‌های دیگر را بررسی می‌کنیم. برای این کار پیکره‌ای که از چند دادگان تشخیص





شکل ۲: معماری روش پیشنهادی برای دسته‌بندی بر پایه ترنسفرمر [۲۰]

طنز و طعنه به زبان‌هایی غیر از زبان فارسی تشکیل شده‌است، همراه با مدل زبانی XLM-RoBERTa استفاده می‌کنیم و نتایج مدل به دست آمده را بر دادگان فارسی بررسی می‌کنیم. این روش مشابه یادگیری بدون نمونه است. چون در مرحله‌ی تطبیق دقیق اول، مدل نمونه‌ای از دسته‌های حاوی طنز و بدون طنز از زبان فارسی نمی‌بیند. بعد از این کار، بررسی نتایج را با تطبیق دقیق روی دادگان فارسی ادامه می‌دهیم و نتایج به دست آمده را مقایسه می‌کنیم.

## ۴ دادگان

دو پژوهش انجام شده در حوزه تشخیص طنز و طعنه فارسی هر کدام از دادگانی فارسی برای کار خود استفاده کرده‌اند. نمونه‌های دادگان یاد شده در [۱۷] که به واسطه هشتگ‌های استفاده‌شده در متن توییت برجسب‌دار بودند، به کمک نیروی انسانی نیز بررسی شده‌اند اما متأسفانه این دادگان در دسترس نیست. نمونه‌ها در دادگان تشخیص طنز فارسی که در [۱۳] معرفی شده‌است، به کمک نیروی انسانی برجسب‌گذاری شده‌اند. این دادگان کمتر از ۳,۰۰۰ توییت را شامل می‌شود و همین‌طور به دلیل مشخص نبودن دادگان آموزش و آزمایش، نمی‌توانیم روش معرفی شده بر روی این دادگان را با روش‌های پیشنهادی این پژوهش

جدول ۱: جدول جزئیات دادگان معرفی شده

ویژگی	طنز	بدون طنز
تعداد توییت	۷,۰۱۴	۷,۹۳۲
میانگین طول توییت	۳۰	۴۵
طول بیشینه توییت	۲۶۰	۴۳۰

مقایسه کنیم. در نهایت به دلیل این کمبودها بر آن شدیم دادگانی مناسب و غنی با نمونه‌های بیشتر برای حل مسئله تشخیص طنز و طعنه در زبان فارسی و به طور اختصاصی از توییت‌ها ارائه دهیم. تجربه [۱۳] برای جمع‌آوری و برچسب زدن داده، بیان می‌کرد نرخ پیام‌های طنز در کانال تلگرامی «توییت فارسی» بیشتر از توییت‌های روزمره است. نظر به این که به‌روزرسانی پیام‌رسان تلگرام از تاریخ ۳۰ دسامبر ۲۰۲۱ برای هر پیام اجازه ثبت واکنش را از طریق انتخاب یکی از صورتک‌های « 😊 👍 🗨️ ❤️ 😞 » به کاربران تلگرامی می‌دهد، بر آن شدیم که دادگانی از توییت‌ها را از این کانال در پیام‌رسان تلگرام جمع‌آوری کنیم.

به دلیل کمبود تعداد واکنش‌های ثبت‌شده برای پیام‌هایی که زمان ارسال آن‌ها با به‌روزرسانی اخیر تلگرام فاصله زیادی دارد، از مجموع ۱۲۹,۵۳۶ پیام یکتا که از کانال توییت فارسی دریافت شد، تنها به ۳۱,۹۸۳ پیام که در بازه‌ی زمانی ابتدای دسامبر ۲۰۲۱ تا ۲۵ آگوست ۲۰۲۲ ارسال شده بودند اکتفا کردیم. از میان این پیام‌ها، از در نظر گرفتن آن‌هایی که ویدئو یا تصویر همراه خود دارند نیز صرفه نظر کردیم.

برای دادگانی که به برچسب‌زنی دستی نیاز دارند، برچسب‌زن‌ها طبق مجموعه‌ای از قوانین که معمولاً زبان‌شناسان مشخص می‌کنند، اقدام به اختصاص دسته به هر نمونه می‌کنند. در انتها میانگینی از برچسب‌های اختصاص داده شده، دسته هر نمونه را مشخص می‌کند. نظر به ماهیت خلاقانه طنز، زبان‌شناسان قادر نیستند قوانینی کلی برای تشخیص آن وضع کنند و همین مسئله‌ی برچسب‌زدن را دشوارتر می‌سازد؛ ضمن این که برچسب زدن به خودی خود فرایندی زمان‌گیر است. واکنش‌های ثبت‌شده برای هر پیام می‌تواند نشان‌دهنده برچسب‌هایی باشد که کاربران تلگرام به هر پیام اختصاص داده‌اند. می‌توانیم این مسئله را برچسب‌گذاری با تعداد زیادی برچسب‌زن ببینیم که پیام‌ها را خوانده‌اند و در صورتی که متوجه طنز آشکار یا پنهان پیام شده‌اند از واکنش « 😊 » برای بیان نظرشان استفاده کرده‌اند.

برای ۱۳۳,۱۸ پیام باقی‌مانده تا این مرحله، راهکاری خودکار برای اختصاص برچسب اعمال کردیم. این فرایند که برای هر نمونه بر اساس دو واکنشی که تکرار بیشینه داشتند انجام می‌شد، به پیام‌هایی که بیشترین واکنش آن‌ها « 😊 » بود برچسب ۱ به نشانه طنز اختصاص می‌داد. اگر بیشترین واکنش ثبت‌شده برای نمونه‌ای « 👍 » باشد درحالی که واکنش دوم از نظر تعداد صورتک « 😊 » است، مرز تشخیص طنز و جدی ساده نیست و این دسته پیام‌ها را نادیده می‌گیریم. سایر پیام‌ها برچسب ۰ به نشانه پیامی جدی دریافت می‌کنند. در جدول ۱ جزئیات مربوط به دادگان معرفی شده و در جدول ۲ نمونه‌هایی از این دادگان مشاهده می‌شود.

## جدول ۲: جدول نمونه‌هایی از دادگان معرفی شده همراه با برچسب

توییت	برچسب
پشت به کامیونه نوشته بود: سلطان خیانت هیدروژن! هم پیوند کوالانسی میگیره هم هیدروژنی! فکر کنم رانندش لیسانس شیمی داشته 😞😓👤	۱
آره مهاجرت خوبه ولی قشنگترش این بود که همینجا کنار خانواده و دوستانمون به خواسته‌هایی که داشتیم برسیم:	۰
تاس کباب داشتیم بابام جفت شیش آورد همه‌شو خورد	۱
مدیون تاول های پامون تو راه اشتباه نباشیم! هر جا که فهمیدیم مسیر درست را انتخاب نکردیم، بدون تردید دور بز نیم و برگردیم!	۰

برای اجرای راهکار پیشنهادی دوم، پیکره تشخیص طنز و طعنه را از دادگان تشخیص طنز یا طعنه به زبان‌های انگلیسی، پرتغالی، برزیل، عربی و هندی را گرد هم آوردیم که شامل ۹۴۴۲۸ توییت یکتا است که از این تعداد، ۶۵۷۱۱ توییت طنز هستند.

## ۵ آزمایش‌ها

در این بخش به آزمایش‌هایی که برای بررسی راهکارهای پیشنهادی انجام شده‌اند، می‌پردازیم. برای اجرای آزمایش‌های از پیکره چند زبانه تشخیص طنز و دادگان فارسی معرفی شده که هر دو در فصل چهارم بررسی شدند استفاده می‌شود. برای آموزش و ارزیابی مدل‌ها، دادگان تشخیص طنز در زبان فارسی را به تصادف با نسبت ۸ به ۲ به قسمت‌های آموزش و آزمایش تقسیم شدند. معیارهای دقت، صحت، فراخوانی و  $F1$  برای ارزیابی و مقایسه مدل‌ها به ما کمک می‌کنند.

### ۱.۵ مدل‌های پایه

برای مقایسه عملکرد روش‌های پیشنهادی، به مدل‌های پایه نیاز داریم. از الگوریتم‌های یادگیری ماشین به عنوان مدل پایه استفاده می‌کنیم.

الگوریتم نایبو بیز، ماشین بردار پشتیبان و مدل شبکه عصبی چندلایه را همراه با روش tfidf به عنوان راهکاری برای تبدیل متن به بردار استفاده می‌کنیم.

برای الگوریتم نایبو بیز از روش گاوسی بهره‌بردیم و برای الگوریتم ماشین بردار پشتیبان از هسته تابع پایه‌ای شعاعی استفاده کردیم. در الگوریتم پرسپترون چندلایه، شبکه‌ای با دو لایه پنهان که هر لایه شامل ۵۰ گره است مورد استفاده قرار گرفت. این شبکه با تابع تانژانت هیپربولیک فعال‌سازی می‌شد و با تابع آدام بهینه‌سازی صورت می‌گرفت.

در میان سه الگوریتم یاد شده، الگوریتم ماشین بردار پشتیبان با  $F1 = 79\%$  عملکرد بهتری از خود نشان داد.

## ۲.۵ آزمایش‌های روش تطبیق دقیق مدل‌های زبانی بر پایه ترنسفرمر

به عنوان روش پیشنهادی اول، از مدل‌های زبانی بر پایه ترنسفرمر استفاده شد. مدل زبانی پارس‌برت و دو نسخه مدل زبانی XLM-RoBERTa ترنسفرمرهای انتخابی هستند. هر کدام از این ترنسفرمرهای مورد نظر، بر روی قسمت آموزش دادگان تطبیق دقیق داده شدند. از میان سه مدل زبانی انتخابی، نسخه بزرگ XLM-RoBERTa با معیار  $F1$  برابر با  $84/6\%$  کارایی بهتری را نمایش می‌دهد.

## ۳.۵ آزمایش‌های روش آموزش بدون نمونه

روش پیشنهادی دیگر، استفاده از پیکره متشکل از چندین زبان غیر از زبان فارسی است. برای انجام این آزمایش، تطبیق دقیق مدل زبانی XLM-RoBERTa بزرگ را بر روی پیکره چندزبانه انجام می‌دهیم. این مدل زبانی به دلیل چندزبانه بودن و پیش‌آموزش بر روی صد زبان که هر چهار زبان پیکره طنز و طعنه چندزبانه گردآوری شده را شامل می‌شود، انتخاب شده است. مدل حاصله را بر روی بخش آزمایش دادگان فارسی معرفی شده ارزیابی شد. مدلی که هیچ نمونه‌ای حاوی شوخی یا بدون شوخی از زبان فارسی را ندیده است، می‌تواند با دقت  $70/6\%$  مقدار  $F1$  برابر با  $70/6\%$  کسب کند. مدل زبانی که در این مرحله به دست آمده را بر روی دادگان فارسی معرفی شده نیز تطبیق دقیق داده شد. مدل نهایی می‌تواند وجود طنز و طعنه در قسمت آزمایش دادگان را با دقت و  $F1$  برابر با  $84/5\%$  پیش‌بینی کند.

## ۴.۵ مقایسه نتایج

در روش‌هایی که مدل از تطبیق دقیق مدل‌های زبانی بر روی دادگان فارسی به دست می‌آید، می‌توانیم مدل‌ها را از دو دیدگاه بررسی کنیم؛ دیدگاه پیکره‌ای که مدل بر آن از پیش آموزش دیده شده است و دیدگاه معماری. در دیدگاهی که به تعداد زبان و حجم پیکره برای پیش‌آموزش توجه می‌شود، نتایج آزمایش‌ها نشان می‌دهد استفاده از مدل چندزبانه عملکرد بهتری نسبت به مدل زبانی که تنها بر روی زبان فارسی از پیش آموزش دیده شده است دارد. کارایی دو مدل چندزبانه می‌تواند به دلیل حجم بزرگ‌تر پیکره‌ای باشد که بر روی آن آموزش دیده شده‌اند. با توجه به این که پیکره این مدل زبانی چندزبانه شامل نمونه‌هایی از متون با زبان محاوره و عامیانه می‌شود، دقت بالاتر این دو مدل زبانی برای مسئله‌ای که نمونه‌های آن لزوماً به زبان فارسی رسمی نوشته نشده‌اند نسبت به پارس‌برت با پیکره‌ای که غالباً به زبان فارسی رسمی است، توجیه می‌شود. از دیدگاه معماری، مدل زبانی XLM-RoBERTa بزرگ با داشتن تعداد پارامترهای بیشتر، کارایی بهتری از خود نشان می‌دهند. به همین دلیل از میان آزمایش‌های تطبیق دقیق مدل‌های زبانی بر پایه ترنسفرمر بر دادگان فارسی، استفاده از نسخه بزرگ مدل زبانی XLM-RoBERTa عملکرد بهتری برای تشخیص طنز بر روی قسمت آزمایش دادگان فارسی معرفی شده دارد.

در آزمایشی که مدل زبانی XLM-RoBERTa بزرگ در دو مرحله بر روی دو پیکره تشخیص طنز چندزبانه و دادگان تشخیص طنز فارسی تطبیق دقیق داده می‌شود، می‌بینیم نتیجه معیارهای ارزیابی با حالتی که تنها بر روی دادگان زبان فارسی تطبیق دقیق انجام می‌شود تفاوتی کمتر از  $0/3\%$  دارد و به نظر

جدول ۳: نتایج آزمایش‌های انجام شده بر روی دادگان فارسی معرفی شده

آزمایش	دقت	فراخوانی	صحت	F1
نایبو بیز	۶۶٪	۶۸٪	۶۷٪	۶۵٪
ماشین بردار پشتیبان	۷۹٪	۷۸٪	۷۹٪	۷۹٪
شبکه پرسپترون چندلایه	۷۳٪	۷۳٪	۷۳٪	۷۳٪
پارس برت، نسخه ۳	۸۱.۳٪	۸۱.۴٪	۸۱.۳٪	۸۱.۳٪
XLM-RoBERTaBase	۸۲.۶٪	۸۲.۸٪	۸۲.۶٪	۸۲.۵٪
XLM-RoBERTaLarge	۸۴.۷٪	۸۴.۷٪	۸۴.۶٪	۸۴.۶٪
پیش‌آموزش دیده بر روی سایر زبان‌ها	۷۰.۶٪	۷۰.۷٪	۷۰.۶٪	۷۰.۶٪
تطبیق دقیق مدل پیش‌آموزش دیده بر روی سایر زبان‌ها بر روی دادگان فارسی	۸۴.۵٪	۸۴.۶٪	۸۴.۴٪	۸۴.۵٪

می‌رسد استفاده از دادگان زبان‌های دیگر برای تطبیق دقیق هنگامی که از مدل زبانی چندزبانه استفاده می‌شود، تاثیر مثبتی در عملکرد تشخیص طنز زبان فارسی ندارد.

جزئیات ارزیابی هر یک از آزمایش‌های بیان شده در قسمت‌های ۱.۵ تا ۳.۵ در جدول ۳ دیده می‌شود. از میان آزمایش‌ها بر روی مدل پایه، مدل‌های زبانی بر پایه ترنسفرمر و روش استفاده از پیکره تشخیص طنز زبان‌های دیگر، تطبیق دقیق نسخه بزرگ مدل زبانی XLM-RoBERTa بر روی دادگان فارسی با کسب مقدار ۸۴.۶٪ برای معیار  $F1$  عملکرد بهتری برای تشخیص طنز موجود در قسمت آزمایش دادگان فارسی معرفی شده داشته است.

## ۶ نتیجه‌گیری و کارهای آینده

در این پژوهش ضمن معرفی دادگان جدیدی برای تشخیص طنز در زبان فارسی، دو راهکار کلی برای تشخیص طنز در زبان فارسی ارائه شد. هر دو این روش‌ها با تطبیق دقیق مدل‌های زبانی بر پایه ترنسفرمرها بر روی دادگان معرفی شده و پیکره گردآوری شده از چهار زبان دیگر، مدل‌هایی برای تشخیص طنز در زبان فارسی ارائه می‌دهند. از میان مدل‌های پیشنهادی و آزمایش شده، مدل حاصله از تطبیق دقیق مدل زبانی XLM-RoBERTaLarge بر روی دادگان معرفی شده، بهترین عملکرد را داراست. این مدل بر روی قسمت آزمایش دادگان فارسی معرفی شده می‌تواند با دقت ۸۴.۷٪ و ۸۴.۶٪ وجود طنز در متن فارسی را تشخیص دهد. از آنجایی که یکی از اهداف تشخیص طنز در متن، افزایش عملکرد مدل‌های تحلیل احساسات است، بررسی تاثیر وجود ویژگی که نشان دهد نمونه طنز است یا خیر در کنار متن و سایر ویژگی‌هایی که برای تشخیص قطبیت متن در مسئله خاصی استفاده می‌شود، می‌تواند یکی از کارهای آینده در این زمینه باشد. روش ارائه شده برای جمع‌آوری دادگان می‌تواند به صورت خودکار فرایند برچسب‌زنی را نیز انجام دهد. این روش راه‌اندازی سیستم‌هایی که نیاز به بروزرسانی مداوم مدل را دارند تسهیل می‌بخشد و باعث می‌شود مدل با نمونه‌های طنز تازه‌ای آشنا شود که به خاطر ذات خلاقانه طنز به مرور زمان ایجاد شده‌اند.

## سپاس‌گزاری

اجرای آزمایش‌های مربوط به مدل‌های زبانی بر پایه ترنسفرمر بر روی واحد پردازش گرافیکی به زمان کمتری نیاز دارد. از شرکت دادماتک که سخت‌افزار مورد نیاز اجرای آزمایش‌های این پژوهش را در اختیارمان قرار داد سپاس‌گزاریم.

## مراجع

- [1] AMIR, S., WALLACE, B. C., LYU, H., AND SILVA, P. C. M. J. “Modelling context with user embeddings for sarcasm detection in social media”. *arXiv preprint arXiv:1607.00976* 20, 5 (2016), 1924–1939.
- [2] BAMMAN, D., AND SMITH, N. “Contextualized sarcasm detection on twitter”. *proceedings of the international AAAI conference on web and social media* 9, 1 (2015), 574–577.
- [3] BARBIERI, F., SAGGION, H., AND RONZANO, F. “Modelling sarcasm in twitter, a novel approach”. *proceedings of the 5th workshop on computational approaches to subjectivity, sentiment and social media analysis* (2014), 50–58.
- [4] BOJANOWSKI, P., GRAVE, E., JOULIN, A., AND MIKOLOV, T. “Enriching word vectors with subword information”. *Transactions of the association for computational linguistics* 5 (2017), 135–146.
- [5] DEVLIN, J., CHANG, M.-W., LEE, K., AND TOUTANOVA, K. “Enriching word vectors with subword information”. *arXiv preprint arXiv:1810.04805* (2018).
- [6] ET AL., A. C. “Unsupervised cross-lingual representation learning at scale”. *arXiv preprint arXiv:1911.02116* (2019).
- [7] ET AL., A. V. “Attention is all you need”. *Advances in neural information processing systems* 30 (2017).
- [8] ET AL., J. W. “Finetuned language models are zero-shot learners”. *arXiv preprint arXiv:2109.01652* (2021).
- [9] FARAHANI, M., GHARACHORLOO, M., FARAHANI, M., AND MANTHOURI, M. “Parsbert: Transformer-based model for persian language understanding”. *Neural Processing Letters* 53, 6 (2021), 3831–3847.
- [10] FARHA, I. A., OPREA, S. V., WILSON, S., AND MAGDY, W. “SemEval-2022 Task 6: iSarcasmEval, Intended Sarcasm Detection in English and Arabic”. *Proceedings of the 16th International Workshop on Semantic Evaluation (SemEval-2022)* (2022), 802–814.
- [11] FELBO, B., MISLOVE, A., SOGAARD, A., RAHWAN, I., AND LEHMANN, S. “Using millions of emoji occurrences to learn any-domain representations for detecting sentiment, emotion and sarcasm”. *arXiv preprint arXiv:1708.00524* (2017).



- [12] GHOSH, A., AND VEALE, T. “Fracking sarcasm using neural network”. *Proceedings of the 7th workshop on computational approaches to subjectivity, sentiment and social media analysis* (2016), 161–169.
- [13] GOLAZIZIAN, P., SABETI, B., ASLI, S. A. A., MAJDABADI, Z., MOMENZADEH, O., AND FAHMI, R. “Irony detection in Persian language: A transfer learning approach using emoji prediction”. *Proceedings of The 12th Language Resources and Evaluation Conference* (2020), 2839–2845.
- [14] HAZARIKA, D., PORIA, S., GORANTLA, S., CAMBRIA, E., ZIMMERMANN, R., AND MIHALCEA, R. “Cascade: Contextual sarcasm detection in online discussion forums”. *arXiv preprint arXiv:1805.06413* (2018), 1490–1498.
- [15] KUMAR, A., SANGWAN, S. R., ARORA, A., NAYYAR, A., AND ABDEL-BASSET, M. “Sarcasm detection using soft attention-based bidirectional long short-term memory model with convolution network”. *IEEE access* 7 (2019), 23319–23328.
- [16] LAMPLE, G., AND CONNEAU, A. “Cross-lingual language model pretraining”. *arXiv preprint arXiv:1901.07291* (2019).
- [17] NEZHAD, Z. B., AND DEIHIMI, M. A. “Sarcasm detection in Persian”. *Journal of Information and Communication Technology* 20, 1 (2021), 1–20.
- [18] PENNINGTON, J., SOCHER, R., AND MANNING, C. D. “Glove: Global vectors for word representation”. *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)* (2014), 1532–1543.
- [19] RAJADESINGAN, A., ZAFARANI, R., AND LIU, H. “Sarcasm detection on twitter: A behavioral modeling approach”. *Proceedings of the eighth ACM international conference on web search and data mining* (2015), 97–106.
- [20] RANASINGHE, T., GUPTA, S., ZAMPIERI, M., AND NWOGU, I. “Wlv-rit at hasoc-dravidian-codemix-fire2020: Offensive language identification in code-switched youtube comments”. *arXiv preprint arXiv:2011.00559* (2020).
- [21] REYES, A., ROSSO, P., AND VEALE, T. “A multidimensional approach for detecting irony in twitter”. *Language resources and evaluation* 47, 1 (2013), 239–268.
- [22] WALLACE, B. C., AND CHARNIAK, E. “Sparse, contextually informed models for irony detection: Exploiting user communities, entities and sentiment”. *Proceedings of the 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing (Volume 1: Long Papers)* (2015), 1035–1044.
- [23] ZHANG, M., ZHANG, Y., AND FU, G. “Tweet sarcasm detection using deep neural network”. *Proceedings of COLING 2016, the 26th International Conference on Computational Linguistics: technical papers* (2016), 2449–2460.



## اصول سیستم‌های سبیرنتیکی و انطباق آن با مراکز اطلاع‌رسانی

نعیمه ظریف قاسمیان<sup>۱</sup>، حسن بهزادی<sup>۲</sup>

<sup>۱</sup> دانشجوی دکتری، گروه علم اطلاعات و دانش‌شناسی، دانشگاه فردوسی مشهد، مشهد، ایران  
naeemehzarif@gmail.com

<sup>۲</sup> استادیار گروه علم اطلاعات و دانش‌شناسی، دانشگاه فردوسی مشهد، مشهد، ایران  
hasanbehzadi@um.ac.ir

### چکیده

اصول و قوانین، نقش بیان اساسی‌ترین ایده‌ها را در یک علم و نیز ایجاد چارچوب و روش‌شناسی برای حل مسائل آن علم، بازی می‌کنند. این مقاله بر آن است تا با گذری بر مفاهیم و اصول سبیرنتیک به بررسی انطباق این اصول در مرکز اطلاع‌رسانی بپردازد. در نگارش مقاله رویکرد مروری تحلیلی مورد استفاده قرار گرفته و تلاش شده است تا با بررسی متون علمی این حوزه از طریق روش کتابخانه‌ای، ابتدا گذری بر مفاهیم و اصول سبیرنتیک صورت پذیرد، سپس انطباق این اصول با مراکز اطلاع‌رسانی بررسی شود. یافته‌های این پژوهش بیانگر آن است که مراکز اطلاع‌رسانی، خصوصیات و اصول سیستم‌های سبیرنتیکی را دارا هستند. انطباق مراکز اطلاع‌رسانی با اصول سیستم‌های سبیرنتیکی می‌تواند نگرش و بینش عمیق‌تری نسبت به شناسایی مشکلات و چالش‌های این مراکز به دست بدهد و زمینه را جهت ارتقای عملکرد این سازمان‌ها فراهم نماید. به دلیل دارا بودن ماهیتی بین‌رشته‌ای در علم اطلاعات و دانش‌شناسی، این رشته می‌تواند با بهره‌گیری از این اصول و انطباق آن با مراکز اطلاع‌رسانی ضمن بهبود وضعیت فعلی نسبت به بنیان‌اندیشه‌های خود بر اساس اصول سبیرنتیک اقدام نموده و از آن بهره‌بردارد.

**کلمات کلیدی:** سبیرنتیک، اصول سیستم‌های سبیرنتیکی، مراکز اطلاع‌رسانی، قوانین سبیرنتیک، کتابخانه‌ها.

### ۱ مقدمه

وظیفه هر علمی شناخت جهان بر پایه حقایق است و نقطه آغاز آن پذیرش همبستگی متقابل بین تمامی پدیده‌ها و هدف آن یافتن روابط موجود و توجیه آنها بر پایه عینیات است [۱۱]. در قرن اخیر با کم‌رنگ‌تر شدن مرز بین علوم مختلف و کم شدن فاصله زمانی میان پژوهش علمی و کاربردهای علمی آن در زندگی بشر، دانش‌های میان‌رشته‌ای زیادی پا به عرصه وجود گذاشته‌اند. سبیرنتیک علاوه بر اینکه علمی فرا رشته‌ای است، علمی میان رشته‌ای نیز است که در بسیاری حوزه‌ها کاربرد دارد و از ترکیب آن با علوم دیگر می‌توان

رشته‌ای جدید ایجاد کرد. به این ترتیب سیبرنتیک ارتباط بین علوم را تسهیل می‌کند. سیبرنتیک را علمی ابر رشته‌ای و علمی درباره علوم دیگر نیز می‌دانند. زیرا به نقد و بررسی اشکال مختلف دانش و شباهت‌ها و تفاوت‌های حوزه‌های متنوع علمی می‌پردازد و دانشمندان همه علوم را مدلساز، کنترل‌کننده و پیش‌بینی‌کننده می‌پندارد [۱۸].

نوربرت وینر به عنوان بیانگذار علم سیبرنتیک، آن را علم کنترل و ارتباط در حیوان و ماشین می‌داند [۹]. بنابراین، نظر به اینکه کنترل ارتباط انسان و فناوری‌های اطلاعاتی را می‌توان از مسائل سیبرنتیکی فرض کرد، ورود این فناوری‌ها و ضرورت استفاده از آنها در مراکز اطلاع‌رسانی می‌تواند چالش‌هایی را ایجاد کند. همانطور که ساراسویک [۲] بر این باور است که فناوری‌های اطلاعاتی اکثریت فعالیت‌های اطلاعاتی مثل گردآوری، سازماندهی، ذخیره و بازیابی، به اشتراک‌گذاری، تعامل و کاربری اطلاعات را با تحولاتی روبه‌رو کرده است. آگاهی از اصول سیبرنتیک و مدیریت نظام‌مند می‌تواند استفاده از این فناوری‌ها را بهینه‌تر سازد. وی معتقد است که در نظر گرفتن کتابخانه‌ها و مراکز اطلاع‌رسانی به‌عنوان یک نظام زنده و پویا، ضرورت دید نظام‌مند به فرآیندها و فعالیت‌های آن را نشان می‌دهد.

کتابخانه‌ها و مراکز اطلاعاتی، نظام‌های ذخیره و بازیابی اطلاعات محسوب می‌شوند و هدف سیبرنتیک هم پیشرفت نظام‌هاست، از این‌رو، نظامی که قصد پیشرفت و توسعه دارد ناگزیر از به‌کارگیری این قوانین است [۳]. در این راستا، پژوهش حاضر بر آن است تا با در نظر گرفتن کتابخانه‌ها و مراکز اطلاع‌رسانی به‌عنوان یک نظام سیبرنتیکی، انطباق اصول و قوانین علم سیبرنتیک را در مورد این نوع از سازمان‌ها بررسی کند تا در نهایت بتواند در شناسایی مشکلات و چالش‌های این مراکز و حل آنها و تلاش در جهت بهبود عملکرد و ارائه خدمات مؤثر به جامعه علمی کمک کند؛ چرا که سیبرنتیک علمی است که از یکسو، سیستم‌های باز را از دیدگاه تبادل متقابل اطلاعات میان آنها و محیط‌شان مورد بررسی قرار می‌دهد و از سوی دیگر، به بررسی ساختار این سیستم‌ها از دیدگاه تبادل متقابل اطلاعات میان عناصر مختلف می‌پردازد.

## ۲ اصول سیبرنتیک بر پایه دیدگاه‌های حاکم

اصول و قوانین در هر علم نقش بیان ایده‌های اساسی آن علم و ایجاد چارچوب و روش‌شناسی برای حل مسائل آن را دارند. حوزه سیبرنتیک به‌طور ویژه به چنین اصولی نیاز دارند؛ چرا که این حوزه ادعا دارد که تفکر را به طور کلی و نه فقط در یک رشته علمی خاص راهنمایی می‌کند [۱۵]. هیچ علمی بدون اصل شکل نمی‌گیرد. اصول پایه‌های علم هستند که چارچوب‌های کلی یک علم را تشکیل می‌دهند. این اصول غالباً تغییرناپذیرند و مهم‌ترین گام در فهم هر رشته‌ای آشنایی با اصول آن رشته است [۱۰]. نظریه‌پردازان سیبرنتیک مانند اشبی، وینر و ... اصول مختلفی را برای سیبرنتیک مطرح کرده‌اند. با بررسی متون ۱۲ اصل سیبرنتیکی شناسایی شد که این اصول عبارتند از: بقای انتخاب، رشد خود مجاورتی، انتقال نامتقارن یا آنتروپی و انرژی، تنوع کور یا تغییر بدون بصیرت، تنوع انتخابی، دانش ناقص، توسعه‌پذیری و تکامل‌پذیری، اشتراک یا دوسویگی،

مکملیت و متمیت، ساخت‌مندی یا ساختارمندی، پیچیدگی، و انعطاف‌پذیری یا بازگشت‌پذیری، که در ادامه به ۱۰ مورد از آنها به اختصار پرداخته شده است.

## ۱.۲ اصل بقای انتخابی

در یک سیستم، حالت‌های پایدار حفظ شده و آنهایی که ناپایدار هستند حذف می‌شوند و یا به حالت‌های پایدار تبدیل می‌شوند. بنابراین، ثبات آن چیزی است که تغییر نمی‌کند یا ناپایدار نمی‌شود و بی‌ثبات چیزی است که تمایل به محو و یا جایگزینی توسط حالت‌های دیگر دارد. این واقعیت که رشد نیازمند منابع است به این معناست که رشد به دلیل محدودیت منابع سرانجام متوقف می‌شود. دو موقعیت که از منابع همسان استفاده می‌کنند برای استفاده از منابع با همدیگر رقابت می‌کنند. به طور معمول موقعیت برتر بیشتر از منابع استفاده خواهد کرد، به طوری که برای موقعیت دیگر منبعی باقی نخواهد ماند. چنین تعمیمی از اصل بنای انتخابی ممکن است اصل انتخاب طبیعی نامیده شود [۸].

رشد فناوری‌های اطلاعاتی و عرصه انواع مختلف منابع اطلاعاتی در قالب‌های مختلف سبب شده است تا مراکز اطلاع‌رسانی با کاهش مراجعه‌کننده روبه‌رو شوند و سازمان‌های موازی با کتابخانه‌ها شکل بگیرند. در این حالت کتابخانه‌ها و مراکز اطلاع‌رسانی برای بقای خود باید با آنها رقابت نموده و مزیت رقابتی بهتری نسبت به سایر سازمان‌های مشابه به دست آورند تا همچنان مورد استفاده قرار گیرند. کتابخانه‌های دیجیتال نوعی از این اقدامات است. اگر اطلاعات به صورت مناسبی از طریق کتابخانه‌های دیجیتالی ارائه شود و ساختارهای شبکه نیز مهیا باشد، می‌تواند به طور کارآمدی در دسترس باشد. بنابراین توسعه کتابخانه‌های دیجیتال برای پردازش و در دسترس قرار دادن اطلاعات بسیار حائز اهمیت است به ویژه که با ارسال و مبادله اطلاعات در سطوح گسترده ملی و فراملی امکان تکرار فعالیت‌های موازی که با صرف هزینه مالی و انسانی همراه است از بین خواهد رفت. همچنین در کتابخانه‌های سنتی نیز وجین کردن منابع می‌تواند مثال مناسبی برای این انطباق باشد. در واقع وجین خود نوعی انتخاب است با این تفاوت که بعد از تهیه مجموعه اتفاق می‌افتد؛ از این رو، این امر به ارزشیابی مجموعه منتج می‌شود [۱۲].

## ۲.۲ اصل رشد خود مجاورتی

حالت‌های پایداری که پیدایش حالت‌های شبیه به خودشان را تسهیل می‌کنند، بسیار فراوان می‌شوند. این اصل تکمیل‌کننده اصل بقای انتخابی است. در حالی که اصل بقای انتخابی بیانگر جنبه محافظه کارانه تکامل است، اصل رشد خود مجاورتی جنبه مترقی رشد و توسعه را بیان می‌کند [۸]. در خصوص این اصل می‌توان به کارکردهای مراکز اطلاع‌رسانی برجسته و بزرگ اشاره نمود که می‌توانند نقش راهبری سایر کتابخانه‌ها و مراکز اطلاع‌رسانی را ایفا نمایند. به عنوان مثال، سازماندهی منابع اطلاعاتی برای هر مرکز اطلاع‌رسانی کار سخت، زمان‌بر و پرهزینه‌ای است و حتی ممکن است با صرف هزینه و زمان زیاد نیز خطاها و اشتباهاتی در این زمینه صورت پذیرد. برای حل این مشکل کتابخانه ملی هر کشور با فهرست‌نویسی کتاب‌های منتشر شده، زمینه استفاده آنان را از پیشینه‌های فهرست‌نویسی مناسب را فراهم می‌کند.

## ۳.۲ اصل انتقال نامتقارن یا آنتروپی و انرژی

انتقال از حالت ناپایدار به یک حالت پایدار امکان پذیر است اما احتمال عکس این قضیه بسیار کم است. شبیه این اصل توسط اشبی در اصول سیستم، سیستم خود سازمانده مطرح شد. از نظر اشبی سیستم‌ها به طور کلی به سوی تعادل در حرکت هستند. سیستم از حالت‌های متعدد عدم تعادل به سوی حالت‌های اندکی که دارای حالت تعادل هستند حرکت می‌کنند. در این روش سیستم، عمل انتخاب را انجام داده و با کاهش تعداد حالت‌های قابل دسترس و تنوع در اصل آنتروپی آماری کاهش پیدا می‌کند [۹]. در مراکز اطلاع‌رسانی، کارمند بخش امانت با توجه به میزان مراجعه -کنندگان می‌تواند انتخاب کند که به مراجعه‌کننده چه سطحی از خدمات را ارائه کند. به عنوان مثال در بازه‌های زمانی‌ای که تعداد مراجعان در بیشترین حالت خود است، از آموزش فردی به مراجعان برای یافتن منابع اطلاعاتی مورد نیازشان در مخزن خودداری می‌کند و صرفاً به صورت اجمالی روند بازیابی را برای مراجعه‌کننده توضیح می‌دهد.

## ۴.۲ اصل تنوع کور یا تغییر بدون بصیرت

در بنیادی‌ترین سطح معلوم نیست که کدام یک از انواع متفاوت فرایندهای تغییر انتخاب خواهند شد. کوری تنوع یا بی بصیرت بودن تغییر در تکامل زیست‌شناختی بر پایه جهش و باز ترکیب‌های تصادفی امری بدیهی است. بر این اساس حتی سیستم‌های پویای کاملاً قطعی را می‌توانیم کور بنامیم. به این معنا که اگر سیستم به اندازه کافی پیچیده باشد، پیش‌بینی انتخاب حالت پایدار از بین حالت‌های مختلف غیر ممکن است. البته بسیاری از تعامل‌ها کور نیستند. در حل یک مسئله علمی به طور معمول عملیات حل مسئله را به صورت تصادفی انتخاب نمی‌کنیم. دانایی ما خود نتیجه آزمون و خطاهای قبلی است. از تجربه موقعیت‌ها و شکست‌های دیگران برای هدایت فعالیت‌های بعدی استفاده می‌کنیم. بر پایه اصل رشد خود مجاورتی موقعیت‌هایی که به وسیله تنوع کور انتخاب شده‌اند می‌توانند انتقال به بقای انتخابی را به وجود بیاورند [۹].

در مراکز اطلاع‌رسانی برای ارائه خدمت جدید علاوه بر همفکری با همه کارکنان، بررسی می‌شود که خدمت مذکور در دیگر مراکز مشابه در چه سطحی و با چه کیفیتی اجرا می‌شود و آن مراکز برای آن خدمت خاص چه بازخوردهایی دریافت کرده‌اند. به عبارت ساده‌تر هر مرکز اطلاع‌رسانی برای ارائه یک خدمت جدید علاوه بر دانش و دانایی کارکنان خود به تجربه آن موقعیت توسط دیگر مراکزی که آن خدمت را ارائه می‌کنند و یا می‌کرده‌اند، می‌پردازد تا بتواند برای ارائه یا عدم ارائه آن خدمت جدید تصمیم درستی بگیرد.

## ۵.۲ اصل تنوع انتخابی

هر چه حالت‌های یک سیستم متنوع‌تر باشد، احتمال اینکه حداقل یکی از این حالت‌ها بتوانند به طور انتخابی حفظ بشود بیشتر خواهد بود. از طرفی، هر چه شمار حالت‌های پایدار بالقوه کمتر باشد، به همان میزان احتمال بیشتری دارد که حداقل یکی از این ساختارها به صورت انتخابی باقی بماند. سیستم‌ها و ساختارهای کم تعداد یا دارای پایداری کمتر، تنوع بیشتری دارند. سیستم می‌بایست به منظور حفظ و نگهداری فرصت‌های خود



برای ساختار پایدار تغییر کند [۸]. تا دهه ۱۹۸۰ کتابخانه‌ها انحصار ارائه اطلاعات موجود در منابع چاپی را در اختیار خود داشتند استفاده کنندگان آنها هم در مورد انتشارات مورد نیاز خود کاملاً به کتابخانه‌ها وابسته بودند اما اکنون با ظهور فناوری‌های نوین اطلاعاتی که حجم انبوهی از اطلاعات به صورت پیوسته و با قالب الکترونیکی برای همگان قابل دسترس گشته شرایط به طور کلی دگرگون شده است و کارکنان آگاه دسترسی منسجم به اطلاعات را بدون توجه به محل اطلاعات برای کاربران چه در محل مرکز یا در مکان دور دستی باشند، تأمین می‌نمایند [۱۴]. روش‌های دسترسی به اطلاعات نیازها و خواسته‌های اطلاعاتی فرد را وادار به جستجی اطلاعات با رغبت برای رفع نیاز می‌نماید. به طور سنتی حرفه‌مندان اطلاعاتی گستره متنوعی از فنون تحلیل، تثبیت، سازماندهی و تأمین دسترسی به اطلاعات را ایجاد کردند. روش‌های زیادی وجود دارند که فرد از طریق آنها اطلاعات مورد نیاز خود را جستجو کند. در یک بیان کلی سه روش برای جستجوی اطلاعات وجود دارد که عبارتند از: ارتباطات شخصی، شبکه‌های رایانه‌ای، مراجعه به کتابخانه [۱۷].

## ۶.۲ اصل دانش ناقص

مدل گنجانده شده در سیستم کنترل لزوماً ناقص است و مدل‌ها به وسیله فرایندهای تنوع کور ساخته می‌شوند. بنابراین، نمی‌توانیم انتظار داشته باشیم که به بازنمون کاملی از یک محیط بی‌نهایت پیچیده دست پیدا کنیم [۹]. ارزشیابی موقعیت فعلی و آینده محیط کمک می‌کند تا تعیین شود که چه عواملی بر مراکز اطلاع‌رسانی تأثیر خواهد گذاشت. واضح است داشتن اطلاعات خوبی از رقبا به دانش در مورد کتابخانه و سازمان مادر و دانش درباره بازار شما بسیار مهم است [۱]. با وجود اهمیت برنامه‌ریزی استراتژیک هنوز در بسیاری از سازمان‌ها تأثیر حیاتی آن در رسیدن به اهداف سازمان به خوبی درک نشده و حتی در بعضی از مواقع مدیران آن را یک امر تجملی و پرهزینه می‌دانند. در میان این سازمان‌ها، مراکز اطلاع‌رسانی و کتابخانه‌ها به دلیل ارائه نوع خدمات و ذخیره و اشاعه دانش‌های جدید و قدیمی و توسعه و تقویت نیازهای اطلاعاتی فرهنگی و اجتماعی جامعه از اهمیت ویژه برخوردار است و مسلماً مدیران آنها باید از قوه خلاقیت و توانایی خود بتوانند این نهاد اجتماعی را از پیچیدگی‌ها و پویایی محیط‌ها، رسانه‌ها و محل‌های اطلاعاتی جدید مصون دارند و خود را آماده پذیرش فرصت‌ها و رفع تهدیدهای آنها بنمایند. در واقع، مدیریت استراتژیک یکی از ابزارهایی است که میان عناصر درون سازمان و فشارها و تغییرات محیط خارجی هماهنگی لازم را ایجاد می‌کند [۷].

## ۷.۲ توسعه‌پذیری و تکامل‌پذیری

سیستم‌های سبیرنتیکی در یک موقعیت فرصت‌طلبانه تهدیدها را به فرصت تبدیل می‌کنند و در این فرصت خود را گسترش، تکامل و تغییر می‌دهند و به واسطه این فرصت‌ها تکامل سیستم‌های سبیرنتیکی اتفاق افتد. بنابراین، سیستم‌های سبیرنتیکی تمایل دارند در یک موقعیت فرصت‌طلبانه، خودشان را توسعه دهند [۸]. عرصه‌های مختلف زندگی به ویژه از بعد فناوری نیازمند توسعه مداوم برای تجدید سازمان بر اساس اندیشه‌ها و بینش‌های جدید است [۱۹] و در این بین کتابخانه‌های دیجیتالی نیز به عنوان نوید عصر فناوری اطلاعات برای توسعه‌پذیری و پاسخگویی به نیازها و رفتارهایی که با راه اندازی آنها ایجاد شده از این امر

مستثنی نیستند. چن [۱۳] بیان میکند که اکثر تلاش‌های مربوط به افزایش جریان اطلاعات و دانش در کشورهای غربی بر برنامه‌های توسعه کتابخانه‌ها و مراکز اطلاع‌رسانی دیجیتالی متمرکز شده است. لو زیمرمن [۱۶] نیز بیان میدارند با توسعه اینترنت در قرن حاضر مراکز اطلاع‌رسانی تلاش خود را در زمینه توسعه کتابخانه‌ها و مراکز دیجیتالی متمرکز کردند. بنابراین توسعه کتابخانه‌های دیجیتالی با توجه به پیشرفت‌های صورت گرفته در عرصه فناوری و ایجاد محیط فعالیت جدید جزء اولویت‌های عرصه علم اطلاعات و دانش‌شناسی در آمده است.

## ۸.۲ اشتراک یا دوسویگی

اجزای سیستم‌های سبیرنتیکی باهم تعامل دارند و این تعامل با اجزای خود و با زیر سیستم‌های آنها برقرار است؛ یعنی در عین استقلال داشتن از هم، به یکدیگر وابسته‌اند و در عین واگرایی همگرا هستند. به عبارت دیگر، اجزای سیستم سبیرنتیکی به صورت موازی و مشارکتی با همدیگر به تعامل می‌پردازند. تعامل یک ارتباط دوسویه است که در نهایت به هماهنگی و همکاری منجر می‌شود [۹]. مراکز اطلاع‌رسانی هم به عنوان یک سازمان از این اصل پیروی می‌کند و بخش‌های مختلف آن علاوه بر اینکه فعالیت محوله خود را به صورت مستقل انجام می‌دهند. با دیگر بخش‌ها در تعامل و مشارکت هستند. همچنین مدیران در این مراکز بر ارتباط با سایر مراکز برون‌سازمانی تاکید دارند [۴]. همکاری میان کتابخانه‌ها و مراکز اطلاع‌رسانی عبارت است از کار مشترک میان دو یا چند مرکز به منظور تهیه و تدارک خدمات بهتر برای مراجعان با استفاده از امکانات و فن‌آوری مناسب [۶].

## ۹.۲ پیچیدگی

ساختار سیستم سبیرنتیکی اساساً و در بنیان پیچیده است. ساختارهای پیچیده با عناصر متعامل و نامتجانس به وجود آمدند. به عبارت دیگر، اجزاء و عناصر ضمن آنکه باهم در ارتباط بوده و از هم تأثیر می‌پذیرند، از هم جدا بوده و ضمن جدا بودن استقلال نسبی دارند [۸]. مراکز اطلاع‌رسانی نیز به مثابه یک سیستم سبیرنتیکی در بنیان پیچیده است. بخش‌های مختلف کتابخانه یک مرکز اطلاع‌رسانی از یکدیگر تأثیر می‌پذیرند، اگر چه در ظاهر این بخش‌ها از هم جدا هستند اما ضمن در عمل با هم در ارتباط هستند و ضمن تعامل و برهمکنش، استقلال نسبی نیز دارند.

## ۱۰.۲ ساخت‌مندی یا ساختارمندی

منظور این است که سیستم‌های سبیرنتیکی، تمایل به روند توسعه و پیچیدگی دارند و این در حالی است که پیوند و پابندی خود را با موقعیت قبل سیستم و وضعیت سابق حفظ کنند. بنابراین، سیستم‌های سبیرنتیکی ساخت‌مند هستند و در حالی که گرایش به افزایش اندازه و پیچیدگی دارند، به لحاظ تاریخی به وضعیت‌های پیشین هم وابسته هستند تا زمانی که مقارن با یکدیگر خصلت‌ها و ویژگی‌های جدید را گسترش دهند [۹]. پیشرفت‌های فناوری اطلاعات از جمله تولید نرم‌افزارها، بانک‌های اطلاعاتی، ارتباطات دوربرد، پیدایش اینترنت، اینترانت و امکانات انتقال اطلاعات مانند پست الکترونیکی و

تصویری، دسترس پذیری به منابع اطلاعاتی را بهبود بخشیده است. هم‌اکنون ما شاهد تحولات و تغییرات اساسی در خدمات مراکز اطلاع رسانی، و روش‌های ارائه اطلاعات و کاربرد فناوری اطلاعات در جامعه هستیم. البته منابع ارزشمند فراوانی در این نهادها موجود است که به شکل کنونی خود قابل استفاده در محیط‌های شبکه‌ای نیستند. لازم است این منابع به قالب دیجیتال تبدیل شده و به روشی سامان یابند که در محیط وب و شبکه‌های از راه دور قابل استفاده باشند. کتابخانه دانشگاهی علاوه بر ارائه خدمات الکترونیکی به کاربرانی که از دور با کتابخانه در ارتباط هستند [۵].

### ۳ نتیجه‌گیری

راه‌حل‌های معمولی سنتی دیگر جوابگوی آشفتگی‌های موجود در دنیای کنونی نیست و به راه‌حل‌های جدیدی نیازمندیم تا بتوانیم پیچیدگی‌های موجود در این دنیا و عصر حاضر را کنترل کنیم. سبیرنتیک یکی از این راه‌حل‌هاست. سبیرنتیک نگرشی عام به تمامی پدیده‌های عالم اعم از طبیعی و اجتماعی دارد. لذا قلمرو مطالعاتی آن در برگرفته سیستم‌های فیزیکی و اجتماعی است. برای استفاده از این علم نیاز به شناخت مفاهیم و اصول آن داریم. با دسته‌بندی اصول و مفاهیم هر رشته خط فکری و چارچوب نظری آن علم برای پژوهشگران بهتر و بیشتر ترسیم شده و می‌تواند به پژوهش‌های آن حوزه خط سیر و چارچوب کلی دهد. از آنجایی که پارادایم‌های غالب بر رویکردهای مختلف می‌تواند متفاوت و حتی در برخی از مواقع متضاد باشد را شناخت این دیدگاه‌ها و مشخص کردن اصول حاکم بر هر دیدگاه می‌تواند در فهم موضوع بسیار حیاتی باشد. مرور اصول و قوانین حاکم بر سبیرنتیک نشان داد که برخی اصول از تجربیات حسی برگرفته شده و امکان شناخت پدیده‌ها و روابط آنها با یکدیگر را شناخت. همچنین این اصول چستی پدیده‌ها و تاثیر آنها بر یکدیگر و بر قلمروهای دیگر را مشخص می‌کنند. با توجه به سیر تحول دیدگاه‌های فلسفی و تفاوت نوع نگاه این رویکردها به پدیده‌های عالم میتوان خاستگاه مراتب و اصول متفاوت ارائه شده در سبیرنتیک را در قالب تفاوت در مفهوم مشاهده و مشاهده‌گر دانست. نحوه نگرش و زاویه نگاه اندیشمندان به پدیده‌های هستی موجب شکل‌گیری دیدگاه‌های مختلف و اصول متفاوت برای علوم شدند. بنابراین می‌توان گفت بن مایه فکری نسل‌ها و اصول سبیرنتیک آینده‌ای از رویکردهای پوزیتویستی، ارگانیستی، جهان‌بینی سیستمی و فیزیک جدید است. بر این اساس رویکردی سبیرنتیکی در طی عمر کوتاه آن متکی بر دیدگاه‌های حاکم متحول شده است. در ادامه انطباق اصول سیستم‌های سبیرنتیکی با مراکز اطلاع رسانی نشان داده شد و مشخص شد که این مراکز خصوصیات و اصول اصلی سیستم‌های سبیرنتیکی را داراست. انطباق مراکز اطلاع رسانی با سیستم‌های سبیرنتیکی، می‌تواند نگرش و بینش عمیق‌تری نسبت به شناسایی مشکلات و چالش‌های این مراکز به دست بدهد و زمینه را جهت رفع مشکلات این سازمان فراهم کند. با به‌کارگیری اصول و قوانین سبیرنتیکی در این مراکز میتوان در جهت بهبود عملکرد و پیشرفت علمی آنها حرکت کرد.

## مراجع

- [۱] متیوز، جوزف آر. برنامه‌ریزی و مدیریت راهبردی در کتابخانه‌ها، ترجمه عبدالحسین فرج پهلوی. دانشگاه شهید چمران اهواز، ۱۳۸۷.
- [۲] ساراسویک، تفکو. ربط در علم اطلاع‌رسانی، ترجمه‌ی حیدر مختاری، عباس میرزایی، ویراسته‌ی اعظم صنعت‌جو، ویرایش ۱. تهران، انتشارات خرسندی، ۱۳۸۹.
- [۳] اسماعیل‌پور، رضیه. عوامل اجتماعی و جرم. پژوهش‌نامه کتابداری و اطلاع‌رسانی، ۶، ۱ (۱۳۹۵)، ۲-۵.
- [۴] محمدزاده روشتی، زیبا؛ قیاسی، میترا؛ کاردان نشاطی، محمد. مطالعه ابعاد سایبرنتیک در کتابخانه مرکزی دانشگاه‌های دولتی شهر تهران از دیدگاه کتابداران. فصلنامه مدیریت اطلاعات و دانش‌شناسی، ۵، ۱ (۱۳۹۷)، ۲۱-۳۶.
- [۵] شه‌میرزادی، طیبیه؛ داودزاده، سیروس. ضرورت توسعه کتابخانه دیجیتال کشاورزی. مجله ترویجی علوم و فناوری اطلاعات کشاورزی، ۳، ۶ (۱۳۹۹)، ۴۳-۴۹.
- [۶] کاشانی، پروانه. همکاری بین کتابخانه‌ها و اشتراک منابع. تحقیقات اطلاع‌رسانی و کتابخانه‌های عمومی، ۱۳، اول و دوم (۱۳۸۲)، ۶۹-۸۷.
- [۷] سهیلی، فرامرز. تحلیل نقاط قوت، ضعف، فرصت‌ها و تهدیدهای کتابخانه‌های دانشگاه رازی و ارائه راهبردهای استراتژیک مناسب برای این کتابخانه‌ها. نشریه تحقیقات کتابداری و اطلاع‌رسانی دانشگاهی، ۴۴، ۵۵ (۱۳۹۰)، ۷۳-۹۵.
- [۸] جباری، لیلا؛ زندیان، فاطمه. آشنایی با مفاهیم، اصول و کاربرد سیبرنتیک، ویرایش ۸. تهران: چاپار، ۱۳۹۹.
- [۹] داورپناه، محمدرضا. سیبرنتیک: نظریه عمومی کنترل مکانیسم‌ها در سیستم‌های مکانیکی و ارگانیکی. تهران: دبیرش، ۱۳۹۰.
- [۱۰] داورپناه، محمدرضا. تقریرات درس ارتباطات و سیبرنتیک (دوره دکتری علم اطلاعات و دانش‌شناسی). مشهد: دانشگاه فردوسی مشهد، دانشکده علوم تربیتی و روانشناسی (۱۳۹۳).
- [۱۱] لرنر، آلکساندر یا کاولیویچ. مبانی سیبرنتیک، ترجمه‌ی کیومرث پریانی، ویرایش ۱. تهران: دانش پژوه، ۱۳۶۶.
- [۱۲] نوروزی، یعقوب. محورهای توسعه کتابخانه‌های دیجیتالی. فصلنامه علمی-پژوهشی نهاد کتابخانه‌های عمومی کشور، ۱۷، ۱ (۱۳۹۵)، ۱۲۹-۱۵۳.
- [13] CHEN, H. Digital library research in the US: an overview with a knowledge management perspective, Program. *Electronic Library and Information Systems* 38, 3 (2004), 67-157.
- [14] COOGAN, E., DEPALO, D., GERVAIS, S., KLINE, C., KNOFF, C., TATIAN, C., AND ET AL. *Service to Users Task Force*. Brown University Library, October 1998.
- [15] HEYLIGHEN, F. *Principles of systems and cybernetics: an evolutionary perspective*. 1999.
- [16] LOU, H., AND ZIMMERMAN, J. The Development of Digital Libraries in China and the USA. *Information Development* 19, 13 (Retrieved Feb. 16, 2010).

- [17] MANJUNATHA, K., AND SHIVALINGAIAH, D. *Information access in Libraries: Methods and Problems*. In M. Bavakutty and et al, *Information access, Management and exchange in the technological age*. New Delhi: ESS Publication, 2003.
- [18] SCOTT, B. *Second-order cybernetics: an historical introduction*. *Kybernetes*, 33(9/10), 2004.
- [19] UNESCO. *Change in Continuity. Concepts and tools for cultural approach to development*. UNESCO, Paris, 2000.





## سازگاری یا ناسازگاری توصیه‌نامه‌ی اخلاق هوش مصنوعی یونسکو با نظریه اخلاقی اسلام

حمید محسنی<sup>۱</sup>، کاظم فولادی قلعه<sup>۲</sup>

<sup>۱</sup> دانشجوی دکتری، مؤسسه آموزشی و پژوهشی امام خمینی، قم  
h.mohseni1297@mailfa.com

<sup>۲</sup> استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدهگان فارابی دانشگاه تهران؛  
سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران  
kfouladi@ut.ac.ir

### چکیده

یونسکو به تازگی سندی بین‌المللی با عنوان «توصیه‌نامه‌ی اخلاق هوش مصنوعی» تصویب کرده است. در این سند مجموعه‌ای از ارزش‌ها مشخص شده و از کشورهای عضو خواسته شده است مفاد آن را در جوامع خود به نحوی اجرا کنند. در واقع، نهادهای بین‌المللی سعی دارند با تصویب این‌گونه اسناد بالادستی، قوانین و ارزش‌های ملت‌ها را با خود همراه سازند. بنابراین، مسئله اصلی این پژوهش، بررسی سازگاری و یا عدم سازگاری مبانی ارزش‌های اخلاقی توصیه‌نامه‌ی مذکور با مبانی اخلاقی اسلام می‌باشد. بر اساس یافته‌های این تحقیق می‌توان گفت برخی مفاد این توصیه‌نامه مبتنی بر مکتب اخلاقی قراردادگرایی است. از این رو، این توصیه‌نامه به لحاظ موضوع و هدف اخلاقی، وظیفه‌گرا و عمل‌محور می‌باشد. اما نظریه‌ی اخلاق مکتب اسلام به لحاظ موضوع و هدف اخلاقی، فضیلت‌محور، غایت‌گرایانه و کمال‌جو می‌باشد. نتیجه این‌که در سند اخلاق هوش مصنوعی یونسکو تنها اصلاح رفتار فرد بدون معنویت و دین در نظر گرفته شده است. ولی در نظام اخلاقی اسلام، هدف، اصلاح رفتار و صفات نفسانی و ساخت شخص انسان و به پیرو آن نزدیک شدن به کمال مطلق می‌باشد. افزون بر این، در پژوهش حاضر دو نظریه، یکی ناظر به امکان اخلاق‌مندی خود سیستم‌های هوشمند و دیگری ناظر به تعامل انسان با هوش مصنوعی ارائه شده است.

**کلمات کلیدی:** اخلاق، هوش مصنوعی، یونسکو، نظریه اخلاقی اسلام.

### ۱ مقدمه

هوش مصنوعی به‌عنوان یک تکنولوژی نوظهور، برای انسان معاصر فایده‌هایی را به ارمغان آورده است، ولی خطرهایی نیز از این ناحیه ارزش‌های اخلاقی انسان را تهدید می‌کند. بسیاری معتقدند که در آینده‌ای نه‌چندان دور، ظهور ابرهوش<sup>۱</sup> امری اجتناب‌ناپذیر است؛ هر چند در مدت زمان روی دادن این رخداد اختلاف

<sup>1</sup> Super Intelligence

نظر وجود دارد [۱۳]. اما این پدیده می‌تواند مخاطراتی بسیار جدی برای بشریت به همراه داشته باشد. از این رو دانشمندان می‌بایست مجموعه‌ای از ملاحظات را در نظر بگیرند. افزون بر این، همین هوش مصنوعی فعلی (هوش مصنوعی محدود<sup>۲</sup>) در زندگی بسیاری از انسان‌ها تأثیرگذار می‌باشد [۱۵]. این فناوری‌ها در کنار مزایای متعدد، خطرات و چالش‌هایی را نیز ایجاد می‌کنند که بخشی از آن ناشی از استفاده‌ی بدخواهانه از فناوری است. از این رو، سازمان بین‌المللی یونسکو به این فکر افتاده است که چارچوب‌های نظارت بین‌المللی و ملی را فراهم آورد تا این فناوری در جهت منفعت بشریت توسعه پیدا کند.

یونسکو متن اولیه سندی را با عنوان «توصیه‌نامه اخلاق هوش مصنوعی» زیر نظر یک گروه ۲۴ نفری از متخصصان ویژه (AHEG) تنظیم کرد. با بررسی رزومه‌ی این گروه ویژه مشاهده می‌شود که تخصص بیشتر آنها در حوزه‌ی فنی و مهندسی است، هرچند تعدادی حقوق دان و فیلسوف نیز از کشورهای مختلف - غیر از ایران - در بین آنها دیده می‌شود. همچنین حدود سه کارشناس با رویکرد اخلاق هوش مصنوعی از کشورهای آمریکا، بریتانیا و چین نیز در فرآیند تهیه‌ی این سند حضور داشته‌اند. به هر حال، پس از ماه‌ها گفت‌وگو و مذاکره‌ی نمایندگان کشورهای عضو و أخذ دیدگاه آنها و اعمال برخی نکات زیر نظر کارشناسان مزبور، اعضای یونسکو بر روی یک متن برای توسعه‌ی ارزش‌های اخلاقی در حوزه‌ی هوش مصنوعی به توافق رسیدند. سرانجام، این توصیه‌نامه در چهل و یکمین جلسه‌ی کنفرانس عمومی یونسکو در تاریخ ۲۴ نوامبر ۲۰۲۱، به تصویب رسید.

در این سند که متشکل از یک مقدمه و ۱۴۱ بند است، یک سری اهداف و باید و نبایدها آورده شده و از کشورهای عضو - از جمله ایران - خواسته شده است مفاد این سند را در کشورهای خودشان به نحوی اجرا کنند. نهادهای بین‌المللی با تصویب این گونه سندها - هر چند به ظاهر غیر الزام‌آور - سعی دارند آنها را به عنوان اسناد بالادستی قراردادده تا ارزش‌ها و قوانین جوامع دیگر را با خود همراه سازند. در بخشی از گزارش‌هایی که پیش از سند اصلی آمده است، بدین مطلب تصریح شده است که یونسکو سعی دارد رهبری اخلاقی خود را با تنظیم استانداردها و ایجاد ظرفیت‌هایی در حوزه علم و فناوری و هوش مصنوعی با رویکردی انسان‌محور تقویت کند [۱۶]<sup>۳</sup>. از این رو، این توصیه‌نامه سعی دارد هنجارهای اخلاقی را متناسب با اهداف خود در بین ملت‌ها مورد توجه قرار دهد.

بنابراین مفاد این توصیه‌نامه در قلمروی ارزش و هنجاری‌های اخلاقی بوده و هنجارهای اخلاقی نیز مبتنی بر یک سری مبانی و اصول هستند. در علم اخلاق، مکاتب متعدد اخلاقی وجود دارد که هرکدام مبتنی

<sup>۲</sup>Artificial Narrow Intelligence (ANI)

<sup>۳</sup>Reinforce UNESCO's leadership on global ethical reflection, standard setting, and building analytical capacities, to ensure human-centred progress in science and technologies, including in digital innovations and converging fields such as AI, gene-editing, and neuro-technologies; and build national capacities to maximize the benefits of these technologies and to address the associated risks. <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>

<sup>۴</sup>این متن در سند اصلی نیامده است ولی این عبارت در یکی از گزارش‌های پیش از متن نهایی تصویب شده، ذکر شده است. در این عبارت تصریح شده است که یونسکو سعی دارد رهبری خود درباره‌ی تنظیم استانداردها و ایجاد ظرفیت‌های اخلاقی را در جهان تقویت کند و زمینه‌ی پیشرفت انسان‌محور را در علم، فناوری، نوآوری‌های دیجیتال و زمینه‌های همگرا همچون هوش مصنوعی، ویرایش ژن‌ها و فناوری عصبی را به نفع بشریت فراهم آورد.

بر قواعد و اصولی می‌باشند. به‌طور کلی، مکاتب اخلاقی در برخی کتب فلسفه‌ی اخلاق به مکاتب واقع‌گرا و غیر واقع‌گرا تقسیم می‌شود.

از این رو برای بررسی سند مذکور نخست می‌بایست یک نگاه کلی به مکاتب اخلاقی داشته باشیم، سپس متن توصیه‌نامه را بر اساس آن ارزیابی کنیم. در این صورت، مشخص خواهد شد که منشأ ارزش‌های اخلاقی این سند، آیا برخاسته از دیدگاه‌های واقع‌گرایی و متناسب با نظریه اخلاقی مکتب اسلام است یا اینکه ارزش‌های اخلاقی مزبور متأثر از نظریه‌های غیرواقع‌گرایی و قراردادگرایی بوده و با ارزش‌های اخلاقی اسلام بسیار فاصله دارد. بنابراین، ضروری است مبانی و ارزش‌های اخلاقی این سند بین‌المللی با مبانی ارزش‌های اخلاق اسلامی مقایسه شود. پس مسئله‌ی اصلی این مقاله، بررسی سازگاری و یا ناسازگاری مبانی ارزشی سند اخلاق هوش مصنوعی یونسکو با نظریه‌ی اخلاقی مکتب اسلام می‌باشد. از این رو، عمده‌ی بحث ما - پس از تبیین اخلاق هوش مصنوعی و امکان اخلاق‌مندی ربات‌ها - تحلیل مبانی ارزش‌های سند مذکور و ارائه‌ی نظریه‌ی اخلاق هوش مصنوعی با استفاده از اندیشه‌ی برخی از فلیسوفان اسلامی می‌باشد. به همین دلیل با روش توصیفی و تحلیلی به کنکاش این سند بین‌المللی در حوزه‌ی اخلاق هوش مصنوعی می‌پردازیم.

## ۲ مروری بر کارهای دیگران

در خصوص کارهای مشابه، تنها پیشینه‌ای که به‌صورت رسمی و مدون یافت شد، گزارشی است که با عنوان «نقد و بررسی اولین پیش‌نویس توصیه‌نامه‌ی اخلاق هوش مصنوعی (یونسکو)» توسط بهزاد خداقلی‌زاده و همکاران و تحت نظر محمد مهدی نصره‌رندی (مدیر گروه مطالعات اخلاقی) در پژوهشگاه مرکز ملی فضای مجازی چاپ شده است [۱]. در این گزارش نقدهایی به‌صورت بند به بند و نقدهایی کلی مطرح شده است، اما در آن هیچ اشاره‌ای به مبانی اخلاقی و سازگاری آن با نظریه‌ی اخلاقی اسلام نشده است. افزون بر این طبق فراخوانی که دفتر فقه معاصر حوزه علمیه قم برای بررسی سند مزبور داد، تحقیقاتی در این راستا انجام شد که از میان آنها حدود ده مقاله برگزیده شده و در قالب کتاب به‌زودی انتشار خواهد یافت. در آن مقالات - به دلیل اینکه پیش از تصویب نهایی سند تدوین شده‌اند - با رویکردهای مختلف به نقد و بررسی نقاط قوت و ضعف سند پرداخته شده است و در ضمن آن پیشنهادهای تکمیلی نیز ارائه داده شده است. مقاله‌ای از نگارنده اول نیز در آن کتاب وجود دارد که در این پژوهش به برخی نتایج آن تحقیق اشاره خواهیم کرد. افزون بر آن، در مقاله‌ی حاضر با زاویه دیدی متفاوت به بررسی سند اخلاق هوش مصنوعی خواهیم پرداخت.

## ۳ تبیین اخلاق هوش مصنوعی

به نظر می‌رسد برای تبیین و تحلیل بهتر، پیش از ورود به بررسی سند، بایسته و شایسته است به‌طور خلاصه مقصود از اخلاق هوش مصنوعی و رویکردهای مختلف در این زمینه تبیین شود. در یک رویکرد، خود هوش مصنوعی و ربات‌ها مورد خطاب باید و نباید قرار می‌گیرند. می‌توان «قوانین سه‌گانه‌ی رباتیک» که نخستین بار در سال ۱۹۴۲ توسط ایزاک آسیموف برای جلوگیری از آسیب‌رسانی ربات‌ها به انسان ارائه شد را از این قسم دانست [۱۵]. در رویکردی دیگر، اخلاق هوش مصنوعی بخشی از اخلاق ماشینی می‌باشد. هدف اخلاق

ماشین این است که ماشینی می‌بایست ساخته شود که دست کم از یک اصل اخلاقی ایده‌آل و یا مجموعه‌ای از اصول اخلاقی پیروی کند [۱۲]. اما مراد از اخلاق هوش مصنوعی در رویکردی دیگر، این است که چگونه می‌توان کدهای اخلاقی را در سیستم‌های هوشمند تدوین کرد تا از خطرات احتمالی هوش مصنوعی علیه انسان‌ها جلوگیری شود [۱۳].

به نظر می‌رسد این نوع نگاه‌ها متأثر از دو گونه هدف‌گذاری مختلف برای مقوله‌ی هوش مصنوعی است. یک هدف‌گذاری، با اصطلاح هوش مصنوعی ضعیف<sup>۵</sup> بیان می‌شود. در این هدف‌گذاری تنها معیار این است که کارکرد ایجاد شده در قالب هوش مصنوعی، به‌درستی و رضایت‌مندانه انجام شود. اما در هدف‌گذاری مقابل که با عنوان هوش مصنوعی قوی<sup>۶</sup> از آن یاد می‌شود، رفتار هوش مصنوعی با رفتار انسان سنجیده می‌شود، در حالی که در هدف‌گذاری ضعیف با عملکرد سیستم سنجیده می‌شود. در هدف‌گذاری قوی به دنبال شبیه‌سازی سیستم ادراکی و آگاهی انسان در هوش مصنوعی هستند. افزون بر این، طرفداران هوش مصنوعی قوی بر این باورند که به‌دلیل دستیابی به اکتشافات، الگوریتم‌ها و دانش برنامه‌های نوین، هوش مصنوعی می‌تواند دارای حس هشیاری و آگاهی باشد [۱۴].

به نظر می‌رسد در توصیه‌نامه‌ی اخلاقی یونسکو، هدف‌گذاری ضعیف اتخاذ شده است. همان‌طور که در بند ۲، به‌خصوص بخش a تأکید شده است که نگاه این سند به سیستم‌های هوش مصنوعی به‌عنوان یک فناوری پردازش اطلاعات می‌باشد. افزون بر این، در بند ۲۶ اشاره می‌کند که هوش مصنوعی نباید تصمیم‌گیر نهایی در مسائل مهم همچون مرگ و زندگی باشد، بلکه اختیار آن باید به دست انسان‌ها باشد. افزون بر این، مراد از اخلاق هوش مصنوعی در توصیه‌نامه‌ی یونسکو بیشتر در ارتباط با رفتار انسان‌ها و بازیگران هوش مصنوعی می‌باشد، نه اینکه خود سیستم‌های هوشمند را مورد خطاب باید و نباید اخلاقی قرار دهد.

آیا بنا بر مبانی علم النفس اسلامی ربات‌ها می‌توانند به باید و نباید اخلاقی متصف شده و همانند انسان تصمیم‌های اخلاقی بگیرند؟ بررسی این مسئله نیازمند یک تحقیق و پژوهش مستقل و اساسی هست. از این رو، در اینجا به‌طور مختصر این مسئله را بررسی و نقد می‌کنیم. انجام رفتار اخلاقی متوقف بر آگاهی و درک معنای خوب و بد و مبتنی بر اختیار و اراده می‌باشد. اراده نیز مستلزم داشتن ذهن و یا نفس می‌باشد. در عین حال، بنا بر مبانی علم النفس اسلامی، هوش مصنوعی نمی‌تواند ذهن و یا نفس خودآگاه داشته باشد. دلیل این امر به‌طور مختصر با تأمل در تعریف و حقیقت نفس در اندیشه‌ی حکمای اسلامی مشخص می‌شود. ابن سینا نفس را این‌گونه تعریف کرده است: «نفس کمال اول برای جسم طبیعی است» [۵]. بنا بر این تعریف، نفس یک حقیقت و کمال وجودی است که به جسم طبیعی تعلق پیدا می‌کند، نه به جسم مصنوعی. در اندیشه‌ی صدرالمتألهین بین ترکیب جسم مصنوعی و جسم طبیعی و آثار و احکام مترتب به آن تفاوت‌های بسیار عمیقی وجود دارد. در ترکیب صناعی، اجزاء به یکدیگر ضمیمه می‌شوند و با کنار هم قرار گرفتن آنها، شیء دارای یک حقیقت واحد نمی‌گردد. اما در ترکیب «طبیعی بالذات» شیء به‌تمام ذات تبدیل به شیء دیگری می‌شود، همچون جنین که تبدیل به انسان می‌شود [۶]. بنا بر این، در هوش مصنوعی با ترکیب اجزاء آن، هر چند اجزاء موجود هستند و کارکردهای بسیاری نیز از ماشین پیچیده‌ی هوشمند بروز و ظهور پیدا

<sup>5</sup>Weak AI<sup>6</sup>Strong AI

می‌کنند ولی بنابر علم النفس اسلامی، جسم مصنوع نمی‌تواند دارای ذهن (غیر فیزیکی) یا نفس مجرد شود تا بتواند از روی اختیار آگاهانه فعل اخلاقی را تشخیص داده و تصمیم به انجام آن بگیرد. بنابراین، ربات و ماشین‌های هوشمند، نفس یا ذهن ندارند تا آگاهی و اراده‌ی آزاد در انجام افعال داشته باشند. از این رو، امکان اخلاق‌مندی ربات‌ها بدین معنا منتفی است. البته همان‌طور که در مقدمه و برخی بندهای توصیه‌نامه‌ی یونسکو آمده است باید هوش مصنوعی را به سمت ارزش‌های اخلاقی هدایت کرد. همچنین بعضی دانشگاه‌ها، مراکز و مؤسسات - همچون مرکز آینده‌ی اطلاعات در کمبریج یا مطالعه صدساله هوش مصنوعی AI۱۰۰ در دانشگاه استنفورد - به دنبال ابتکارات در زمینه‌ی به‌کارگیری کدهای اخلاقی در هوش مصنوعی هستند [۱۳]. بنابراین، می‌توان این ایده را درباره‌ی امکان اخلاق‌مندی ربات‌ها مطرح کرد: «می‌توان با به‌کاربردن الگوریتم‌ها و سیستم‌ها، داده‌ها و برنامه‌های مبتنی بر ارزش‌های اخلاقی اسلامی، از این سیستم‌های هوشمند به‌گونه‌ای در ترویج ارزش‌های اخلاقی و مقابله با مقوله‌های ضد اخلاقی در فضای سایبر و فضای فیزیکی استفاده کرد».

## ۴ تحلیل منشأ ارزش اخلاقی توصیه‌نامه‌ی یونسکو و سازگاری آن با نظریه‌ی اخلاقی اسلام

اکنون نوبت آن است که ببینیم منشأ ارزش و لزوم اخلاقی به‌کاربرده شده در این توصیه‌نامه به کدام یک از مکاتب اخلاقی نزدیک است. به نظر می‌رسد منشأ ارزش و لزوم اخلاقی و هنجارهایی که در این توصیه‌نامه به آن اشاره می‌شود، از نوع قراردادگرایی باشد. مکتب قراردادگرایی نیز ذیل مکاتب غیرواقع‌گرایی قرار می‌گیرد [۱۱]. با تأمل در برخی مفاد مقدمه‌ی سند مشخص می‌شود این سند حقوق بشر و آزادی‌ها را به تأیید و پذیرش مردم مقید کرده است. همچنین در بند ۶ بیان می‌شود: «هدف این توصیه‌نامه رسیدن به یک ابزار هنجاری پذیرفته شده در سطح جهانی است»؛ در نتیجه این مفاهیم را ملاک و منشأ هنجارهای اخلاقی معرفی می‌کند و براساس آنها «بایدها و نبایدهای اخلاقی» را در حوزه‌ی هوش مصنوعی معین می‌سازد. عبارت‌های مذکور ما را به این سمت سوق می‌دهد که بپذیریم برخی از مبانی به‌کاررفته در این متن برخاسته از مکاتب غیرواقع‌گرایی و از نوع قراردادگرایی است.

اما قراردادگرایی چه اشکال و ایرادی دارد؟ مسئله نسبی‌گرایی و کثرت‌گرایی برخی لوازم مهم قراردادگرایی هستند [۱۱]. با این وجود، مفاد بندهای ۱۳۱ تا ۱۳۴ که در حوزه‌ی نظارت و ارزیابی تأثیرات اخلاقی فناوری‌های هوش مصنوعی می‌باشد و سعی دارد روشی را برای این ارزیابی ارائه دهد، دچار مشکل اساسی می‌شوند. زیرا، بنابر کثرت‌گرایی، نمی‌توان روش واحدی را برای بررسی تأثیرات اخلاقی در کشورهای عضو ارائه داد.

مطلب دیگری که شایسته است در این کاوش به آن پرداخته شود، تبیین موضوع و هدف علم اخلاق می‌باشد. در فلسفه‌ی اخلاق دیدگاه‌های متفاوتی درباره‌ی موضوع و هدف اخلاقی وجود دارد. با تبیین برخی دیدگاه‌ها درباره‌ی موضوع و هدف علم اخلاق، رویکرد این توصیه در این مسئله نیز روشن می‌شود. همان‌طور که گذشت ارزش‌های اخلاقی در این سند مبتنی بر نظریه‌ی قراردادگرایی است. نظریه‌ی



قراردادگرایی ذیل دیدگاه وظیفه‌گرایی اخلاقی<sup>۷</sup> می‌گنجد. در این دیدگاه، معیار ارزیابی اخلاقی، عمل به تکلیف و وظیفه است [۲]. نظریه‌ی «اخلاق وظیفه» دیدگاهی است که از سوی برخی اندیشمندان علم اخلاق مغرب زمین مطرح شده است و در آن ارزش‌های اخلاقی را صرفاً ناظر به رفتارها می‌دانند و علم اخلاق را بیان‌کننده‌ی ارزش و لزوم رفتارها معرفی می‌کند [۷] و هدف اصلی اخلاقی را نیز تصحیح خود رفتار دانسته و ورای آن هدف دیگری را نشان نمی‌دهند [۱۱].

اما در دیدگاه اخلاق فضیلت<sup>۸</sup> صفات درونی و نفسانی انسان متصف به ارزش‌های اخلاقی شده، و علم اخلاق عهده‌دار بیان ارزش و لزوم این صفات هست. هدف علم اخلاق در این رویکرد آراستن نفس به کمالات نفسانی پسندیده و زدودن صفات ناپسند از آن است. افزون بر این، رفتارها و اعمال انسان که وسیله‌ای برای تحقق صفات نفسانی هستند، نیز در این رویکرد ارزش‌گذاری می‌شوند. به عبارت دیگر، هدف در این رویکرد دستیابی به کمال نفس است. برخی علمای شیعه براساس انسان‌شناسی خاص خود، همین دیدگاه را اختیار کرده‌اند. از نظر ایشان حقیقت وجود انسان، نفس مجرد اوست و کمال و نقص واقعی انسان نیز ناظر به همین نفس یا روح است. کمال و نقصی که با افعال اختیاری انسان در این دنیا به دست می‌آید در نفس او باقی می‌ماند و انسان پس از مرگ با همان‌ها محشور می‌شود [۸].

در رویکرد فضیلت‌محور، ارزش‌گذاری مربوط به اشخاص است نه به رفتار. اما این تأکید در فلسفه‌ی اخلاق نوین غربی جای خود را در رویکردی به‌شدت قانون‌پرستانه به کردار و رفتار داده است. از این رو، قواعد و اصول بر صدر نشسته‌اند [۳]. در واقع، وجه تمایز اصلی آنها این است که اخلاق فضیلت‌ناظر به ارزش‌های اخلاقی است و دیدگاه وظیفه‌گرا ناظر به الزام اخلاقی است. از این رو، مسئله‌ی اصلی در اخلاق فضیلت این است که «چگونه فردی باشیم» و در نظریه وظیفه‌محور دغدغه اصلی این است که «چه فعلی را باید انجام دهیم» [۴]. بنابراین، یک فرد ممکن است از فضایل اخلاقی بی‌بهره باشد ولی به‌قصد انجام وظیفه یک عمل اخلاقی را انجام دهد.

از این رو، نقد مبنایی و اساسی به سند توصیه‌نامه‌ی اخلاق هوش مصنوعی یونسکو این است که مفاد این توصیه‌نامه به دلیل اینکه از قسم مکاتب قراردادگرایی هست، تابع یک مکتب اخلاقی غیرواقع‌گرا و وظیفه‌محور می‌باشد. پس ارزش‌های اخلاقی آن تنها متوجه کنش و رفتار ظاهری انسان است. در نتیجه، در این سند اخلاقی اصلاً به مباحثی همچون کمالات نفسانی، رابطه‌ی انسان با خدا، تأثیر واقعی ارزش‌های اخلاقی در روح و نفس انسان و مواردی از این دست، پرداخته نشده است. اما نظریه‌ی اخلاقی مکتب اسلام با رویکرد متعالیه در دیدگاه برخی فلیسوفان معاصر مسلمان یافت می‌شود. این دیدگاه نکات مثبت دیدگاه فضیلت‌گرایی اسلامی را در خود داشته و افزون بر آن یک نوع دیدگاه غایت‌انگارانه و کمال‌جویانه می‌باشد. در این اندیشه، رفتار نیز موضوع علم اخلاق می‌باشد [۱۰]. زیرا برخی صفات نفسانی با تکرار رفتار اختیاری به دست می‌آید [۹]. در این اندیشه، هم رفتار اختیاری و هم صفات نفسانی مورد توجه است.

در نظریه‌ی اخلاقی اسلام، مفاهیم ارزش‌های اخلاقی مبتنی بر واقعیت هستند [۱۱]. از این رو این مکتب ذیل نظریه واقع‌گرا قرار می‌گیرد و همچنین این دیدگاه به‌نوعی دیدگاه غایت‌انگارانه و کمال‌جویانه

<sup>7</sup>Ethics of Duty

<sup>8</sup>Ethics of Virtue



به معنای خاص خود می‌باشد. هدف از فعل اختیاری، قرب وجودی به کمال مطلق و خداوند متعال می‌باشد. در این نظریه‌ی مبتکرانه، میان فعل اختیاری انسان و نتیجه‌ی آن رابطه‌ی ضرورت بالقیاس برقرار هست. از این رو، ارزش اخلاقی فعل اختیاری انسان تابع تأثیر آن فعل در رسیدن انسان به کمال حقیقی است. پس هرکاری به اندازه‌ای که در رسیدن به کمال حقیقی انسان مؤثر باشد، ارزنده خواهد بود و اگر تأثیر منفی داشته باشد ارزش آن نیز منفی خواهد بود و اگر هیچ ارزش مثبت و منفی نداشته باشد، خنثی خواهد بود [۱۰].

بنابراین، نظریه اخلاقی مکتب اسلام درباره ارزش‌های اخلاقی هوش مصنوعی را می‌توان این گونه تبیین کرد: «اگر چرخه‌ی حیات سیستم‌های هوش مصنوعی از اختراع و کشف گرفته تا کاربرد و استفاده از آن، در راستای این باشد که موجب کمال انسانی و تقرب وی به خداوند متعال باشد، این امر ارزشی اخلاقی خواهد داشت و بر عکس اگر فناوری‌های هوش مصنوعی موجب دوری انسان از کمال حقیقی خود باشد، ضد ارزش به حساب می‌آیند و در غیر این صورت، آن تکنولوژی خنثی بوده و دارای ارزش و یا ضد ارزش اخلاقی نمی‌باشد».

## ۵ نتیجه‌گیری

در گزارش [۱] به توصیه‌نامه‌ی یونسکو این ایراد گرفته می‌شود که در بیان نسبت ارزش‌ها و اصول باید در متن روشن‌تر عمل می‌کرده است و از کلی‌گویی‌های نابجا پرهیز می‌نموده است؛ از این رو منتقدان پیشنهاد داده‌اند که بند ۹۱ به عنوان الگویی برای نگارش سایر بندها باشد [۱]. در حالی که مفاد این بند با توجه به محتوای سایر بندها در راستای ترویج فرهنگ برابری جنسیتی می‌باشد. حتی پیشنهاد می‌شود در این سند تکرار ارزشی و فرهنگی گنجانده شود [۱]. اگر منظور از این عبارت این است که یونسکو به ارزش‌های فرهنگ اسلام نیز بها بدهد، این نکته تا حدی قابل پذیرش است؛ اما قبول تکرار ارزشی منجر به نسبی‌گرایی و کثرت‌گرایی در ارزش‌های اخلاقی می‌شود و لازمه‌ی این امر عدم امکان ارزیابی و داوری میان مکاتب مختلف اخلاقی بوده و همه به یک اندازه معتبر می‌باشند. در حالی که، تحقیق حاضر به لحاظ مبانی این سند اخلاقی را مورد بررسی قرار داد. و مشخص شد که این سند مبتنی بر قراردادگرایی بوده و در این مکتب، هدف عمل به وظیفه بدون توجه به صفات کمالی و حقیقی انسان است. اما نظریه‌ی اخلاقی اسلام جزو مکاتب واقع‌گرایی و در اندیشه‌ی برخی علما فضیلت‌محور و از منظر برخی غایت‌گرایانه و کمال‌جویانه می‌باشد. در این رویکرد افزون بر اصلاح رفتار و صفات نفسانی، تقرب به کمال مطلق و خداوند متعال مد نظر است.

از این رو پیشنهاد می‌شود در قراردادهای بین‌المللی، بررسی اسناد، اعلام نظرها و توافق‌ها و به‌طور خاص در اجرای آنها در ایران اسلامی دقت لازم به کار رود و سازگاری آن با مبانی اندیشه‌ی اسلامی لحاظ شود؛ همچنان که مقام معظم رهبری (مدظله) می‌فرمایند ما در بحث فناوری باید پیشرفت کنیم و در این بخش شاگردی و علم‌آموزی کنیم، اما نباید به توصیه‌ها و برنامه‌های آنها [غربی‌ها] خوش‌بین بوده و عمل کنیم.<sup>۹</sup> افزون بر این، پیشنهاد می‌شود در تدوین «سند ملی هوش مصنوعی کشور» متناسب با ارزش‌ها و چارچوب‌های تمدن نوین اسلامی برای حوزه‌ی اخلاق هوش مصنوعی ریل‌گذاری شود.

<sup>۹</sup> بیانات در دیدار مسئولان و محققان ستاد توسعه علوم شناختی با رهبر معظم انقلاب، <https://khl.ink/f/41471>

## مراجع

- [۱] ب، خداقلیزاده. نقد و بررسی اولین پیش نویس توصیه نامه اخلاق هوش مصنوعی (یونسکو). پژوهشگاه فضای مجازی، تهران، ۱۳۹۹.
- [۲] ح، حمدی، ح. و محیطی. ظرفیت‌سنجی اندیشه‌های اخلاقی در ایجاد نظام ارزشی تمدن نوین اسلامی، مطالعات بنیادین تمدن نوین اسلامی، ۲(۱)، ۱۳۹۸.
- [۳] ر، هولمز. مبانی فلسفه اخلاق هولمز، ترجمه‌ی مسعود علیا. ققنوس، تهران، ۱۳۸۹.
- [۴] ز، خزاعی. اخلاق فضیلت. حکمت، تهران، ۱۳۸۹.
- [۵] ابن سینا. الشفاء (الطبیعیات)، مکتبه آیت‌الله المرعشی، قم، ۱۴۰۴ق.
- [۶] صدرالمتألهین. المتعالیه فی الاسفار العقلیه الاربعه، ویرایش ۳. دار احیاء، بیروت، ۱۹۸۱م.
- [۷] ژکس. فلسفه اخلاق (حکمت عملی)، ترجمه‌ی ابوالقاسم پورحسینی، ویرایش ۲. امیرکبیر، تهران، ۱۳۶۲.
- [۸] م، نراقی. جامع السعادات، تحقیق محمد کلانتر. مؤسسه الاعلمی للمطبوعات، بیروت، ۱۲۰۹ق.
- [۹] م.ت، مصباح یزدی. دروس فلسفه اخلاق. اطلاعات، تهران، ۱۳۷۳.
- [۱۰] م.ت، مصباح یزدی. نقد و بررسی مکاتب اخلاقی، تحقیق و نگارش احمدحسین شریفی. مؤسسه آموزشی و پژوهشی امام خمینی، قم، ۱۳۸۴.
- [۱۱] م، مصباح. بنیاد اخلاق (روشی نو در آموزش فلسفه اخلاق)، ویرایش ۷. مؤسسه آموزشی و پژوهشی امام خمینی، قم، ۱۳۹۰.
- [12] ANDERSON, M., AND ANDERSON, S. L. Machine ethics: Creating an ethical intelligent agent. AI magazine, 28(4), 2007.
- [13] BODDINGTON, P. *Towards a code of ethics for artificial intelligence*. Springer, 2017.
- [14] LUCCI, S., AND KOPEC, D. *Artificial intelligence in the 21st century: A living introduction, mercury learning and information*. 2016.
- [15] RUSSELL, S., AND NORVIG, P. *Artificial Intelligence: A Modern Approach*, 4th ed., Prentice Hall, 2020.
- [16] UNESCO. Recommendation on the ethics of artificial intelligence. <https://en.unesco.org/artificial-intelligence/ethics>, Ret: 6 Feb 2022.

## واکاوی بنیاد فکری نظام سایبرنتیک و راهکار مقابله با تهدیدات آن در نظام ولایت

رضوان هامانی<sup>۱</sup>، زهرا حبیبیان<sup>۲</sup>

<sup>۱</sup> طلبه سطح سه فلسفه اسلامی جامعه الزهرا (س) قم  
و فارغ التحصیل کارشناسی ارشد فیزیک نظری دانشگاه شهید بهشتی  
hamani1360@gmail.com

<sup>۲</sup> طلبه سطح سه فلسفه اسلامی جامعه الزهرا (س) قم  
و دانشجوی کارشناسی ارشد فلسفه و کلام اسلامی، دانشکده الهیات دانشکدگان فارابی دانشگاه تهران  
habibian213@gmail.com

### چکیده

مفهوم سایبرنتیک کاملاً مجزا از مفهوم تکنولوژی است و ریشه در مباحث نظری و علوم انسانی دارد. بنیاد فکری این پدیده‌ی نوین با هدف حاکمیت بر اساس جریان اطلاعات طرح‌ریزی شده است. بنیان‌گذار این نظریه، نوربرت وینر، با الهام از الهیات یهود، کنترل جریان اطلاعات و آگاهی را ابزار کنترل جوامع معرفی می‌کند. بر این اساس، از آنجا که گستره‌ی نفوذ شیطان در قوای ادراکی انسان در محدوده وهم، خیال و حس امکان‌پذیر است، وینر حکمرانی بر باورهای بشری و کنترل قوه خیال انسان‌ها را ابزار حاکمیت سلطه و ایجاد نظم نوین جهانی می‌داند. اما قوه ادراکی که از دسترس شیطان خارج است، قوه عاقله انسان است. چنانچه بر طبق روایت تکامل عقول در عصر ظهور، بشریت در پرتو تبلیغ و تربیت حجت الهی با شکوفا شدن عقول در مسیر تکامل عقلانی قرار می‌گیرد. لذا در مقابله با حاکمیت سلطه، مبانی حاکمیت ولایت، بر محور عقلانیت پایه‌ریزی می‌شود؛ بنابراین راه مقابله با نفوذ شیطان و نیل به معرفت توحیدی از طریق حجت درون و برون و مدیریت و اشراف عقل بر کارکرد قوای ادراکی امکان‌پذیر است و راهکار مقابله با تهدیدات حاکمیت سلطه و استقرار تمدن نوین اسلامی این است که عقلانیت را در جامعه تقویت و حقایق را جهادگونه تبیین کرد.

**کلمات کلیدی:** سایبرنتیک، نوربرت وینر، نظام ولایت، قوه خیال، عقلانیت، جهاد تبیین.

### ۱ مقدمه

دانش سایبرنتیک (Cybernetics) یا رایانیک، دانش کنترل و حاکمیت بر پدیده‌های هوشمند از طریق کنترل و اشراف بر جریان اطلاعات است. مبحث این دانش طرح‌ریزی حاکمیت بر اساس جریان اطلاعات می‌باشد و امروزه جایگزینی برای علوم سیاسی شده است. زیرا مدیریت فضای فکری در افکار عمومی خارج از دایره

حاکمیت‌هاست و راه سلطه بر بشریت و تضعیف حاکمیت‌ها، کنترل فضای سایبری کشورهاست. بنیانگذار این نظریه نوربرت وینر، دانشمندی یهودی با اندیشه‌های پوزیتویسمی است، که این نظریه را نخستین بار در سال ۱۹۴۸ میلادی در کتاب «سایبرنتیک: کنترل و ارتباط در جانداران و ماشین» مطرح ساخت. وینر دو سال پس از آن در کتاب «استفاده انسانی از انسان» دلالت‌های اخلاقی و جامعه‌شناختی اثر قبلی را بیان کرد و در نهایت در سال ۱۹۶۶ میلادی اثر «خدا و گولم: یادداشت‌هایی در باب دست‌یازی‌های سایبرنتیک بر دین» را نگاشت و مبانی الهیاتی که زیر بنای تفکر او در تدوین دانش سایبرنتیک است را عنوان کرد. او با نفی اوصاف مطلق خداوند، خلقت انسان را خلق یک موجود زنده به دست موجود زنده دیگر می‌داند و خلق ماشین به دست انسان را تداوم جریان خلقت معرفی می‌کند و تکثیر ماشین را در مشابهت با تولید مثل ممکن می‌داند. او خدا را در رقابتی ناعادلانه با شیطان تصور می‌کند که در نهایت جبهه اهریمن همچون ماشینی که خالق خود را در بازی شکست می‌دهد، با اتکا بر تجارب خود و با اشراف بر اذهان و کنترل باور انسان‌ها، پیروز میدان خواهد بود و حکمرانی بر جهان را به قبضه خود در خواهد آورد.

اما چنانچه در آیات و روایات آمده، گستره نفوذ شیطان در قوای ادراکی انسان در محدوده وهم، خیال و حس امکان پذیر است و عقل انسان از دسترس شیطان خارج است. بنابراین در تقابل با این تفکر که امروزه زیر بنای نظام سایبرنتیک است، نظام ولایت که مالکیت حقیقی عالم را از آن خدا می‌داند، بر محور عقلانیت پایه‌ریزی شده و با اتکا بر عقل به عنوان حجت درون و حاکمیت انسان کامل به عنوان حجت برون، قوای ادراکی انسان‌ها را به مدیریت عقل در خواهد آورد و انسان را به غایت آفرینش خواهد رساند.

در این پژوهش به روش تحلیلی-توصیفی و با نظر به آثار وینر، مبانی الهیاتی نظام سایبرنتیک از منظر بنیان‌گذار این دانش مطرح می‌شود و با تأکید بر گستره نفوذ شیطان، راهکار مقابله با تهدیدات این نظام مطرح می‌شود تا در مواجهه با این مسئله نظریه پردازان جامعه اسلامی با آگاهی از هدف اصلی ایجاد نظام سایبرنتیک بر بارورسازی عقلانیت مردم اهتمام داشته باشند.

## ۲ مبانی نظام سایبرنتیک

### ۱.۲ پیشینه‌های الهیاتی و فلسفی نظریات حاکمیت و سلطه

اصل مشترک همه جوامع، نیاز به حاکمیت برای رفع فروپاشی و رسیدن به نظم در پرتو سلطه است. بررسی نظریات جامعه‌شناسانه و سیر تطور تاریخی حاکمیت در جوامع مختلف، ریشه‌های الهیاتی و فلسفی آن‌ها را در پیاده‌سازی سلطه و حاکمیت عرضه می‌دارد. از پیدایش انسان‌های اولیه و شکل‌گیری تمدن‌های ابتدایی گرفته تا کنکاش در سیر تمدن‌های مختلف امروزی، در جای جای سرزمین‌های بشری، مبانی فلسفی از قبیل اندیشه‌های الهیاتی سنتی یا امتدادی<sup>۱</sup>، اندیشه الحادی، نگرش طبیعت‌گرایانه، قدرت، سود و سرمایه جریان داشته است. پس از قرون وسطی، گرایش‌های ضد کلیسا و با ابتنا بر نگرش‌های پوزیتویستی، با رویکرد روشنفکر مآبانه علم بر ضد دین که واکنشی در مقابل الهیات به انحراف رفته مسیحیت و یهودیت تحریف شده بود، غلبه و جریان یافت (مطهری، ۱۳۹۲، ۷۳) [۱۳]. و پیشرفت علوم بر مبنای ضد دینی، به گسترش

<sup>۱</sup> الهیات امتدادی نگرش الهیاتی است که در امتداد آن نظام ولایی شکل گرفته است

این مبنای فکری انجامید. از این رو فضای فکری یا فضا سازی فکری جوامع، در پذیرش سلطه بر مبانی خاص، موثر بوده است.

آخرین محصول تلاش غرب در زمینه حاکمیت، دستیابی به مفهوم آگاهی<sup>۲</sup>، به عنوان ابزار سلطه است، به این معنا که کنترل جوامع از طریق کنترل جریان اطلاعات و آگاهی آن‌ها انجام پذیر است. پیش از این برای کنترل جوامع، تسلط بر پنج رکن تشکیل دهنده قدرت، شامل سیاست، فرهنگ، اقتصاد، اجتماع و امنیت، مطرح بود. اما با پیشرفت‌های علمی به تدریج در حال گذر از این چارچوب حکمرانی و ورود به عرصه حاکمیت بر اساس کنترل جریان آگاهی هستیم.

این رویکرد در نظر ابتدایی، علمی یا سیاسی تلقی می‌شود؛ در حالی که نوعی تلقی با بنیاد الهیاتی و اندیشه فلسفی است. در این نگرش که نگرشی مشرکانه است و نه الحادی؛ حاکمیت انسان ضد خدا، بر انسان رخ می‌دهد (معمارزاده، ۱۳۹۹، ۱) [۱۷]. پایه‌های اندیشه فلسفی هستی‌شناسانه، انسان‌شناسانه و بنیاد معرفتی مکاتب، تعیین‌کننده نگرش سیاسی و اجتماعی جوامع، به هویت، غایت، تعالی و تکامل انسان است و ثمره جامعه تنیده در افکار انسان‌گرایانه<sup>۳</sup> و پوزیتیویستی، با ثمره جامعه خداگرایانه و متکی بر فلسفه اسلامی، متفاوت است و به لحاظ قیاس تاریخی، سلطه جهان اسلام، که امروزه مورد تغافل بررسی‌های علمی واقع شده، با سلطه جهان غرب پس از رنسانس، از لحاظ بنیادهای معرفتی قابل قیاس نیست. اگرچه غرب پس از رنسانس در تقابل با مسیحیت و یهودیت انحرافی و برافراشتن پرچم علم بر ضد دین و خدا، ادعای الحاد و هدم الهیات را دارد؛ اما آنچه به واقع از این رویکرد نوین مشاهده می‌شود، منشأ یافته از اندیشه‌های سکولار و مدرنیته است، که قصد دارد انسان را در جایگاه خدا بنشانند و انسان را نقطه آغاز آفرینش در نظر گیرد. در حالی که خدایی انسان بر زمین و جاودانگی انسان، همه از سنخ نگرش‌های الهیاتی هستند (همان).

## ۲.۲ مفهوم‌شناسی سایبرنتیک

واژه سایبرنتیک<sup>۴</sup> اولین بار توسط نوربرت وینر ریاضیدان و اندیشمند آمریکایی-لهستانی، برای نام‌گذاری دانش کنترل جوامع از طریق کنترل جریان اطلاعات، که خود به صورت رسمی پایه‌گذاری کرده بود، ابداع شد. او در آثار خود بر این نکته تأکید دارد که «تا دوران اخیر، واژه‌ای که مبین این گروه افکار باشد وجود نداشت، و برای دربرگرفتن این حوزه افکار به تمامه در یک اصطلاح، مجبور به اختراع واژه‌ای مخصوص شدم. لذا سایبرنتیک را که از واژه یونانی کوبرننتیس<sup>۵</sup> به معنای «سکاندار» و منشأ واژه انگلیسی گاورنور<sup>۶</sup> به معنای «تنظیم کننده» انتخاب کردم» (وینر، ۱۳۶۶، ۱) [۱۶].

نظریه سایبرنتیک که در سال‌های بعد به نظریه اطلاعات مشهور شد، تکمیل شده نظریه ریاضی ارتباطی<sup>۷</sup> است که وینر در مقاله‌ای در سال ۱۹۴۶ مطرح کرد. وینر اعتقاد داشت سایبرنتیک علم کنترل و جریان

<sup>2</sup>Consciousness

<sup>3</sup>Humanistic

<sup>4</sup>Cybernetics

<sup>5</sup>Kubernetes

<sup>6</sup>Governor

<sup>7</sup>Mathematical Theory of Communication

اطلاعات در سیستم‌ها، ارگانیزم‌ها و جوامع است، در نتیجه با اغلب شاخه‌های علم مرتبط است و خود یک رشته و شاخه علمی نوین به شمار می‌رود (گراوندی، ۱۳۹۴، ۱) [۱۸].

وینر ثمره نظری کار خود را در قالبی فلسفی و با رویکردی سیاسی و جامعه‌شناسانه، در سطح کلان ارائه می‌دهد و مبنای طرح‌ریزی اقدام خود را کتاب‌های «سایبرنتیک»، «استفاده انسانی از انسان‌ها» و نیز «خدا و گولم» ارائه می‌دهد.

## ۳.۲ ریشه فکری وینر در ارائه نظام سایبرنتیک

اثر نخستین نوربرت وینر با عنوان «سایبرنتیک»، کتابی است فنی که بر اساس دانش ریاضیات و فیزیک جدید نگاشته شده و مهم‌ترین مبنای نظری گسترش کامپیوتر و ظهور شبکه جهانی وب است. وینر در کتاب بعدیش، با عنوان «استفاده انسانی از انسان‌ها»، با تأثیر از فلسفه لایبنیتس و با اشاره به نوآوری‌های گیبز در قانون عدم قطعیت فیزیک کوانتوم به مقایسه انسان و ماشین می‌پردازد. او واژه‌های متافیزیکی همچون «روح» و «زندگی» را بی‌پایه و اساس می‌داند و با نگاهی پوزیتویسمی، ایجاد نسل جدیدی از ماشین‌ها که توانا در نقض اصل دوم ترمودینامیک باشند را ممکن می‌داند که در نهایت با حرکت بر خلاف افزایش آنتروپی جهان، رویای جاودانگی درعالم ماده را دست‌یافتنی خواهند کرد (وینر، ۱۳۶۶، ۲۳ و ۳۰) [۱۶].

او به تأثیر از اندیشه‌های پوزیتویسمی راسل در اثر «خدا و گولم» با نفی معرفت و قدرت مطلق و یگانگی خداوند در عبودیت، ابداع ماشین به دست بشر را از سنخ خالقیت خدا می‌داند. و در مطالعه رابطه دین و علم رهایی از قید و بندهای حفظ تعهد بر تکریم امور متافیزیکی را رسالت یک دانشمند متفکر و پارسا می‌داند و قدرت، معرفت و پرستش را از دریچه علوم تجربی بدون تقیّد بر این عقیده که: «باور دارم چون باورپذیر نیست» بررسی می‌کند [۲۰].

از نظر وینر طبیعی است که آفرینش ماشین به دست ماشین به شکل خودش، تداوم جریان خلقت انسان به دست خدا به شکل خودش است و در اصل ایجاد شکاف بین جاندار و غیرجاندار، متعاقباً موجب شکاف بین خالق و مخلوق می‌شود (همان). او تقابل میان شیطان و خدا را به بازی شطرنجی تشبیه می‌کند که خدا به عنوان عالم مطلق و مالکِ تئوری بازی، بازیکن همیشه برنده بازی است و به اعتقاد او این به معنی تقلیل بازی در حد ابتذال است (همان).

او در مبنای خود، خواسته یا ناخواسته به قلمرو نفوذ شیطان در قوای ادراکی انسان، یعنی قوه خیال، توجه کرده و به مطالعه روند استفاده از آگاهی و اطلاعات، جهت دادن به آن و مدیریت و کنترل اذهان از طریق قوه خیال پرداخته است. این همان ساحتی است که بر طبق اندیشه‌دینی و فلسفه اسلامی، قابلیت تسخیر انسان توسط شیطان از طریق آن امکان‌پذیر است. وی تحت تأثیر اندیشه‌های الهیاتی و تحت سیطره نظام فلسفی پوزیتویسمی، نظام سایبرنتیکی خود را در سطح جامعه و سیاست امتداد داده و طرح‌ریزی کرده است. این تفکر به جای آنکه از مفهوم «از خدا ناشی شدن» استمداد بگیرد؛ مفهوم «به خدا تبدیل شدن» را به کار می‌گیرد و از آنجا که در کتاب آفرینش تورات، «درخت دانش» به عنوان میوه ممنوعه معرفی شده است، وینر با الهام از این الهیات، راه «به خدا تبدیل شدن» را در کنترل جریان دانش و اطلاعات بشر و جوامع یافته است.



## ۳ گستره نفوذ شیطان در قوای ادراکی انسان

### ۱.۳ جایگاه قوه خیال در قوای ادراکی

قوه خیال یکی از قوای ادراکی باطنی نفس است که خزانه نگهداری صور دریافتی توسط حس مشترک است. یکی از کارکردهای خیال، نقش دوسویه خیال در انعکاس معانی باطنی در صفحه نفس و گذار از طبیعت به ملکوت عالم است. در صورت هماهنگی و اعتدال این قوه با سایر مراتب و قوای نفس و به کارگیری صحیح آن، این کارکرد فطری سعادت انسان را تأمین خواهد کرد. زیرا هر انسانی بالوجدان می‌یابد که در انجام افعال خود دارای اراده و اختیار است. از طرفی فلاسفه مبدأ شکل‌گیری اراده و صدور افعال اختیاری را صورت‌های خیالی می‌دانند؛ زیرا تا زمانی که انسان به چیزی علم نداشته‌باشد، هیچ شوق و میلی به آن نخواهد داشت. در این صورت یا این تصور خیالی تصدیق عقلانی را نیز به دنبال دارد و در نتیجه صدور فعل اختیاری از انسان موافق با تعالی و کمال حقیقی وی است؛ یا صرف تصور خیالی موجب شکل‌گیری شوق و اشتیاق مؤکد و سپس اراده بر انجام آن فعل می‌شود و هیچ تصدیق عقلانی مؤید و کمک‌کار خیال نیست. در این حالت، ممکن است عوامل گوناگونی غیر از عقل، مانند شیطان و شهوت و امیال حیوانی، بر خیال تأثیر بگذارند و موجب سوء اختیار و انحراف انسان از تعالی و کمال حقیقی شوند (یوسفی سوته، ۱۳۹۸، ۷۶) [۱۵].

بر اساس انسان‌شناسی اسلامی، نفس تحت تأثیر خیالاتی که خود آن را انتخاب و نگهداری کرده‌است به فعل و انفعالات پرداخته و بر اساس نوع خیالات از حالات انسانی به ملکاتی که سازنده جوهر ذاتی او و تعیین‌گر سعادت یا شقاوت اوست تبدیل می‌شود (صدرالدین شیرازی، ۱۳۶۳: ۲۰۳) [۹]. اگرچه مرتبه خیال فروتر از ساحت عقل و ورای مرتبه حس است، به جهت حلقه میانی بودن بین عقل و حس محل جمع اضداد است. هر آنچه عقل به جهت تجرد، و حس از روی محدودیت و انحصار بر جزئیات، نمی‌یابد، مرتبه خیال ظرف کشف آن است؛ تا حدی که وحی بر نبی، رؤیا و تمام امور خلقی و خلاقیت‌ها و افعال انسانی انسان، در تمام مراتبش به واسطه قوه خیال صورت می‌گیرد. با این تفاوت که در مرتبه بالای خیال که مثال منفصل است نفس به انشاء و خلق مستقل از بدن قدرت پیدا می‌کند (جوادی آملی، ۱۳۹۶: ۴۶۷) [۴].

این قدرت بر خلق را در بیان آیت‌الله حسن‌زاده آملی نیز می‌توان یافت که می‌فرماید: «خداوند نفس را مثال برای افعال خودش قرارداد؛ یعنی به او مملکتی شبیه مملکت خودش داد تا هر چه می‌خواهد بیافریند و هر چه اراده می‌کند ایجاد شود» (حسن حسن‌زاده آملی، ۱۴۱۷، ۴۱) [۳].

### ۲.۳ قوه خیال قلمرو اغوا و اضلال شیطانی

شیطان از آن حیث که از جنس آتش و از تبار جنیان است؛ از دیدگان انسان، پوشیده و پنهان بوده؛ اما در عین حال، به گونه‌ای با او زمزمه می‌کند و به کارهای باطل و سوسه می‌نماید؛ به گونه‌ایی که انسان تفاوتی میان آن‌ها و افکار خودش نمی‌گذارد و آن‌ها را افکار خویش می‌پندارد. از نظر علامه طباطبائی، زمزمه‌ها و سوسه‌های شیطان فقط تا محدوده ادراکات جزئی و محسوس است (طباطبائی، ۱۳۹۴، ۴۰) [۱۰]؛ زیرا شیطان تجرد برزخی دارد و محدوده شیطنت وی نشئه طبیعت و خیال است. از این رو، دسترسی به نشئه عقل و ادراکات عقلانی برای وی مقدور نیست. اما نفوس انسان‌هایی که تجرد خیالی دارند و هنوز به مقام

تجرد عقلی صعود نکرده‌اند، همواره مورد هجوم و حملات زهرآگین القائات شیطانی قرار می‌گیرند (یوسفی سوته، ۱۳۹۸، ۱۲۲) [۱۵].

بر این اساس آیت الله جوادی آملی می‌فرماید: «سقف تجرد شیطان وهم و خیال است و انسانی که از طریق قوه قدسیه، عقل کامل شده یا به مقام اخلاص بار یافته‌است؛ شیطان به خواسته‌های مشروع و موانع تحقق آن‌ها آگاهی نمی‌یابد و قدرت راهزنی نسبت به چنین انسانی را ندارد، بلکه قوه واهمه که محل ظهور شیطنت و وسیله مکر و حیلست است از باب «و مکررو و مکرر الله و الله خیر الماکرین» (آل عمران، آیه ۵۴) در استخدام او قرار می‌گیرد» (جوادی آملی، ۱۳۹۰، ۱۸۵) [۵].

وجود شیطان در نظام عالم تکوین، زمینه آزمایش انسان را با شکل‌گیری جهاد درونی میان عقل و خیال فراهم می‌سازد. اضلال و اغوای شیطان از طریق وهم و خیال و حس در قالب تدلیس، تلبیس، تسویل، تأییس و تسویف برای آدمی پیش می‌آید. قلب آدمی کانون القا و هجوم شیطان است که از طریق اندام‌ها و قوای حسی و شیطنت وهم رخ می‌دهد (مؤدب و سالمی، ۱۳۹۹، ۲۰۵). بنابراین شیطان به تنهایی مانعی برای تعالی انسان نیست؛ بلکه هر انسانی با سوء اختیار و تمرد از فرامین عقلی، گرفتار تسویلات و تزییناتی می‌شود که شیطان با دخالت در صورت‌های خیالی ایجاد کرده‌است و وی را در علوم نظری و عملی دچار مغالطه کرده و منجر به تسلط خیال بر عقل می‌گردد (یوسفی سوته، ۱۳۹۸، ۱۲۴) [۱۵]. از این رو خیال می‌تواند سعادت و شقاوت انسان را رقم بزند؛ نفس می‌تواند در مرتبه خیال تحت مدیریت عقل درآید و از امور مادی و توهمات، تزکیه و تنزیه شود، ظرف علوم و معارف معنوی گردد یا می‌تواند از جنود شیطان باشد و موجب هلاکت و گمراهی انسان شود (جوادی آملی، ۱۳۷۸، ۵۱۷) [۶].

فطرت الهی آدمی، خاستگاه خیر مطلق و ضامن سعادت انسان است؛ ولی این ضمانت تا هنگامی است که انسان گرفتار طبیعت و دام‌های ابلیس نشود. این تنزه از طبیعت و حجاب‌هایش، با تبعیت حیات طبیعی انسان از حیات حقیقی‌اش رخ خواهد داد. نشانه این تبعیت، فرمانروایی عقل بر وهم، حس و به‌ویژه خیال است. جهت‌گیری صحیح دستگاه ادراکی، به عنوان مقدمه و شرط کمال و سعادت، مشروط به این فرمانروایی است. نیل به معرفت توحیدی از طریق حجت درون و برون، که غایت آفرینش انسان دانسته شده، و مدیریت و اشراف عقل بر کارکرد قوای ادراکی، راه مقابله با نفوذ شیطان است (مؤدب و سالمی، ۱۳۹۹، ۲۰۵) [۱۴].

## ۴ نگرش متقابل نظام‌ولایی

### ۱.۴ حاکمیت از منظر نظام‌ولایی

بر مبنای نظام‌ولایی، مالکیت حقیقی عالم از آن خداست و این حق در سیری تشکیکی و تنازلی، مبتنی بر اذن او، بر انبیاء و سپس معصومین به جهت عصمت و برخوردارگی از شایستگی‌های روحی و معنوی و پاکی از هر نوع غرض‌ورزی و آفت‌های انسانی جریان دارد و در زمان غیبت ایشان بر اساس «اصل تنزل تدریجی» بر نزدیکترین ایشان از لحاظ فقهی، تدبیری و کفایت سیاسی به نحو انتصابی واقع می‌شود. از این رو سربان قوانین و مبانی در این نظام، بر اساس تشریح حکیمانانه خداوند پیش می‌رود (مصباح یزدی، ۱۳۹۴، ۲۷۱-۲۷۲) [۱۲].

طبق این دیدگاه انسان تنها مخلوقی است که سزاوار جانشینی خداوند در زمین است و همانطور که بیان شد، به جهت قوه خلاقه‌ای که در نهاد او نهادینه شده می‌تواند حکمران سرزمین وجودی خود و حتی خارج از خود باشد و بر عوالم خارج از وجود خویش تأثیر بگذارد، آن‌گونه که همچون خالقش، قدرت خلق و امر پیدا کند (یوسفی سوته، ۱۳۹۸: ۱۱) [۱۵].

از سوی دیگر، اساس نظام‌ولایی مبتنی بر توحیدمحوری است و نظام توحیدی متکامل هنگامی محقق شده و تعالی بشری را به دنبال دارد، که حاکمیت الهی در تمام ساحات معرفتی، عملی و ابزاری عقل انسان سیطره یابد و این امر هنگامی رخ می‌دهد که سامان عقلی بشری در پرتو تبعیت از ولایت مأذون چیدمان یابد. رویکرد انبیاء و اولیاء الهی و در امتداد آن ائمه علیهم السلام و ولی فقیه، که همگی چنین همان نظام‌ولایی است، تأکید و تکیه بر تعقل و به فعلیت رساندن دفینه‌های عقول انسانی، از طریق ایجاد بستر مناسب برای رساندن انسان به قدرت مهار خیال خویش با عقل است.

فلسفه و حکمت اسلامی که به نوعی پشتوانه نظام‌ولایی است، با مؤیدات قرآنی و روایی از تأثیر قوه خیال در تعالی یا تنازل انسانی و فقدان یا وجدان خطا در او اشاره دارد (صدرالدین شیرازی، ۱۳۶۳، ۲۰۳) [۹]. قدرت خیال خلاقه انسانی، در مسیر عبودیت خدای کامل ادیان حقیقی ابراهیمی، او را به قدرت خلق هم می‌رساند. و انسان با سیطره عقلانی و الهی بر خیال خود می‌تواند از افسار محسوسات درآید و آن را به سلطه خود درآورد.

## ۲.۴ تأکید بر عقلانیت

در نگرش نظام‌ولایی انتخاب‌ها، اراده‌ها، حاکمیت و هدایت، همگی بر اساس بارورسازی قوه عقلانی و اندیشه آدمی است. ولایت فقیه نیز در چارچوبی مبتنی بر فطرت و عقلانیت تبیین شده است. مراد از عقلانیت نظام ولایی، نوعی عقلانیت فطری با لایه‌های مختلف است و عقلانیت ابزاری، یکی از لایه‌های آن است که تنها در صورت سیطره عقل کل نگر ایمن از انحراف است.

رسالت دین در نظام‌ولایی بارورسازی عقل است، احادیث و روایات بسیاری بر سیطره عقل بر قوه خیال اشاره دارد. تلاش انبیاء و اولیاء بر این است که قوه‌ی عاقله انسان به اختیار خود مهار قوه‌ی خیال را به دست بگیرد، از این رو باید بتواند قوه‌ی خیال را تحت سیطره و کنترل خود قرار دهد، وگرنه نفس انسان دچار تشتت و کثرت می‌شود و به مرتبه حیوانی و حتی پست‌تر سقوط کرده و از تعالی خود باز می‌ماند (یوسفی سوته، ۱۳۸۹، ۶۲) [۱۵].

با توجه به فلسفه اسلامی و روایات مؤید بر آن، اثر شیطان در پیدایش مغالطات انسانی تا جایی است که انسان هویت خویش را از دست داده و حقیقتاً به شیطان و حیوان تبدیل شود (همان، ۱۷) [۱۵]. از این رو مهار افسار خیال در پرتو عقل الهی به تعالی انسان و رفع سوء استفاده‌های ظالمانه حاکمیت‌های غیر حق، منجر می‌شود.

### ۳.۴ ظهور و عصر تکامل عقول

شکوفایی عقل رسالت همه انبیاء و اولیا بوده است. مردم در عصر ظهور در اثر تجربه و بلوغ تاریخی، آمادگی لازم برای تکامل عقول را خواهند داشت و امام رسالت جهانی خویش را با تکامل عقول انسان‌ها آغاز می‌کند. بر اساس برخی احادیث، عقول در عصر ظهور تکامل می‌یابد و ابزار این اجماع و تکمیل عقول، دستان پرتوان ولایت است.

در زمینه عقلانیت در عصر ظهور، روایات متعددی وارد شده‌است که در این میان، روایت تکامل عقول اهمیت فراوانی دارد. این حدیث به روایت امام باقر و به سند صحیح در اصول کافی چنین نقل شده: «زمانی که قائم ما قیام کند دست لطف و رحمتش بر سر بندگان قرار دهد (یعنی به بندگان توجه کند) پس اندیشه و عقل‌هایشان را جمع کند و آنها را کامل سازد (تا حقایق و واقعیت‌های زندگی را بخوبی درک کنند و بجای پیروی از خواسته دل، از عقل پیروی کنند و تن به خواسته آن دهند)»<sup>۸</sup> (کلینی، ۱۳۸۷، ۴۱) [۱۱].

همان‌گونه که در برخی فرهنگ‌ها ذکر شده، «ید» کنایه از ولایت است (زمخشری، بی‌تا، ۷۱۲) [۸] و منظور از ولایت در اینجا، ولایت عام است؛ چه ولایت الهی و چه ولایت قائم (ع) و چه ولایت امام که تابع ولایت خداوند متعال و در طول آن و ناشی از تفویض الهی است. بنابراین در بیان مقصود آیه کسانی که جمع شدن عقل را ناظر به اجتماع و اجماع مردم دانسته‌اند، اختلافی در چگونگی جمع شدن عقول ندارند و کیفیت آن را تبلیغ و تبیین مکتب نورانی اسلام و تربیت، که همان پیاده کردن ایدئولوژی واحد اسلامی است، دانسته‌اند (دریگوند، ۱۳۹۴، ۵۷) [۱۹].

حاصل شدن سعادت و حقیقت حیات انسانی در جنبه‌های مختلف زندگی و رسیدن به کمال مطلوب، هدف نهایی انزال کتب و رسالت همه انبیاء و اولیای الهی بوده‌است. این هدف به سرمنزل مقصود نخواهد رسید؛ مگر در سایه هدایت عقل نظری و راهبردهای عقل عملی و کمال این دو. این همان وعده حتمی خداوند متعال است که به رهبری آخرین حجت الهی تحقق می‌یابد (همان، ۶۰). علامه جوادی آملی «آثاره دفائن عقول» را از برترین برنامه‌های وجود مبارک امام عصر دانسته‌است (جوادی آملی، ۱۳۸۷، ۱۸۶) [۶].

امیرالمؤمنین (علیه الصلاة والسلام) در خطبه نهج‌البلاغه به این مهم اشاره فرمود که علت بعثت پیامبر (ص) و پیامبران بزرگ الهی را این‌گونه معرفی کرده‌است: پیامبر آمده تا انسانها را به فطرت انسانی و سرشت انسانیت که همراه با شرف و کرامت است برگرداند؛ نعمت‌های فراموش شده الهی را به یاد آنها بیاورد و خردهای دفن شده را مبعوث کند<sup>۹</sup> (سیدرضی، ۱۳۹۴، ۱۵) [۲].

بنابراین بر خلاف مکاتب غربی، ما معتقدیم در آینده، دستان پرتوان ولایت بر سر مردم دنیا قرار می‌گیرد و بشریت در پرتو تبلیغ و تربیت حجت الهی از نیروهای نهفته و توانایی‌های خفته خویش بهره‌مند می‌شود و با شکوفا شدن عقول‌شان در مسیر تکامل عقلانی قرار می‌گیرند. امام سطح عقلانیت جامعه را در هر سه حوزه

<sup>۸</sup> الْحُسَيْنُ بْنُ مُحَمَّدٍ عَنْ مُعَلَّى بْنِ مُحَمَّدٍ عَنِ الْوَشَاءِ عَنِ الْأَمْتَنِيِّ الْحَنَاطِ عَنِ قُتَيْبَةَ الْأَعْمَشِيِّ عَنِ ابْنِ أَبِي يَعْفُورٍ عَنْ مَوْلَى لَبْنِي شَيْبَانَ عَنْ أَبِي جَعْفَرٍ عَلَيْهِ السَّلَامُ قَالَ: إِذَا قَامَ قَائِمُنَا وَضَعَ اللَّهُ يَدَهُ عَلَى رُؤُوسِ الْعِبَادِ فَجَمَعَ بِهَا عُقُولَهُمْ وَ كَمَلَتْ بِهِ أَحْلَامَهُمْ.  
<sup>۹</sup> «لَيْسَتْ أَدْوَاهُ مِثْقَالَ فِطْرَتِهِ وَ يُدْكَرُوهُمْ مَنْسِي نِعْمَتِهِ ... وَ يُشِيرُوا لَهُمْ دَفَائِنَ الْعُقُولِ» (خطبه ۱)

عقلانیت معرفتی، اخلاقی و ابزاری شکوفا می کند (رحیم پور ازغدی، ۱۳۸۸، ۵۹) [۷].

## ۵ راهکار مقابله با تهدیدات نظام سایبرنتیک

تقابل با نظام سلطه گر از اصول اساسی سیاست خارجی نظام اسلامی است و همانطور که بیان شد، در جایی که عرصه این سلطه گری قوه خیال بشریت است راهکار مقابله با آن بارورسازی عقلانیت بشر و مهار قوه خیال به دست عقل است و در این مهم «جهاد تبیین» یکی از نیازهای اساسی جامعه امروز است. تبیین به معنای روشنگری و بیان حقیقت و واقعیت است. در حقیقت آنچه در تبیین مدنظر است، زدودن غبار بدفهمی، تحریف و کج فهمی از مفاهیم و معارف اسلامی و همچنین فهمیدن تحلیل های نادرست، غلط و مغرضانه از رویدادها و پیشگیری از تحریف و دریافت نادرست است؛ بنابراین، تبیین در جهت روشنگری است، بدون جهت گیری خاصی که بخواهیم مطلبی را توجیه کنیم یا امر نادرستی را درست جلوه دهیم. وجه تمایز روشی که منجر به روشنگری می شود با سایر روش ها، در مواجهه عقلانی با پدیده هاست. به عبارتی دیگر روشنگری برخلاف جریان رادیکال ایدئولوژیک که هر متن را با فرامتن خود تعریف می کند، در دایره استدلال و عقلانیت می گنجد. لذا ماهیت تبیین در دایره تفکرات اسلامی، عیار حق و باطل است. تبیین در دو امر اندیشه و پدیده های تاریخی، باید روایتی را پدید آورد که اولاً از دل عقلانیت بیرون آمده باشد و ثانیاً «حقیقی» باشد. لذا، در جهاد تبیین بر همگی واجب است تا آینده ای روشن براساس واقعیات و عقلانیت به مردم نشان دهند.

اگر بخواهیم تبیین را در معارف اسلامی ریشه یابی کنیم، مشاهده می کنیم که اصولاً پیامبران برای تبیین آمده اند؛ تبیین حقایق عالم، تبیین وجود خود انسان، تبیین ظرفیت های انسان و تبیین راه تعالی انسان در رسیدن به هدف آفرینش. به همین جهت، یکی از نام های قرآن کریم بیان است: «هَذَا بَيَانٌ لِلنَّاسِ»؛ قرآن تبیین کننده ای برای مردم است. رسالتی که پس از وفات پیامبر (ص)، بر عهده حضرت صدیقه طاهره سلام الله علیها قرار گرفت، رهبری جریان تبیینی ولایت امیرالمؤمنین علیه السلام بود که با خطبه فدکیه در مسجدالنبی اقدام به استدلال بر علیه خلفای ظالم کرد. خطبه های امیرالمؤمنین نیز مملو از تبیین واقعیاتی است که در جامعه آن روز مطرح بود. مبنای قیام حسینی نیز تبیین بود. مسیری که حضرت به نام خط تبیین و به نام جهاد تبیین از منی و عرفات آغاز کرد، همان خطی است که حضرت زینب کبری سلام الله علیها در ماجرای عاشورا و شام ادامه داد.

یکی از دلایلی که بسیاری از تبیین ها در مورد وقایع تاریخ رخ نداده است، نبود زیرساخت های درست در ایجاد تبیین است. خلأ این زیرساخت می تواند به جهت بازتولید استدلال های معطوف به هدف باشد، یا به سبب وجود رسانه هایی که قدرت تأثیر بر افکار عمومی را داشته باشند. در هر صورت عدم وجود زیرساخت، امر تبیین را برای افراد هزینه زا کرده است.

## ۶ نتیجه گیری

شناخت بنیان‌های فکری نظام سایبرنتیک اولین گام در ریل‌گذاری صحیح برای رسیدن به اهداف نظام‌ولایی است. اگرچه بنیان‌گذاران این نظام ریشه‌های الهیاتی این تفکر را کتمان می‌کنند؛ اما مبانی این نظام بر گرفته از نگاهی خداستیز به الهیات یهود است و ابزار پیاده‌سازی این تفکر، سلطه بر وجه مشترک سلطه‌پذیر انسانی، قوه‌خیال انسان‌هاست.

در مقابل، نظام‌ولایی با تأکید بر عقلانیت و تطهیر خیال، در پرتو تبیین و روشن‌گری حجت بیرونی (انبیاء) از قدرت و توانایی‌های خفته حجت درونی (عقل) در تقابل با تفکر سلطه بهره می‌گیرد. اینکه چه نوع تبیینی و چگونه و با چه روشی می‌تواند در بارورسازی عقلانیت جوامع و رسیدن به اهداف نظام ولایت مؤثر باشد، پژوهش‌های جدیدی را می‌طلبد.

## مراجع

- [۱] قرآن کریم.
- [۲] نهج البلاغه، سید رضی (ترجمه محمد دشتی)، چاپ اول، رواق روشن مهر، ۱۳۹۴.
- [۳] حسن زاده آملی، حسن. رسالة النور المتجلی فی الظهور الظلی، مکتب الاعلام الاسلامی مرکز النشر، ۱۴۱۷ هـ. ق.
- [۴] جوادی آملی، عبدالله. ریحیق مختوم: شرح حکمت متعالیه (تنظیم و تدوین حمید پارسا، تحقیق و پژوهش قاسم جعفری‌زاده، میثم واثقی، مهدی سلطانی)، ج ۲۰، چاپ اول، اسراء، قم، ۱۳۹۶.
- [۵] جوادی آملی، عبدالله. تحریر تمهید القواعد (ویرایش علی اسلامی، تهیه و تنظیم حمید پارسایان)، اسراء، قم، ۱۳۹۰.
- [۶] جوادی آملی، عبدالله. تسنیم (تفسیر ترتیبی قرآن کریم)، جلد ۸ (تنظیم و ویرایش علی اسلامی) اسراء، قم، ۱۳۷۸.
- [۷] رحیم‌پور ازغدی، حسن. چهار گفتار، طرح فردا، ۱۳۸۸.
- [۸] زمخشری، محمود. أساس البلاغه، دار صادر، چاپ اول، بیروت، بی تا، ۱۳۸۵ هـ. ق.
- [۹] صدرالدین شیرازی، محمدبن ابراهیم. مفاتیح الغیب (مقدمه و تصحیح از محمد خواجه‌جوی) چاپ اول، مؤسسه تحقیقات فرهنگی، تهران، ۱۳۶۳.
- [۱۰] طباطبائی، سید محمد حسین. ترجمه تفسیر المیزان (سید محمد باقر موسوی همدانی)، چاپ پنجم، دفتر انتشارات اسلامی، قم، ۱۳۷۴.
- [۱۱] کلینی، محمد بن یعقوب. اصول کافی (ترجمه سید مهدی آیه‌الهی) چاپ دوم، جهان‌آرا، تهران، ۱۳۸۷.
- [۱۲] مصباح یزدی، محمد تقی. چکیده‌ای از اندیشه‌های بنیادین اسلامی، چاپ هفتم، مؤسسه امام خمینی، قم، ۱۳۹۳.
- [۱۳] مطهری، مرتضی. علل گرایش به مادی‌گری، صدرا، تهران، ۱۳۹۲.



[۱۴] مؤدب، سید رضا و سالمی، حسین. چگونگی نفوذ شیطان در قوای ادراکی آدمی و اقسام کنش‌های آن از منظر قرآن با تأکید بر دیدگاه امام خمینی (ره)، دوفصلنامه علمی انسان‌پژوهی دینی، سال هفدهم، شماره ۴۳، ۱۳۹۹، صفحات ۲۰۵-۲۲۱.

[۱۵] یوسفی سوته، رقیه. بررسی تحلیلی نقش قوه خیال در تعالی انسان بر مبنای حکمت متعالیه، چاپ اول، دانشگاه باقرالعلوم، قم، ۱۳۹۸.

[۱۶] وینر، نوربرت. استفاده انسانی از انسان: سایبرنتیک و جامعه (ترجمه مهرداد ارجمند)، چاپ اول، سازمان انتشارات و آموزش انقلاب اسلامی، ۱۳۶۶.

[۱۷] معمارزاده، امیر. چگونه می‌توان از الهیات در جهان سایبری سخن گفت؟ سایبر پژوه، ۱۳۹۹.

<https://cyberpajoo.com/>

[۱۸] گراوندی، محسن. معرفی و مروری بر کتاب سایبرنتیک نوشته ریاضیدان نابغه قرن، وبلاگ تخصصی آمار، ۱۳۹۴.  
<http://statistics94.blogfa.com/post/277>

[۱۹] دریکوند، روح‌الله و جعفری، جواد. تمرکز و تکامل عقول در عصر ظهور. اندیشه نوین دینی، شماره ۴۲، پاییز ۱۳۹۴، صفحات ۴۹ تا ۶۶.

[20] WIENER, N. *GOD AND GOLEM, Inc. A Comment on Certain Points where Cybernetics Impinges on Religion*, Massachusetts, edited and corrected by überivison, December 2019.



## ارتقاء خبررسانی جمهوری اسلامی با استفاده از خبرگزاری جمع‌سپار مبتنی بر فناوری بلاک‌چین

سیدمحمدحسین موسوی<sup>۱</sup>، مرتضی انصاری<sup>۲</sup>

<sup>۱</sup> طلبه سطح سه موسسه تخصصی فقه امام کاظم علیه السلام، عضو جامعه نخبگانی حوزه علمیه  
sayed.m.h.mousavi@gmail.com

<sup>۲</sup> طلبه سطح دو موسسه تخصصی فقه امام کاظم علیه السلام، عضو جامعه نخبگانی حوزه علمیه  
s.mansari@chmail.ir

### چکیده

یکی از ارکان حکومت، مقبولیت در بین مردم جامعه و جهان است و یکی از اصلی‌ترین عوامل مقبولیت، رسانه و بالأخص خبررسانی است اما فضای خبررسانی علیه جمهوری اسلامی است؛ چرا که انبوه خبرگزاری‌های خارجی و کانال‌های خبری در شبکه‌های اجتماعی، اقدام به نشر شایعات کرده و اخبار صحیح و مثبت را سانسور یا تحریف می‌کنند. و از طرفی خبرگزاری‌های متعهد به جمهوری اسلامی به سه دلیل نمی‌توانند نظر مخاطبین داخلی و خارجی را جلب کنند: ۱. عدم اعتماد مخاطب به محتوای خبری، ۲. ضعف تکنیک‌های رسانه‌ای جلب مخاطب، ۳. فیلتر و مسدود شدن سایت‌ها و کانال‌های خبری. در این گزارش اثبات شده است که یک نرم‌افزار خبری مبتنی بر پروتکل بلاک‌چین می‌تواند با اعتبارسنجی غیرمتمرکز اخبار و حذف واسطه خبرگزاری، باعث از بین رفتن اخبار جعلی، تحریفات و سانسور اخبار شود. و از طرفی به خاطر شفافیت مراحل تولید خبر و پالایش جمع‌سپار اخبار، باعث افزایش اعتماد مخاطبین به محتوای تولید شده در آن می‌شود. همچنین فیلتر کردن و مسدودسازی پروتکل‌های مبتنی بر دفتر کل توزیع شده، بسیار دشوار و هزینه‌بر است. در نهایت این نرم‌افزار خبری به دلیل تقسیم درآمد تولید شده در سیستم بین کاربران به وسیله رمزارز، ایجاد استقلال صنعت خبر از تبلیغات، اعتباردهی حرفه‌ای به تولیدکنندگان محتوا و حفظ حق نشر خبرنگاران و تحلیلگران، باعث جذب خبرنگاران و خوانندگان داخلی و خارجی خواهد شد. سپس روش عملیاتی پیاده‌سازی و تولید پلتفرم خبرگزاری بر بستر بلاک‌چین به صورت مفصل توضیح داده شده و مزایا و فوائد به همراه چالش‌های استفاده از فناوری بلاک‌چین برای تولید یک خبرگزاری شرح داده می‌شود.

**کلمات کلیدی:** بلاک‌چین، خبر، خبررسانی، جمهوری اسلامی، جمع‌سپار، غیرمتمرکز، اخبار جعلی.

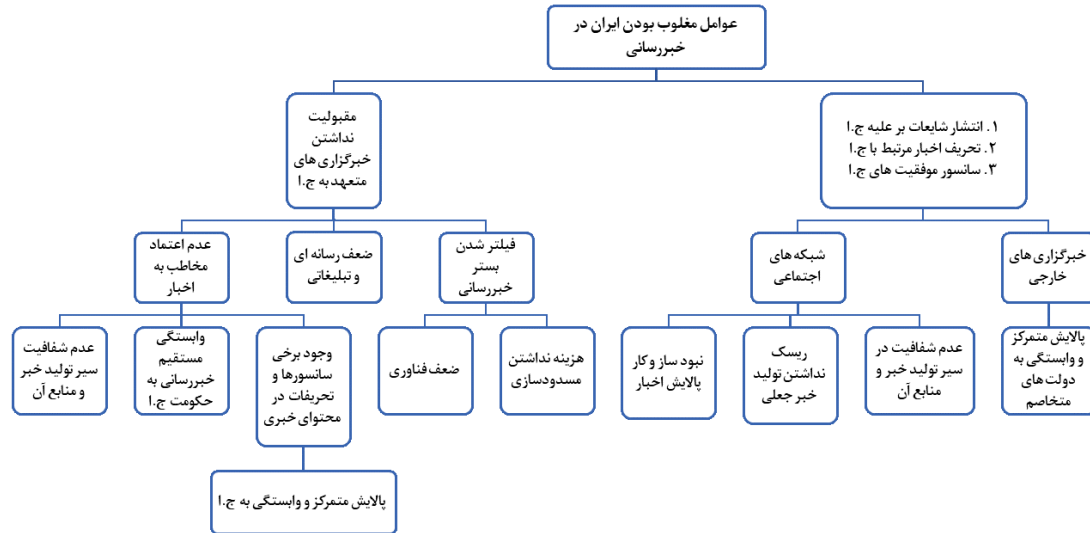
## ۱ مقدمه

نیکی از ارکان حکومت، مقبولیت در بین مردم جامعه و جهان است و یکی از اصلی ترین عوامل مقبولیت، رسانه و بلاخص خبررسانی است. اما جمهوری اسلامی به دو علت در فضای خبررسانی مغلوب است، نخست آنکه خبررسانی های جهانی به علت تفاوت ایدئولوژیک، اقدام به نشر شایعات، تحریف و سانسور اخبار علیه جمهوری اسلامی می کند، به طوری که بعضی از متخصصان مدعی شده اند ایرانیان ۱۸۰ برابر متوسط جهانی در معرض اخبار دروغ و ناامیدکننده توسط ۲۶۰ کانال تلویزیونی فارسی زبان و شبکه های اجتماعی هستند. دومین علت هم این است که خبرگزاری های متعهد به جمهوری اسلامی مورد توجه مخاطبین داخلی و خارجی نبوده و لذا جریان ساز نیستند.

منشأ اخبار جعلی بر علیه جمهوری اسلامی، خبرگزاری های خارجی و شبکه های اجتماعی است. در خبرگزاری ها، پالایش متمرکز اخبار و وابستگی به حکومت های متخاصم باعث انتشار شایعات و سانسور موفقیت های جمهوری اسلامی شده است. و در شبکه های اجتماعی سه عنصر نبود شفافیت در سیر تولید خبر، نبود ساز و کار پالایش اخبار و ریسک نداشتن تولید خبر جعلی منجر به گسترش شایعات شده است. همچنین مدیریت متمرکز در شبکه های اجتماعی سبب فیلتر شدن محتوای مخالف با سیاست های مدیران شبکه می باشد. مثل مسدود شدن اخبار و محتوای مربوط به حاج قاسم در پلتفرم اینستاگرام. از طرفی عدم شفافیت منابع و فرآیند تولید خبر، وابستگی مستقیم به جمهوری اسلامی و سانسور برخی از اخبار، منجر به بی اعتمادی مخاطبین به خبرگزاری های متعهد به جمهوری اسلامی شده و استفاده نکردن از تکنیک های جذب مخاطب هم باعث تشدید این عدم توجه شده است. در نهایت هم با اندک توجهی از طرف مخاطبین خبرگزاری ها یا کانال های خبری به خاطر ضعف فناوری مسدود و فیلتر می شوند. مثل مسدود شدن سایت العالم به همراه چند سایت خبری متعلق به ایران و محور مقاومت از سوی دولت آمریکا در تیرماه سال ۱۴۰۰. در نتیجه ۶ ریزمسئله وجود دارد که برای ارتقاء خبررسانی باید آن ها را حل کرد.

۱. پالایش متمرکز اخبار و وابستگی خبرگزاری ها به حکومت ها و سازمان ها، اعم از وابستگی رسانه های غربی به حکومت های متخاصم و وابستگی رسانه های ایرانی به حکومت جمهوری اسلامی.
۲. عدم شفافیت در سیر تولید خبر و منابع آن.
۳. امکان مسدودسازی محتوای خبری یا بسترهای انتشار خبر.
۴. ضعف رسانه ای و تبلیغاتی.
۵. نبود ساز و کار پالایش خبر در شبکه های اجتماعی.
۶. نبود ریسک برای تولید محتوای دروغ در شبکه های اجتماعی.

به نظر می رسد استفاده از دفتر کل توزیع شده بلاک چین بتواند مسائل یک تا چهار را به طور مستقیم حل کند و پلتفرم پیشنهاد شده در این گزارش، مسائل ۵ و ۶ را حل خواهد کرد.



شکل ۱: سلسله عوامل مغلوب بودن ایران در فضای خبررسانی

تکنولوژی بلاک چین در ابتدا به عنوان یک زیرساخت برای رمزنگاری ارزهای دیجیتال در نظر گرفته می شد، اما پس از مدتی، به طور گسترده به عنوان روشی برای تمرکززدایی از حوزه های مختلف صنعتی مورد استفاده قرار گرفت [۱۷]. دولت ها و سازمان های خصوصی بسیاری در حال تحقیق و سرمایه گذاری برای بهره برداری از فرصت های بالقوه بلاک چین می باشند. برای مثال سازمان مشارکت بلاک چین اروپا EBPC<sup>۱</sup> تا فوریه ۲۰۲۲، ۳۴۷ میلیون یورو برای تحقیقات و نوآوری های در زمینه بلاک چین هزینه کرده است<sup>۲</sup> و دولت چین میلیارد ها دلار در تحقیقات بلاک چین سرمایه گذاری کرده است و بیش از هر کشور دیگری ایده های مبتنی بر بلاک چین را ثبت اختراع کرده است<sup>۳</sup>.

استفاده از بلاک چین در صنعت خبررسانی ایده ای نوین است که تحقیقات کمی پیرامون آن صورت گرفته است. تا این تاریخ هیچ دولت و سازمان بزرگی این ایده را پیگیری نکرده است و هیچ مقاله فارسی در این رابطه وجود ندارد و تنها نوشته های محدودی به زبان انگلیسی در این رابطه یافت شد، که از تمامی آنها در این مقاله استفاده شده، ولی مقاله موجود ابعاد تازه تری را نسبت به نوشته های مشابه مورد بررسی قرار داده است.

به چند دلیل از بلاک چین به عنوان راه حل مشکلات خبررسانی، یاد شده است:

۱. **روند تکامل خبررسانی ها:** روند تکامل خبررسانی از روش سینه به سینه تا اینترنت، مبتنی بر افزایش چهار مؤلفه واقع نمایی، گستره ی قابل پوشش مخاطبین، سرعت انتشار و سادگی در استفاده بوده است. این چهار عنصر در خبرگزاری مبتنی بر بلاک چین هم وجود دارد.

<sup>1</sup> European Blockchain Partnership

<sup>2</sup> <https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership>

<sup>3</sup> <https://govchain.world/china>

۲. کلان-روندهای جهانی: ابزارها و ایده‌هایی تثبیت می‌شوند که منطبق با کلان-روندهای جهانی باشند. ایده خبرگزاری بر بستر بلاک‌چین منطبق با چهار کلان روند است: ۱. دیجیتالی شدن همه چیز، ۲. دموکراسی الکترونیک، ۳. توزیع قدرت میان غرب، شرق و تمدن اسلامی و ۴. عدم اطمینان فزاینده به ساختارهای موجود.

### ۳. نشانک‌های ضعیف:

(آ) اقبال زیاد به فناوری غیرمتمرکز بلاک‌چین: موفقیت بیت‌کوین به عنوان یک رمزارز مبتنی بر پروتکل بلاک‌چین باعث توجه روزافزون نخبگان به این فناوری غیرمتمرکز شد. پژوهشگاه‌های فراوانی در سرتاسر جهان مشغول به مطالعه در رابطه با کارکردها و فرصت‌های مختلف این پروتکل می‌باشند. برای مثال بانک مرکزی چین، کارگروه بررسی زنجیره بلوکی دولت روسیه، مجلس ملی فرانسه و پارلمان اتحادیه اروپا مطالعه و بهره‌مندی از مزایای این فناوری را در دستور کار خود قرار داده‌اند.<sup>۴</sup>

(ب) گسترش رمزارزها و نیاز به بسترهای جدید برای شتاب‌دهی به آنها: رمزارز یکی از گونه‌های دارایی دیجیتالی است که از فناوری بلاک‌چین در طراحی آن استفاده شده و معمولاً به صورت غیرمتمرکز اداره می‌شود. زمانی ارزش یک رمزارز بالا می‌رود که اقبال عمومی به شبکه‌ای که آن رمزارز روی آن شکل گرفته بیشتر شود. یکی از روش‌های افزایش اقبال عمومی ایجاد خدماتی مبتنی بر شبکه رمزارز است. مثل ایجاد شبکه اجتماعی تلگرام بر روی پلتفرم TON<sup>۵</sup> یا کاربایی غیرمتمرکز Ethlance<sup>۶</sup> مبتنی بر پروتکل اتریوم. به نظر می‌رسد یکی از بسترهای مورد استفاده برای جلب اقبال عمومی، خدمات اطلاع‌رسانی خواهد بود.

ساختار این مقاله به شرح زیر است:

- بخش ۲ مفهوم بلاک‌چین را توضیح می‌دهد.
- بخش ۳ اثبات می‌کند که نرم‌افزار خبری مبتنی بر بلاک‌چین می‌تواند مشکلات خبررسانی را حل کند.
- بخش ۴ روش پیاده‌سازی یک خبرگزاری بر بستر بلاک‌چین را توضیح می‌دهد.
- بخش ۵ و ۶ مزایا و چالش‌های خبررسانی مبتنی بر بلاک‌چین را تبیین می‌کند.

<sup>۴</sup> فعالیت کشورهای مختلف به طور مفصل در بخش ۶ توضیح داده شده است.

<sup>۵</sup> Durov, Nikolai. (2017) "Telegram Open Network," [?] p. 14

<sup>۶</sup> <https://ethlance.com/#/how-it-works>



## ۲ مفهوم‌شناسی بلاک چین

بلاک چین (یا زنجیره بلوکی)، پروتکل ثبت شفاف داده با نفی واسطه و تأمین امنیت است [۴].<sup>۷</sup>

### ۱.۲ پروتکل

پروتکل‌ها یا قراردادهای شبکه‌های رایانه‌ای، به مجموعه قوانینی گفته می‌شود که چگونگی ارتباطات بین سیستم‌های رایانه‌ای مختلف را قانون‌مند می‌کند. نقش پروتکل در کامپیوتر مانند نقش زبان برای انسان است. برای ارتباط موفقیت‌آمیز دو دستگاه در شبکه، باید هر دو دستگاه از یک پروتکل یکسان استفاده کنند.

### ۲.۲ ثبت شفاف داده

بلاک چین در دو ناحیه «کد منبع»<sup>۸</sup> و «محتوای اطلاعات» شفافیت دارد. شفافیت آن در کد منبع به این صورت است که می‌توان به منبع و سورس آن الگوریتم‌ها دسترسی داشت. البته توجه شود که این به معنای لزوم متن‌باز<sup>۹</sup> بودن بلاک‌چین نیست [۲۴].<sup>۱۰</sup> گرچه بسیاری از نرم‌افزارهای مبتنی بر پروتکل بلاک‌چین، مانند بیت‌کوین متن‌باز هم هستند.

اما نسبت به محتوای اطلاعات، قابلیت درجات مختلفی از شفافیت وجود دارد. در بالاترین درجه ممکن است اطلاعات داخل بلوک‌های یک نرم‌افزار مبتنی بر بلاک‌چین به صورت کامل برای همه کاربران شفاف باشد و در درجات دیگر ممکن است که تنها فرستنده و گیرنده توان مشاهده محتوای بلوک‌ها را داشته باشند؛ اما در پایین‌ترین درجه هم مشخص است که کسی مطالبی را در زمان معین ثبت کرده است [۵].

### ۳.۲ نفی واسطه

پروتکل‌های رایج در بستر اینترنت<sup>۱۱</sup>، قواعد انتقال و ثبت داده‌ها را بر پایه سرور-کاربر تعیین می‌کنند، یعنی تولید داده همگانی است اما بستر انتقال و ثبت آن داده همگانی نیست، بلکه واسطه خاص (سرور) این وظیفه را به عهده گرفته است.

اما در پروتکل بلاک‌چین ثبت داده‌ها به صورت هم‌تا به هم<sup>۱۲</sup> است؛ یعنی همان رایانه‌هایی که تولید محتوا می‌کنند، می‌توانند به ضبط و انتقال داده‌ها نیز پردازند. به زبان فنی، رایانه‌های کارده و کارخواه هر دو در یک سطح کار می‌کنند، و هر رایانه می‌تواند از اطلاعات رایانه دیگر استفاده کرده یا به رایانه‌های

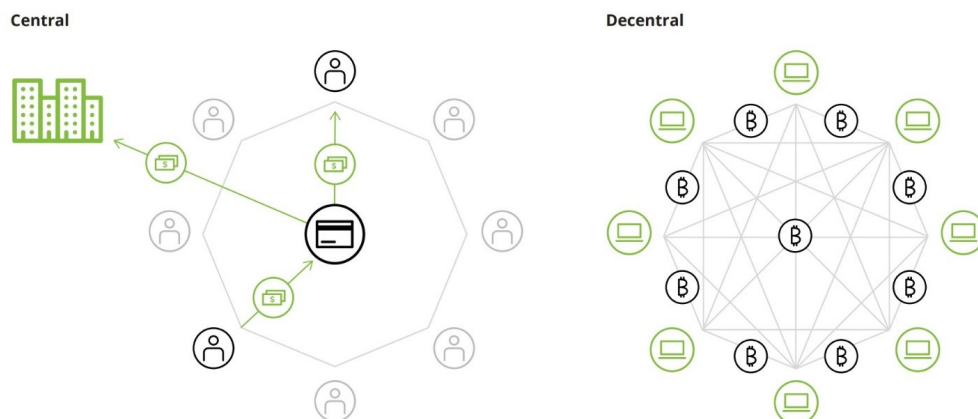
<sup>۷</sup> در واقع این گزاره، تعریف «دفتر کل توزیع‌شده» می‌باشد و بلاک‌چین یکی از مصادیق دفترکل توزیع‌شده است. اما چون این عنوان اولین فرد دفتر کل توزیع‌شده بوده برای آن علم بالغیه شده است (رجبی، ابولقاسم، ۱۳۹۷) [۵].

<sup>۸</sup> کد منبع (source code): هر برنامه رایانه‌ای به یکی از زبان‌های برنامه‌نویسی نوشته شده است (مانند پایتون، جاوا، سی++ و...) که متن این برنامه‌ها ممکن است چند خط یا میلیون‌ها خط داشته باشند. به متن این برنامه‌ها کد منبع می‌گویند. کد منبع شامل مواردی همچون تعریف متغیرها، دستورها، توابع، حلقه‌ها، و دیگر عباراتی می‌شود که به برنامه می‌گوید چگونه باید عمل کند.<sup>۹</sup> متن‌باز یا open source یک کد منبع است که برای اصلاح و توزیع مجدد احتمالی آزادانه در دسترس قرار می‌گیرد.

<sup>۱۰</sup> اگرچه بلاک‌چین به لحاظ فنی ممکن است منبع‌باز نباشد، اما سیستم‌های بلاک‌چین معمولاً با نرم‌افزار منبع‌باز و با استفاده از مفهومی که فرهنگ باز را در بر می‌گیرد، پیاده‌سازی می‌شوند.

<sup>۱۱</sup> مانند پروتکل TCP/IP پروتکل کنترل انتقال یا پروتکل HTTP پروتکل انتقال صفحات وب در شبکه

<sup>۱۲</sup> peer-to-peer



شکل ۲: مقایسه شبکه غیرمتمرکز (سمت راست) و شبکه متمرکز (سمت چپ)

دیگر اطلاعات بفرستد. با این فناوری، نیاز سیستم به واسطه برای ثبت اطلاعات رفع می‌شود [۱۴]. در واقع بلاک چین یک دفتر ثبت اطلاعات توزیع شده<sup>۱۳</sup> است.

## ۴.۲ تأمین امنیت

جعل و تخریب اطلاعات در بلاک چین عملاً امکان ندارد و بعد از ثبت اطلاعات در بلوک‌ها، دیگر نمی‌توان آن‌ها را تغییر داد؛ چرا که اولاً هر بلوک دارای نوعی رمز منحصر به فرد به نام «هش»<sup>۱۴</sup> است و ثانیاً همه اعضای شبکه به داده‌های ذخیره شده دسترسی و نظارت دارند [۴].

بلاک چین یک ردیف اطلاعات در حال رشد است. هر رکورد<sup>۱۵</sup> - که در بلاک چین به آن بلوک می‌گویند - با اتصال به بلوک‌های قبلی، یک زنجیره را تشکیل می‌دهند. هر بلوک دارای نشانگر مخصوص خود به نام هش و همچنین یک هش رمزنگاری از بلوک‌های قبلی است. در اصل، هر بلوک به بلوک قبلی متصل شده و زنجیره‌های بلندی ایجاد می‌کند که شکستن آنها غیرممکن است و هر کدام حاوی اطلاعاتی در مورد بلوک‌های دیگر است که برای تأیید تراکنش‌ها استفاده می‌شود [۲۴].

هیچ مرکزی در بلاک چین وجود ندارد. بلوک‌ها در سراسر اینترنت توزیع می‌شوند و یک مسیر حسابرسی قوی ایجاد می‌کنند که قابل ردیابی است. هرکسی که به زنجیره دسترسی داشته باشد می‌تواند یک تراکنش را تأیید کند اما نمی‌تواند سوابق را تغییر دهد [۱].

روش اجرایی بلاک چین به این صورت است که در گام نخست، یک کاربر تراکنشی را در شبکه درخواست

<sup>13</sup>distributed

<sup>14</sup>hash

<sup>15</sup>در علم کامپیوتر، یک رکورد (همچنین به آن ساختار یا داده مرکب گفته می‌شود) مجموعه‌ای از داده‌های ساختار یافته است. رکوردهای موجود در یک پایگاه داده یا صفحه گسترده معمولاً «ردیف» نامیده می‌شوند. یک رکورد مجموعه‌ای از اطلاعات (Field) است که این اطلاعات می‌توانند از انواع مختلف داده‌ها باشند و معمولاً با تعداد و ترتیب ثابت هستند

می‌کند. با ثبت درخواست، اطلاعات آن بین تمام نود<sup>۱۶</sup> های فعال در شبکه پخش می‌شود. در این مرحله، برای نهایی شدن تراکنش و ارجاع‌پذیری آن، باید اطلاعات تراکنش به صورت یک بلوک در زنجیره اصلی اضافه شود و اعضا آن را شناسایی کنند.

اگر هر یک از اعضا، بلوک‌های مد نظر خود را برای درج شدن در زنجیره اصلی به شبکه ارسال کنند، احتمالاً بلوک‌های تکراری و متناقضی تشکیل می‌شود. برای جلوگیری از این مسئله، تنها می‌بایست یک بلوک به زنجیره اضافه شود. پس اعضا باید درباره اینکه بلوک کدام یک از ایشان به زنجیره اضافه شود به توافق برسند. به راه‌کار رسیدن به این توافق، الگوریتم اجماع<sup>۱۷</sup> می‌گویند [۴].

برای مثال در شبکه بیت‌کوین، تنها بلاک کسی به زنجیره اصلی متصل می‌گردد که اثبات کند از سایر اعضا شبکه تلاش بیشتری داشته است<sup>۱۸</sup>. این اثبات تلاش احتمال ثبت اطلاعات نادرست از طرف کاربران را از بین می‌برد؛ چون اولاً نوعی حالت رندم و اتفاقی در الگوریتم آن وجود دارد و ثانیاً در آخرین مرحله برای اتصال بلاک به زنجیره اصلی، می‌بایست این بلاک به تأیید پنجاه درصد به علاوه یک نود برسد. پس کاربر در نود خویش اطلاعات نادرست را ذخیره نمی‌کند تا توسط سایر اعضا - که باید آن بلاک را تأیید کنند - رد نشود.

در نهایت شبکه برای کاربری که بلاک او تأیید شده و به زنجیره نهایی متصل گردیده، حق الزحمه‌ای تعریف کرده است<sup>۱۹</sup> [۴].

### ۳ اثبات فرضیه

آیا خبرگزاری مبتنی بر بلاک‌چین می‌تواند شش مشکل اصلی در جریان خبررسانی را حل کند؟ مشکل اول، وابستگی خبرگزاری‌ها و شبکه‌های اجتماعی به سازمان‌ها و کشورها و متمرکز بودن پالایش اخبار در این سازمان‌ها می‌باشد؛ پس باید اثبات کرد که بلاک‌چین می‌تواند وابستگی به یک نهاد متمرکز نداشته باشد. مشکل دوم، عدم شفافیت منابع و فرآیند تولید خبر است، پس باید اثبات شود که بلاک‌چین و محتوای آن شفاف است. مشکل سوم، امکان فیلتر کردن بسترهای خبرگزاری است، پس باید اثبات شود که بلاک‌چین ضد فیلتر است یا فیلتر را هزینه‌بر می‌کند. مشکل چهارم، نبود سیستم پالایش خبر در شبکه‌های اجتماعی است. پس باید اثبات کرد که این خبرگزاری می‌تواند اخبار را بدون نیاز به یک نهاد متمرکز پالایش کند. مشکل دیگر، ریسک برای تولید و انتشار محتوای دروغ است، پس باید سیستمی طراحی شود که تولید شایعات را هزینه‌بر کند و در نهایت اثبات شود که بلاک‌چین آن قدر جذاب است که خلاءهای رسانه‌ای و تبلیغاتی برای

<sup>۱۶</sup> نود (Node) در شبکه‌ی بلاک‌چین به هر دستگاه الکترونیکی می‌گویند که بتواند نسخه‌ای از بلاک‌چین را ذخیره کند و به عملکرد شبکه کمک کند. هر کاربر روی شبکه با نام نود، شناخته شده و شماره شناسایی مخصوص به خود را دارد؛ و تمام کاربران نسخه‌ی به‌روزی از دفتر کل را در اختیار دارند.

<sup>۱۷</sup> consensus algorithm

<sup>۱۸</sup> به این الگوریتم اجماع در بیت‌کوین، اثبات کار یا Proof of Work می‌گویند. الگوریتم‌های دیگری هم برای اجماع تعریف شده‌اند؛ مثل الگوریتم اثبات سهام (PoS).

<sup>۱۹</sup> در پروتکل‌های مبتنی بر الگوریتم اجماع «اثبات کار» به خاطر سختی حل مسئله و کسب جایزه، این کار را به استخراج از معدن تشبیه کرده و به آن mining می‌گویند.

جذب مخاطبین به خبرگزاری را برطرف کند.

### ۱.۳ نبود پالایش متمرکز و وابستگی

خاصیت غیرمتمرکز بودن بلاک چین می تواند باعث عدم وابستگی آن به نهادها و حکومت های مختلف شود. این عدم وابستگی می تواند مشکل دخالت ذی نفعان در اخبار و در نتیجه پالایش متمرکز و تولید اخبار جعلی و سانسور توسط خبرگزاری های خارجی را حل کند و از طرفی هم منجر به افزایش اعتماد مخاطبین نسبت به خبرگزاری های متعهد به جمهوری اسلامی شود [۲۵]. نمونه این تمرکززدائی و به تبع عدم وابستگی را می توان در رمزارز بیت کوین مشاهده کرد.

البته ممکن است گفته شود که می توان سازمانی طراحی نمود که بدون پشتوانه دولت ها و سازمان های ذی نفع، امر خبررسانی را به عهده بگیرد و بتواند این مشکل را حل کند، اما این سازمان به دلیل اینکه خود احتمال ذی نفع شدن را دارد، مورد تأیید نخواهد بود، بنابراین باید سازوکاری ارائه داد که از ریشه احتمال دخالت ذی نفعان در آن داده نشود.

### ۲.۳ شفافیت

کاربران در سیستم بلاک چین به تمامی داده ها دسترسی دارند. این قابلیت، منجر به شفافیت سیر تولید خبر و ردیابی منابع آن می شود. شفافیت در سیر تولید خبر باعث افت اعتبار اخبار جعلی و جلوگیری از انتشار آنها خواهد شد. بنابراین مشکلی که در شبکه های اجتماعی وجود دارد را می توان حل کرد.

همچنین بیان شد که یکی از عوامل عدم اعتماد مخاطبین به خبرگزاری های متعهد به جمهوری اسلامی شفاف نبودن سیر تولید خبر است. با شفافیت در دو ناحیه کد منبع و سیر تولید خبر در بلاک چین این مشکل حل خواهد شد. برای مثال شفاف بودن کد منبع در رمزارزها، نرم افزارهای مبتنی بر دفتر کل توزیع شده و سیستم عامل لینوکس موجب محبوبیت آنها شده است.

قابلیت شفافیت در بلاک چین های عمومی زمینه ساز تولید یک پلتفرم خبری شفاف است. ساز و کار شفافیت در سیر تولید خبر و تأثیر آن در اعتبارسنجی اخبار به طور مفصل در بخش سوم (روش اجرایی) توضیح داده شده است.

### ۳.۳ ضد فیلتر و هک

سه راه اصلی برای مسدود کردن یک محتوا در اینترنت وجود دارد. نخست، دسترسی به سرور و تغییر محتوا؛ دوم، فیلتر کردن آی پی کاربر و اجازه ندادن به او برای ارتباط با آن محتوای خاص؛ و سوم، مسدود کردن پروتکلی که محتوا در بستر آن در شبکه ثبت و منتقل می شود.

در راه اول، سانسورکننده یا به صورت کامل اطلاعات یک سرور را از بین می برد و یا اینکه بعضی از محتواهای آن سرور را سانسور می کند. این حالت زمانی رخ می دهد که سرور تحت نفوذ آن فرد باشد<sup>۲۰</sup>.

<sup>۲۰</sup> در سال ۲۰۱۸ دولت چین نامه فعالان دانشجویی جنبش #MeToo که از اینترنت منتشر شده بود را در شبکه های رسانه ای چینی سانسور کرد. این نامه توسط دانشجویی از دانشگاه پکن به نام «یو شین» تألیف شده بود و محتوی افشاگری نسبت به

با توجه به ویژگی جمع‌سپاری بودن و پروتکل‌های هش‌نویسی، مشکل اول در بلاک‌چین تصور نمی‌شود. چرا که اولاً هر نوع تغییری در اطلاعات باعث تغییر هش و لو رفتن هک خواهد شد و ثانیاً در بلاک‌چین اصلاً سرور مرکزی وجود ندارد، بلکه تمامی کاربران نقش سرور دارند و اطلاعات بین تمام ایشان پخش شده است؛ و با تغییر اطلاعات یک سرور، تغییری در بلوک‌های اصلی زنجیره پدید نمی‌آید [۲۳].

برای مثال، فرض کنید سند یک معامله میان صد نفر توزیع شده است. حال، اگر یک شخص تغییری در مفاد سندی که پیش اوست ایجاد کند، آیا با این تغییر سایر نسخ هم تغییر پیدا می‌کنند؟ خیر. این شخص برای تغییر می‌بایست تمامی صد نسخه موجود بین اعضاء را تغییر دهد که این کار عملاً ممکن نیست. حال، فرض کنید اعضاء یک میلیون یا بیشتر باشد، آیا تحریف در مفاد اطلاعات ممکن است؟ خیر.

در راه دوم، برخلاف روش قبل، اطلاعات سانسور نمی‌شود، بلکه دسترسی کاربر و آی پی به اطلاعات محدود و فیلتر می‌شود. این محدود کردن یا نسبت به یک سری از کاربران خاص (مانند کاربران یک کشور) می‌باشد، مثل فیلترینگ در ایران. یا نسبت به تمام کاربران اینترنت می‌باشد، مثل مسدود کردن سایت شبکه خبری العالم توسط ایالات متحده<sup>۲۱</sup>.

در روش معمول فیلترینگ، که روش فیلترکردن آی پی است باید گفت که امکان محدود کردن دسترسی برخی کاربران به پروتکل بلاک‌چین وجود دارد که برای حل این مشکل، پروکسی غیرمتمرکز بر پایه‌ی بلاک‌چین تعبیه شده است که روش کار آن شبیه پروکسی‌هایی است که برای تغییر آی پی و دور زدن فیلترینگ موجود استفاده می‌شود [۳۱].

در راه سوم هنوز هم می‌توانند به صورت جهانی، دسترسی کاربران شبکه به آن پروتکل خاص بلاک‌چین را محدود کنند. مثلاً طوری برنامه‌ریزی کنند که هیچ کد مبتنی بر پروتکل بیت‌کوین توانایی ثبت و انتقال در شبکه اینترنت را نداشته باشد.

در پاسخ به این مشکل باید گفت که اگر بتوان خبرگزاری را بر پایه دفتر کل یک اکوسیستم دارای رمزارز مشهور مثل اتریوم پیاده کرد، فیلترکردن آن اگرچه ممکن است ولی بسیار هزینه‌بر بوده و عملاً قابل اجرا نیست؛ یا در صورت عدم استفاده از اکوسیستم‌های مشهور، قبل از بهره‌برداری از پلتفرم، رمزارز آن را پیش‌فروش کرده<sup>۲۲</sup> و به عبارتی کاری کنیم که هزینه سانسور کردن آن بالا برود. مانند کاری که تلگرام در پروژه بلاک‌چین تلگرام (TON) آن را پیگیری می‌کند [۱۵]. در واقع، اصلی‌ترین نقش پروتکل‌های غیرمتمرکز، همین هزینه‌دار کردن مسدودسازی است.

### ۴.۳ مزایای این خبرگزاری برای جذب مخاطبین

مزایای این خبرگزاری نسبت به خبرگزاری‌های مرسوم برای جذب مخاطب عبارت است از: تقسیم درآمد سیستم میان کاربران، اعتباردهی به تولیدکنندگان، حفظ حق نشر تولیدکنندگان محتوا و استقلال آنها از

ماجرای تجاوز جنسی در سال ۱۹۹۸ بوده است. پس از این سانسور «یوشین» این نامه را در شبکه بلاک‌چین اتریوم بارگذاری نمود و با این کار مانع از سانسور آن توسط دولت مرکزی شد [۲۰]  
<sup>۲۱</sup> سه‌شنبه مورخ اول تیرماه ۱۴۰۰ شمسی سایت العالم به همراه چند سایت خبری متعلق به ایران و محور مقاومت از سوی دولت آمریکا تویبخ و مسدود اعلام شد (خبرگزاری تسنیم)  
<sup>۲۲</sup> به رمزارز پیش‌فروش شده ICO گفته می‌شود.

خبرگزاری‌ها و استقلال صنعت خبری از تبلیغات. این عناوین به‌طور مفصل در بخش ۴ مقاله توضیح داده خواهد شد.

### ۵.۳ ایجاد ساز و کار پالایش خبر

مخاطبین اخبار در سرتاسر جهان، به خاطر وجود شایعات و اخبار جعلی خبرگزاری‌های وابسته، به اخبار موجود در شبکه‌های اجتماعی روی آورده‌اند؛ ولی این شبکه‌ها به دلیل فقدان سیستم پالایش اخبار، باز هم محل انتشار شایعات می‌باشند. به همین دلیل، می‌بایست سیستمی برای پالایش اخبار به‌صورت غیرمتمرکز طراحی کرد.

پلتفرم فعال‌شده توسط بلاک‌چین می‌تواند روشی مطمئن برای تأیید محتوا و منابع آن به خوانندگان ارائه دهد [۲۲] و [۲۸]. بحث فنی چگونگی جلوگیری از اخبار جعلی توسط سیستم غیرمتمرکز در بخش پنجم توضیح داده خواهد شد و اثبات می‌شود که نرم‌افزار مبتنی بر بلاک‌چین می‌تواند اخبار را کسب، پالایش و منتشر کند.

### ۶.۳ ایجاد ریسک برای تولید محتوای دروغ

در بخش سوم (روش اجرائی) توضیح داده خواهد شد که با دو عامل «اعتبار اجتماعی» و «ودیع» برای تولید محتوا، می‌توان تولید اخبار جعلی را دارای ریسک کرد و احتمال تولید این اخبار را پایین آورد.

## ۴ روش اجرائی پلتفرم خبرگزاری مبتنی بر بلاک چین

بعد از این که ضرورت ایجاد یک خبررسانی غیرمتمرکز اثبات شد، این مسئله پیش می‌آید که چگونه می‌توان بدون وجود یک مدیریت متمرکز، سه مرحله کسب، پالایش و انتشار اخبار را انجام داد؟ چه کسانی در این سیستم متولی کسب خبر هستند و اخبار را در کجا قرار می‌دهند؟ چه کسانی اخبار صحیح را از شایعات تمییز می‌دهند و این اخبار چگونه منتشر شده و در دسترس عموم قرار می‌گیرند. در این بخش اثبات خواهد شد که یک سیستم غیرمتمرکز می‌تواند با توزیع اختیارات بین کاربران و جمع‌سپاری، این مراحل را مدیریت کند.

### ۱.۴ تعریف بازیگران

۱. خبرنگار: کاربری که متولی تولید خبر هستند.
۲. ارزیاب: کاربر ویژه با اعتبار و سابقه بالا، که می‌تواند خبر خبرنگار را مورد بررسی، نقد و تحلیل قرار دهد. نظر این تحلیل‌گران بر رأی تاییدگرها تاثیر خواهد داشت.
۳. تاییدگر/ رأی‌دهنده: کسانی که به واقعی بودن یا جعلی بودن اخبار و ارزیابی‌ها رأی می‌دهند.



۴. مصرف کننده: عموم کاربران که صرفاً اخبار را مشاهده می‌کنند و هیچ نقشی در فرآیند تولید و پالایش اخبار ندارند.

## ۲.۴ فرآیند اجرائی

**مرحله اول:** خبرنگار یک محتوای خبری جدید ایجاد می‌کند. او برای انتشار باید مقداری توکن پرداخت کند [۸]. این ودیعه در صورت تأیید صحت محتوا به همراه مقداری پاداش بازگردانده خواهد شد.

**مرحله دوم:** بعد از انتشار اولیه، خبر در وضعیت «تحلیل و ارزیابی» قرار می‌گیرد [۱۲] و تمامی کاربران می‌توانند این خبر را در صفحه مخصوص اخبار تأیید نشده مشاهده کنند. در این مرحله کاربرانی که مقدار مشخصی اعتبار و سابقه در سیستم دارند، مهلت دارند تا خبر را ارزیابی کنند. ارزیابی خبر به این است که اگر موافق با تمام محتوای خبری هستند، آن را تأیید کرده و مستندسازی کنند. اگر با تمامی خبر مخالفت دارند مدارک خلاف واقع بودن آن را بگذارند؛ و اگر بخشی از آن را صحیح و بخشی را نادرست می‌دانند، بخش اشتباه را مشخص کرده و برای هر بخش مستندات ذکر کنند.

**مرحله سوم:** پس از پایان زمان وضعیت ارزیابی، خبر وارد وضعیت «صحت‌سنجی» می‌شود. در ابتدا، اعتبار این خبر صفر است. سپس تمامی کاربران به‌جز خبرنگار صاحب خبر و ارزیاب‌هایی که آن خبر را تحلیل کرده‌اند، می‌توانند نسبت به صحیح بودن یا نادرست بودن خبر و ارزیابی‌های ذیل آن رأی بدهند [۸]. رأی‌دهی به‌صورت صفر و یکی است. یعنی فرد یا خبر را قبول دارد یا قبول ندارد. اگر بخشی از آن را قبول داشته باشد و بخش دیگر را قبول نداشته باشند، باید به تحلیل مطابق با نظرش رأی مثبت بدهد<sup>۲۳</sup>.

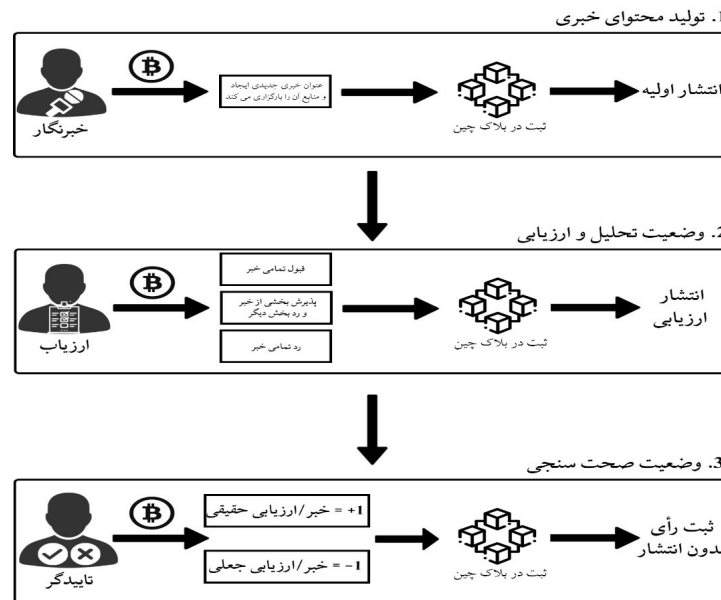
اعتبار خبر و ارزیابی‌ها به‌وسیله عددی بین منفی صد تا مثبت صد نمایش داده می‌شود. مثبت صد یعنی خبر صد در صد صحیح است، صفر یعنی خبر مشکوک است و منفی صد یعنی خبر صد در صد غلط است. نحوه محاسبه این عدد عبارت است از تعداد رأی‌های مثبت منهای رأی‌های منفی تقسیم بر تعداد کل آراء ضرب در صد.

نتیجه رأی‌گیری تنها پس از پایان وضعیت صحت‌سنجی نمایش داده خواهد شد تا تأثیری بر رأی سایر کاربران نداشته باشد [۸].

**مرحله چهارم:** پس از پایان وضعیت صحت‌سنجی عمومی، خبر و ارزیابی‌های ذیل آن وارد وضعیت «قضاوت‌شده» قرار می‌گیرند. در این وضعیت، تعداد مشاهده‌های کاربران اعم از آنهایی که رأی داده‌اند و آنهایی که رأی نداده‌اند، به‌همراه تعداد شرکت‌کنندگان در رأی‌گیری و خروجی رأی‌گیری به نمایش در خواهد آمد.

در این مرحله به خبرنگار و تحلیل‌گرانی که محتوای ایشان تأیید شده باشد، پاداش مالی داده شده و به اعتبار آنها افزوده می‌شود و در صورت رد محتوا علاوه بر از دست دادن مقدار ودیعه، اعتبار آن‌ها نیز کاسته خواهد شد [۸].

<sup>۲۳</sup> در صورتی که نمره یک ارزیابی از خود خبر اصلی بیشتر شود، جای آن خبر را خواهد گرفت.



شکل ۳: مراحل تولید و پالایش خبر

## ۳.۴ نکات روش اجرایی

۱. می توان گزینه دیگری را به پلتفرم اضافه کرد و آن هم درخواست اعتبارسنجی خبر است. مثلاً یک کاربر خبری را در شبکه اجتماعی می بینند و می خواهند بدانند که آیا این خبر صحت دارد یا جعلی است و آن عنوان خبری را در پلتفرم پیدا نمی کند. به همین جهت، آن عنوان خبری را به صورت سؤالی ایجاد می کند تا ارزیابها ذیل آن عنوان تحلیل بگذارند و تأییدگرها به بهترین تحلیل رأی بدهند [۲۱]. در این بخش اگر آن عنوان خبری شایعه باشد، اعتباری از درخواست کننده کم نمی شود. در نهایت هم حق اولویت عنوان و پاداش به معتبرترین تحلیل خواهد رسید.

۲. اجماع در بلاک چین ربطی به رأی گیری برای تأیید خبر در روش اجرایی ندارد. کار ماینرها با تأییدکنندگان فرق دارد. ماینرها متولی ثبت خبر هستند در حالی که کار تأییدکنندگان این است که معین کنند از اخبار ثبت شده، کدام یک مطابق واقع است و کدام یک شایعه می باشد. در واقع، برای خبررسانی غیرمتمرکز دو چالش وجود دارد: نخست، تأمین امنیت در ثبت داده و دوم، راهی برای پالایش اخبار صحیح از ناصحیح به صورت غیرمتمرکز<sup>۲۴</sup>.

<sup>۲۴</sup> شاید سؤال شود که این الگوریتم و روش اجرایی نیاز به بلاک چین ندارد و می توان آن را روی یک سرور متمرکز هم پیاده سازی کرد. جواب این است که نیاز به بلاک چین و سامانه غیرمتمرکز برای خبررسانی، به دلایل دیگری مثل افزایش مقبولیت، اعتمادسازی و جلوگیری از فیلتر و سانسور اثبات شد. بعد از اثبات نیاز به سیستم غیرمتمرکز این مسئله مطرح شد که این سیستم چگونه می تواند

۳. قرار نیست این روش یک خبر را به صورت صد در صدی رد یا تأیید کند. بلکه صرفاً با کنار هم گذاشتن قرائن صدق و کذب، به مخاطب قدرت تحلیل و تفکیک بین خبر واقعی و جعلی می‌دهد.<sup>۲۵</sup>

مثلاً در صورتی که یک خبر مشاهده زیادی داشته باشد، یعنی آن خبر از امور مهم محسوب می‌شود و احتمال کذب در آن زیاد است. اگر تعداد مشارکت در رأی‌گیری زیاد باشد، احتمال تبانی بر کذب در رأی‌دهی پایین می‌آید. اگر نمره و اعتبار یک خبر بالا باشد، می‌توان نسبت به صحت آن اطمینان پیدا کرد. اگر صاحب خبر یا تحلیل، سابقه‌ی خوب و اعتبار بالا داشته باشد، اعتماد به اخبارش افزایش پیدا می‌کند و همچنین اگر ذیل یک خبر تحلیل‌های مثبت وجود داشته باشد، بیشتر می‌توان به آن خبر اطمینان کرد.

۴. سیستم از ۳ روش برای جلوگیری حداکثری از نشر شایعات و تبانی بر کذب استفاده می‌کند:

**الف) اعتبارسنجی عمومی مبتنی بر رأی‌گیری:** اگر تعداد مشارکت در رأی‌گیری بالا باشد احتمال همدستی در تأیید شایعات کاهش می‌یابد. بنابراین، اطمینان به محتوای خبری افزایش پیدا می‌کند؛ و اگر تعداد افراد شرکت‌کننده در رأی‌گیری پایین باشد نشان‌دهنده عدم اهمیت خبر بوده و کم‌اهمیت بودن خبر، خود باعث کاهش احتمال تبانی در کذب است.

**ب) ایجاد ریسک مالی و اعتباری:** در سیستم دو مفهوم «اعتبار اجتماعی» و «کیف پول» مبتنی بر رمزارز تعریف شده است؛ و هر کنش مثبتی در سیستم اعم از تولید خبر، ارزیابی و رأی صحیح، دارای سود مالی و افزایش اعتبار است و از طرفی هر کنش منفی دارای مجازات مالی و اعتباری می‌باشد. اگر اعتبار کاربر از صفر پایین‌تر باشد، نمی‌تواند عنوان خبری ایجاد کند یا در رأی‌گیری شرکت کند و اگر اعتبار آن از یک حد مثلاً ۱۰۰۰ پایین‌تر باشد نمی‌تواند اخبار را ارزیابی کند.

**ج) ایجاد «موقعیت ارزیابی»:** ارزیاب‌ها، خبرنگاران با سابقه و دارای اعتبار در هر رشته هستند. اگر جمعی از آن‌ها خبری را رد کنند، احتمال کذب بودن آن خبر بالا می‌رود.

۵. در رابطه با هویت کاربران، سه سناریو مطرح است که یا همه کاربران هویت نامعلوم داشته باشند یا اینکه در استفاده از هویت واقعی یا مجازی مختار باشند [۲۷] و یا اینکه همه ملزم به فاش کردن هویت واقعی خود باشند. هر کدام از این راه‌ها مزایا و معایب خودشان را دارند. مثلاً اگر سناریوی اول می‌تواند از تقلب جلوگیری کند؛ چرا که به دلیل مخفی بودن هویت افراد، احتمال تبانی ایشان برای رأی‌دهی یا ارزیابی به صفر می‌رسد. ولی عیب آن این است که کسب اعتبار در این پلتفرم منجر به کسب شهرت و اعتبار در واقعیت نخواهد شد.

سه مرحله کسب اخبار، پالایش و انتشار آن را بدون اتکاء به واسطه متمرکز انجام دهد و در عین حال اعتبار سیستم را حفظ کند؟ که این الگوریتم در جواب این سؤال مطرح می‌شود.<sup>۲۵</sup> دلیل این مطلب این است که منطق حاکم بر اعتبارسنجی خبر، منطق فازی است، نه منطق ریاضی.

عیب راه دوم این است که می‌توان اکانت‌ها و هویت‌های جعلی متعدد ایجاد کرد و روی رأی‌گیری تاثیر گذاشت. به‌همین جهت یکی از چالش‌های اصلی این برنامه، جلوگیری از تولید اکانت‌های جعلی و سیستم سنجش هویت خواهد بود.

مزیت بخش سوم این است که افراد به‌دلیل محذوراتی که در دنیای واقعی دارند، به نشر اکاذیب و شایعات اقدام نمی‌کنند. ولی عیبی که این روش دارد این است که به دلیل همین محذورات از بیان بسیاری از حقایق خودداری شود.

۶. هر خبرنگاری که اولین بار یک عنوان خبری را باز کند، صاحب حق امتیاز آن عنوان می‌شود (حق اولویت) و خبرنگاران دیگر تنها می‌توانند ذیل آن عنوان تحلیل بگذارند و هوش مصنوعی (وب معنایی)<sup>۲۶</sup> مانع از تولید اخبار تکراری خواهد شد. اما اگر تاییدگرها رأی بهتری به یک ارزیابی ذیل آن خبر، که بعضی آن خبر را غلط تشخیص داده بدهند و همزمان آن خبر را جعلی بدانند، حق امتیاز آن خبر به ارزیاب منتقل می‌شود.

۷. ذیل یک عنوان خبری، هر کاربر تنها می‌تواند یک نقش ایفا کند. مثلاً اگر به‌عنوان خبرنگار یک خبر را ایجاد کرد، دیگر نمی‌تواند ذیل آن تحلیل بگذارد یا به خبر خود و تحلیل‌های دیگران رأی دهد و اگر به عنوان ارزیاب، خبری را ارزیابی کرد دیگر نمی‌تواند به آن خبر و تحلیل‌های ذیل آن رأی بدهد. اما در دو یا چند عنوان خبری هر کاربر می‌تواند نقش‌های مختلفی را بپذیرد. مثلاً اگر در یک عنوان خبری، خبرنگار است، می‌تواند همزمان در عنوان دیگر ارزیاب بوده و در عنوان دیگر صرفاً تأییدکننده باشد.

۸. یک صفحه نمایش اخبار تاییدنشده وجود دارد و اخباری که در وضعیت‌های «تحلیل و ارزیابی» و «صحت‌سنجی» هستند در آن نمایش داده می‌شوند. یک صفحه نمایش عمومی نیز وجود دارد که اخبار «قضاوت‌شده» بر اساس صحت و اهمیتشان<sup>۲۷</sup> در آن نمایش داده می‌شوند.

۹. در این پلتفرم هرکس آزاد است عنوان خبری جدیدی باز کند، به همین جهت باید نرم‌افزار را طوری برنامه‌ریزی کرد که کاربر مشاهده‌گر خسته نشود. برای این کار، اخبار بر اساس صحت و اهمیتشان مرتب می‌شوند و در نتیجه اخبار مهم در صدر نمایش داده خواهد شد و اخبار ناصحیح یا کم‌اهمیت آنقدر تنزل خواهند کرد که دیده نشوند و سابقه آنها تنها برای خبرنگار آن باقی خواهد ماند.

۱۰. هوش مصنوعی در چند بخش از این روش نقش ایفاء می‌کند. ۱. از تولید اخبار تکراری جلوگیری می‌کند؛ ۲. از تولید عناوین با بار ارزشی جلوگیری می‌کند<sup>۲۸</sup>.

<sup>26</sup>semantic web

<sup>۲۷</sup>البته این ترتیب حالت پیش فرض نرم‌افزار است و می‌توان حالت‌های دیگری مثل ترتیب بر اساس تاریخ یا ترتیب بر اساس محتوا را هم قرار داد و مخاطب در انتخاب این حالت‌ها مختار است.  
<sup>۲۸</sup>چرا که یکی از روش‌های مغالطه در خبر، ایجاد بار ارزشی در عنوان و محتوای آن است.

۱۱. یک سیستم گزارش‌دهی عمومی برای فیلتر و پالایش اخباری که قوانین سیستم را می‌شکنند وجود دارد. مثلاً اگر یک عنوان خبری تکراری وجود داشت و هوش مصنوعی نتوانست آن را تشخیص دهد، اگر تعداد مشخصی از کاربران (مثلاً یکصد هزار نفر) گزارش دهند که این خبر تکراری است، سیستم این خبر را از صفحه نمایش عمومی حذف می‌کند<sup>۲۹</sup>.
۱۲. موضوع هر خبری مثلاً سیاسی یا اقتصادی بودن آن مشخص است و افزایش اعتبار خبرنگار یا تحلیل‌گر تنها در حیطه‌ای است که در آن خبر معتبر منتشر کرده است. مثلاً ممکن است یک کاربر در حیطه سیاسی دارای اعتبار ۱۰۰۰ باشد ولی در حیطه اقتصادی هیچ اعتباری نداشته باشد.
۱۳. می‌توان به‌گونه‌ای سیستم را برنامه‌ریزی کرد که یک خبرنگار یا تحلیل‌گر بتواند محتوای خود را به فروش برساند. یعنی کاربران برای مشاهده محتوای تولید شده توسط وی باید اشتراک تهیه کنند.
۱۴. این سیستم مبتنی بر یک رمزارز می‌باشد. از این رمزارز برای پرداخت‌های درون‌برنامه، گرفتن ودیعه برای جلوگیری از تقلب و دادن پاداش به کاربران استفاده می‌شود.
۱۵. راه‌های تأمین هزینه سیستم برای پرداخت حقوق خبرنگاران و ارزیاب‌ها و پاداش رأی‌دهندگان عبارت است از: فروش رمزارز، مالیاتی که از تراکنش‌های آن رمزارز به دست می‌آید، هزینه‌های رأی‌گیری و ثبت اخبار، تبلیغات مبتنی بر بلاک‌چین به‌صورت مناقصه‌ای<sup>۳۰</sup> و امکان خرید اشتراک خصوصی.

## ۴.۴ جمع‌بندی وظایف بازیگران

### ۱. تأییدگر / رأی‌دهنده:

تأییدگران عموم کاربران سیستم هستند که به واقعی بودن یا جعلی بودن اخبار و ارزیابی‌ها رأی می‌دهند.

کاربران با توجه به هویت و اعتبار خبرنگار، هویت و اعتبار تحلیل‌گران، نظر تحلیل‌گران و محتوای خبر، اقدام به رأی دادن به اخبار می‌کنند. رأی‌دهی به‌صورت صفر و یکی است، یعنی فرد یا خبر را قبول دارد یا قبول ندارد. اگر بخشی از آن را قبول داشته باشد و بخش دیگر را نه، باید به تحلیل مطابق با نظرش رأی مثبت بدهد و اگر چنین تحلیلی ذیل این خبر وجود نداشت، خودش می‌بایست این تحلیل را ایجاد کند<sup>۳۱</sup>.

<sup>۲۹</sup> باید توجه داشت که نمی‌توان یک خبر را از روی بلاک‌چین حذف کرد و نهایتاً می‌توان آن را نمایش نداد و این خبر غیر قانونی به عنوان سوء سابقه برای خبرنگار آن باقی خواهد ماند.

<sup>۳۰</sup> یعنی مکان‌هایی برای تبلیغات در بین اخبار تعبیه شود و حق استفاده از آن به کسانی داده شود که در مناقصه‌های روزانه یا هفتگی یا ماهانه، بیشترین پیشنهاد را بدهند. البته پلتفرم‌های مبتنی بر بلاک‌چین برای تبلیغات نیز ایجاد شده‌اند که می‌توان از آنها هم استفاده کرد.

<sup>۳۱</sup> و اگر اعتبار کافی برای ایجاد این تحلیل نداشت، می‌توان این‌گونه برنامه را نوشت که با پرداخت هزینه بیشتر بتواند تحلیل جدید ایجاد کند و اگر تحلیل اشتباه بود علاوه بر هزینه، اعتبار زیادی را هم از دست بدهد.

رأی هر نفر ۱ امتیاز دارد و رأی کاربران معتبر تفاوتی با کاربران کم‌اعتبار نخواهد داشت. چرا که تفاوت وزن آراء سبب فساد و تقلب خواهد شد. مثلاً اگر ۱۰ نفر با اعتبار بالا بتوانند معادل ۱۰۰۰ نفر رأی داشته باشند، می‌توانند با تبانی، یک خبر ناصحیح را تأیید کنند.

## ۲. خبرنگار :

هر کاربر می‌تواند با هزینه نمودن مقداری اعتبار و توکن، خبر تهیه کند و اگر سیستم تشخیص داد که آن خبر صحیح است اعتبارش افزایش یافته و پاداش می‌گیرد و اگر سیستم تشخیص داد که خبر نادرست است، اعتبارش کاهش یافته و مبلغی که به‌عنوان ودیعه گذاشته بود، از حسابش کسر می‌شود. اعتبار اولیه هر خبرنگار صفر است و نمی‌توان از راهی جز فعالیت در درون همین سیستم کسب اعتبار کرد.

اعتبار و پاداشی که هر خبرنگار از یک خبر کسب می‌کند با دو عامل «صحت خبر» و «اهمیت خبر» رابطه مستقیم دارد. عددی که صحت خبر را نشان می‌دهد همان اعتبار خبر<sup>۳۲</sup> است و متغیرهایی که اهمیت خبر را نشان می‌دهند، تعداد رأی‌دهنده‌ها و اقبال تحلیل‌گران برجسته است. پس عدد اعتباری که خبرنگار برای یک خبر کسب می‌کند برابر است با ضربی از اعتبار خبر، تعداد رأی‌دهندگان و میانگین اعتبار تحلیل‌گرها ضرب در تعداد ایشان<sup>۳۳</sup>.

همچنین اعتبار خبرنگار در هر رشته عبارت است از مجموع اعتباراتی که از فعالیت‌های خبری، تحلیلی و رأی‌دهی ذیل یک حیطه خبری به‌دست می‌آورد. مثلاً ممکن است یک کاربر در حیطه سیاسی دارای اعتبار ۱۰۰۰ باشد ولی در حیطه اقتصادی هیچ اعتباری نداشته باشد.

سابقه خبرنگاران و ارزیاب‌ها شفاف و در دسترس عموم است. همچنین اعتبار خبرنگار در هر حیطه شفاف است. اعتبار خبرنگار تأثیر مستقیم در اعتبار خبر ندارد، چرا که اعتبار خبرنگار محصول اعتبار خبر است.

## ۳. ارزیاب :

ارزیاب با سه گزینه روبه‌رو است که باید یکی را انتخاب کند. ۱. تأیید تمامی خبر ۲. رد تمام خبر ۳. تأیید برخی از مفاد خبر و رد سایر آن. با انتخاب گزینه ۱، تمام رأی‌های مثبت غیرتکراری که به این تحلیل داده می‌شود، برای اصل خبر هم به‌عنوان رأی مثبت لحاظ خواهد شد؛ و با انتخاب گزینه ۲، تمام رأی‌های مثبت غیرتکراری که به تحلیل داده شود، برای اصل خبر به‌عنوان رأی منفی لحاظ خواهد شد.

هر خبرنگاری که اولین بار یک عنوان خبری را باز کند، صاحب حق امتیاز آن عنوان می‌شود (حق اولویت) و خبرنگاران دیگر تنها می‌توانند ذیل آن عنوان تحلیل بگذارند اما اگر تأییدگرها رأی بهتری به

<sup>۳۲</sup> عددی بین مثبت ۱۰۰ و منفی ۱۰۰

<sup>۳۳</sup> این عدد همچنین مبنای رتبه‌بندی پیش‌فرض اخبار در صفحه نمایش عمومی می‌باشد.



یک ارزیابی ذیل آن خبر که برخی از مفاد آن را قبول کرده بدهند و همزمان آن خبر را جعلی بدانند، حق امتیاز آن خبر به ارزیاب منتقل می‌شود.

ارزیابی باعث جلب توجه کاربران به رأی دادن به آن عنوان خبری می‌شود. مثلاً اگر خبری ۱۰ تحلیل داشته باشد که بعضی از تحلیل‌گران مشهور آن را ارزیابی کنند، قهراً مخاطبین بیشتری به آن توجه می‌کنند.

تحلیل‌های ذیل یک خبر با توجه به اعتبارشان رتبه بندی می‌شوند.

## ۵ جمع‌بندی مزایای خبرگزاری بر بستر بلاک‌چین نسبت به خبرگزاری سنتی

۱. جلوگیری از انتشار اخبار نادرست و یا سانسور اخبار درست.

۲. جلوگیری از فیلترینگ و مسدودسازی.

۳. حفظ حق نشر: بر اساس ساختار مبتنی بر امضای دیجیتال، حق نشر محتوا و سابقه اخبار به صورت کامل برای خبرنگار حفظ می‌شود [۲]. تمامی اخبار و اسناد بارگذاری شده در بلاک‌چین منحصراً برای تولیدکننده خواهد بود. همچنین حق اولویت یک عنوان خبری، برای کسی است که اولین بار آن را ثبت کرده باشد. این بخش در روش اجرائی مفصلاً توضیح داده شده است.

۴. اعتباردهی به تولیدکنندگان: در این خبرگزاری یک اعتبار اجتماعی تعریف شده است که منجر به کسب امتیاز تولید خبر و ارتقاء جایگاه ایشان می‌شود؛ و با توجه به غیر قابل تغییر بودن، محتوای ارسالی به اسم آنها باقی خواهد ماند.

۵. استقلال خبرنگار از خبرگزاری: خبرنگار بدون این که نیاز به فروش حق امتیاز خود به یک خبرگزاری را داشته باشد، کسب درآمد می‌کند و مخاطبین می‌توانند اخبار خبرنگاران و تحلیل‌گران محبوبشان را دنبال کنند و مجبور نیستند یک خبرگزاری را دنبال کنند.

۶. تقسیم درآمد سیستم میان کاربران: همانطور که در مفهوم‌شناسی بلاک‌چین گفته شد، یکی از روش‌های جذب کاربر<sup>۳۴</sup> در نرم‌افزارهای مبتنی بر این پروتکل این است که سیستم برای ایشان پاداش در نظر می‌گیرد. معمولاً در این سیستم‌ها رمزارزهایی تعریف می‌شود که دارای ارزش مالی هستند و سیستم از این رمزارزها برای دادن پاداش به افراد استفاده می‌کند. این پاداش یکی از عواملی است که باعث جذب به بلاک‌چین و در نتیجه مقبولیت آن می‌شود. ساز و کار پاداش در بخش پنجم توضیح داده شده است.

<sup>۳۴</sup> در این جا منظور از کاربر، اشخاصی هستند که اقدام به تأیید بلوک‌ها می‌کنند یا به عبارت دیگر همان ماینرها.

۷. **استقلال صنعت خبر از تبلیغات:** وابستگی خبرگزاری‌ها به تبلیغات باعث شده تا مرز بین خبر و رپرتاژ آگهی کمرنگ شود. خبرگزاری مبتنی بر بلاک چین می‌تواند خبرگزاری مستقل از تبلیغات را ممکن کند.
۸. **رویکرد تغییرناپذیر:** محتوای خبری، فیلم‌ها یا تصاویر ذخیره شده در بلاک چین تغییرناپذیر است.
۹. **ترتیب واقعی اخبار:** یکی از راه‌های تحریف و مغالطه در خبر، شیوه ترتیب‌دهی اخبار است. رتبه‌بندی اخبار در این سیستم بر اساس اهمیت واقعی آنها و نیاز مخاطبین خواهد بود نه به ترتیبی که واسطه‌های خبری می‌خواهند برای مخاطبین خود شکل بدهند [۸].
۱۰. **توسعه رمزپول ملی با ساخت خبررسانی بر روی آن بستر:** با توجه به تصویب رمزپول ملی در شورای پول و اعتبار<sup>۲۵</sup>، ایجاد نرم‌افزارهای اطلاع‌رسانی بر بستر پروتکل رمزارز ملی می‌تواند باعث تقویت و افزایش محبوبیت رمز پول ملی شود.
۱۱. **ردیابی و شفافیت سیر تولید خبر و منابع آن.**

## ۶ چالش‌های خبررسانی مبتنی بر بلاک چین

همان‌طور که اجرای فناوری‌ها و ایده‌های جدید گاهی معارض و در تضاد با برخی از مکانیسم‌ها و قواعد است، احتمال می‌رود که استفاده از بلاک چین برای خبرگزاری هم این مشکل را داشته باشد. از این رو به برخی از آن موارد اشاره می‌گردد ولی باید توجه داشت که حل آنها نیاز به مقاله دیگری دارد.

**انتشار اخبار خلاف مصلحت:** گفته شد که در خبررسانی غیرمتمرکز، امکان فیلتر یا سانسور وجود ندارد و تمامی اخبار صحیح منتشر خواهد شد. یکی از مسائل و چالش‌های اصلی این است که انتشار بسیاری از اخبار، هرچند که صحیح هستند، خلاف مصلحت عمومی است [۳].

**خبرگزاری‌های سنتی:** گسترش و مقبولیت خبررسانی غیرمتمرکز باعث تعطیل شدن خبرگزاری‌های سنتی خواهد شد. همان‌طور که به وجود آمدن نرم‌افزارهای حمل و نقل آن‌لاین مثل اسنپ باعث ضرر ذی‌نفعان سنتی این بازار شد. به همین جهت یکی از چالش‌ها ارائه راهکار برای به حداقل رساندن ضرر ذی‌نفعان سابق صنعت خبررسانی می‌باشد.

**فضای ذخیره‌سازی:** در بسیاری از بلاک چین‌های کنونی، اندازه بلاک‌ها یا تراکنش‌ها خیلی زیاد نیستند و نهایتاً هر بلاک مسئول ثبت چند معامله از یک کاربر به کاربر دیگر می‌باشد. گسترش اطلاعات این شبکه‌ها باعث مشکل ماینرها و نودهای شبکه شده است. این مشکل در فضای رسانه، به دلیل حجم انبوه متن، عکس و فیلم قطعاً جدی‌تر خواهد بود.

<sup>۲۵</sup> خبرگزاری مهر، ۴ بهمن ۱۴۰۰

**احراز هویت:** یکی دیگر از چالش‌های جدی این خبررسانی‌ها، احراز هویت واقعی خبرنگاران و تحلیل‌گران است.

**حریم خصوصی:** یکی از چالش‌ها برای همه پلتفرم‌های مبتنی بر دفتر کل توزیع‌شده عمومی<sup>۳۶</sup>، چالش رعایت حریم خصوصی است؛ چرا که تمام اطلاعات از جمله اطلاعات هویتی کاربران در بین تمام گره‌ها پخش می‌شود. خبرگزاری بر بستر بلاک‌چین علاوه بر این، دارای چالش دیگری هم هست و آن چگونگی رعایت حفظ حریم خصوصی اشخاص و عدم نشر اخبار شخصی ایشان است.

## ۷ نتیجه‌گیری

در این مقاله اثبات شده است که یک نرم‌افزار خبری مبتنی بر پروتکل بلاک‌چین می‌تواند با اعتبارسنجی غیرمتمرکز اخبار، حذف واسطه خبرگزاری و ایجاد ریسک در تولید خبر، باعث از بین رفتن اخبار جعلی، تحریفات و سانسور اخبار شود و از طرفی به خاطر شفافیت مراحل تولید خبر و پالایش غیرمتمرکز اخبار، باعث افزایش اعتماد مخاطبین به محتوای تولید شده در آن می‌شود. همچنین فیلتر کردن و مسدودسازی پروتکل‌های مبتنی بر دفتر کل توزیع‌شده، بسیار دشوار و هزینه‌بر است. در نهایت، این نرم‌افزار خبری به دلیل تقسیم درآمد تولیدشده در سیستم بین کاربران به وسیله رمزارز، ایجاد استقلال صنعت خبر از تبلیغات، اعتباردهی حرفه‌ای به تولیدکنندگان محتوا و حفظ حق نشر خبرنگاران و تحلیل‌گران، باعث جذب مخاطبین داخلی و خارجی خواهد شد. به همین دلیل، این خبرگزاری می‌تواند شش مشکل اصلی مغلوب بودن در فضای خبررسانی را حل کرده و منجر به ارتقاء جایگاه خبری جمهوری اسلامی شود.

## مراجع

- [۱] افشار، حمیدرضا (۱۳۹۹). ارائه مدل مفهومی فرصت‌ها و تهدیدات به کارگیری و توسعه فناوری زنجیره بلوکی در جمهوری اسلامی ایران، فصلنامه علمی امنیت ملی، سال دهم، شماره ۳۶، صص ۳۰۷-۳۴۸.
- [۲] اسلامی تبار، امیر؛ ناصر، مهدی (۱۳۹۹). کارکرد بلاک‌چین در حمایت از کپی‌رایت، مجله علمی پژوهش حقوق خصوصی - شماره ۳۰.
- [۳] تناور، عبدالمجید (۱۳۹۷). از اخلاق رسانه تا فقه رسانه، پژوهشنامه تاریخ، سیاست و رسانه، صص ۲۶۷ تا ۲۹۱، سال اول، شماره دوم.
- [۴] شهبازی، محمد (۱۳۹۹). بررسی کاربردی الگوریتم‌های اجماع استفاده شده در شبکه‌های بلاک‌چین، فصلنامه سیاست‌نامه علم و فناوری، دوره ۱۰، شماره ۳، صص ۳۵-۵۴.
- [۵] رجیبی، ابوالقاسم (۱۳۹۷). فناوری دفاتر کل توزیع شده فراتر از فناوری زنجیره بلوکی، مرکز پژوهش‌های مجلس، شماره مسلسل: ۱۵۹۲۰.
- [۶] رجیبی، ابوالقاسم (۱۳۹۶). آشنایی با فناوری راهبردی زنجیره بلوکی و کاربردهای آن، مرکز پژوهش‌های مجلس، معاونت پژوهش‌های زیربنایی و امور تولیدی، دفتر مطالعات ارتباطات و فناوری‌های نوین، کد موضوعی: ۲۸۰، شماره مسلسل: ۱۵۳۴.

<sup>36</sup>public blockchain

- [۷] فرزামী، هومن (۱۳۹۹). فرصت های تحولی فناوری زنجیره بلوکی در بخش معدن و صنایع معدنی (چالش های عملیاتی و سیاستی توسعه آن در ایران)، شماره مسلسل : ۱۷۰۲۳.
- [8] Agrawal, Vaibhav. “Decentralised Ecosystem for Journalism based on Blockchain,” IC-BCT 2019: Proceedings of the International Conference on Blockchain Technology, pp 7-19, 2019.
- [9] Aitamurto, Tanja. “New ecosystem in journalism: Decentralized newsrooms empowered by self-organized crowds” School of Communication, Media and Theatre Centre for Journalism, Communication and Media Research, Tampere University, Finland, 2011.
- [10] “ANSA leveraging blockchain technology to help readers check source of news,” [https://www.ansa.it/english/news/science\\_tecnology/2020/04/06/ansa-using-blockchain-to-help-readers\\_af820b4f-0947-439b-843e-52e114f53318.html](https://www.ansa.it/english/news/science_tecnology/2020/04/06/ansa-using-blockchain-to-help-readers_af820b4f-0947-439b-843e-52e114f53318.html), 2020.
- [11] “Australia’s Blockchain Roadmap,” [www.dfat.gov.au](http://www.dfat.gov.au).
- [12] Balouchestani, Arian. “SANUB: A new method for Sharing and Analyzing News Using Blockchain,” Department of Engineering, Ferdowsi University of Mashhad (FUM), Mashhad, IRAN, 28-29 August 2019.
- [13] Bernat, Ivancsics. “Blockchain in Journalism,” [https://www.cjr.org/tow\\_center\\_reports/blockchain-in-journalism.php#journalism](https://www.cjr.org/tow_center_reports/blockchain-in-journalism.php#journalism).
- [14] Deloitte. “The Blockchain (R)evolution,” 2017.
- [15] Durov, Nikolai. “Telegram Open Network,” 2017.
- [16] Ghodake, Yash. “Design of Realtime Fake News Detection using Blockchain,” Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India, Volume: 07 Issue: 04, 2020.
- [17] J. Daniel, A. Sargolzaei, M. Abdelghani, S. Sargolzaei and B. Amaba. “Blockchain Technology, Cognitive Computing, and Healthcare Innovations,” Journal of Advances in Information Technology, vol. 8, 2017.
- [18] Jeffries, Adrienne. “Blockchain is meaningless,” <https://www.theverge.com/users/adrienne>, 2018.
- [19] Julia Ziemer and Charlie Beckett. What use is blockchain for journalism?, the London school of economics and political science, 2018.
- [20] Lucinda Shen. “As China Censors MeToo Activists, Ethereum’s Blockchain Proves to Be an Unlikely Ally,” <https://fortune.com/2018/04/25/ethereum-blockchain-metoo-rape>, 2018.
- [21] Mondrus, David. “trivetm whitepaper,” <https://trive.news/whitepaper.0.2.6x.pdf>.
- [22] Paula Fraga-Lamas. “Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality,” Faculty of Computer Science, Universidade da Coruña, 15071, A Coruña, Spain , 2019.

- [23] Rocco, Gregory. "Public Blockchains as a Means to Resist Information Censorship" The Graduate Center, City University of New York , 2019.
- [24] Shealy, Matt. "How open source underpins blockchain technology" <https://opensource.com/article/20/10/open-source-blockchain>, 2020.
- [25] Shilina, Sasha. "Journalism + Blockchain: Possible solution for an industry crisis?," <https://medium.com/paradigm-research/journalism-blockchain-possible-solution-for-an-industry-crisis-becd6da3714f>, 2019.
- [26] Sigalos, Mackenzi. "Bitcoin mining isn't nearly as bad for the environment as it used to be, new data shows," <https://www.cnbc.com/2021/07/20/bitcoin-mining-environmental-impact-new-study>, 2021.
- [27] Taghizadeh, Mahdi. "Journalism over the Blockchain," <https://mahdi.medium.com/journalism-over-the-blockchain-or-a-decentralized-medium-com-8b15289d4667>, 2018.
- [28] Takyar, Akash. "Blockchain In Fake News," <https://www.leewayhertz.com/blockchain-fake-news>, 2020.
- [29] Torky, Mohamed. "Proof of Credibility: A Blockchain Approach for Detecting and Blocking Fake News in Social Networks," International Journal of Advanced Computer Science and Applications, Vol. 10, No. 12, 2019.
- [30] Why does journalism need blockchain technology?. <https://blog.joincivil.com/why-does-journalism-need-blockchain-technology-6db1b4ff84ba>.
- [31] Zhang ,Haoqian. "A Decentralized Information Sharing Platform Based on Blockchain" , 2020
- [32] Zheng Z, Xie S, Dai H, Chen X. "An overview of blockchain technology: architecture, consensus, and future trends," In: 6th IEEE international conference on big data. IEEE Press, New York, pp 557–559 , 2017.





## بازجستی در چرایی جرائم رایانه‌ای و راهکارهای مقابله با آن

سهیل معیری<sup>۱</sup>

<sup>۱</sup> کارشناسی ارشد حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی واحد زاهدان  
dr.h.sh31@gmail.com

### چکیده

با توجه به ویژگی‌هایی چون بدون مرز بودن فضای مجازی، کم‌هزینگی و پرتیری و پایین بودن احتمال دستگیری یا مجازات، امکان وارد آوردن خسارات بالا بدون آسیب جسمانی مجرم، آسان بودن تهیه و امکانات و عوامل مورد نیاز جرم، بازتاب جهانی موفقیت، امکان جذب حامی و همکار برای ارتکاب جرم از سراسر جهان بدون حضور فیزیکی، امکان جذب منابع مالی و پول شویی آسان‌تر و هرگونه انجام فعالیت‌های مالی الکترونیکی در جهت اهداف مجرمانه و پیچیدگی جرائم رایانه‌ای، مطالعه و پژوهش بیشتر و نیز تصویب قوانین مورد نیاز در این زمینه، امری بسیار ضروری است. پیشنهادات در حال حاضر با عنایت به پیشرفت‌های لحظه‌ای در عرصه رایانه و فضای سایبر ضرورت آموزش بیش از پیش مشخص شده و برای اجرای یک سیاست کیفری مؤثر جهت پیشگیری از جرائم رایانه‌ای عبارتند از: ۱- از آنجا که پلیس به عنوان ضابط دادگستری و وظیفه کشف جرائم را بر عهده دارد، در کنار آموزش قضات و سایر مقدمات قضایی، آموزش پلیس نیز باید در سرفصل برنامه‌ریزی‌ها قرار گیرد ۲- آموزش‌های عمومی در سطح کارمندان دولت و نظامیان و هم‌چنین مقامات قضایی ۳- تا حد ممکن عدم ذخیره‌سازی داده‌ها و اطلاعات طبقه‌بندی‌شده به شبکه‌های رایانه‌ای به خصوص شبکه جهانی اینترنت. ۴- مسدود کردن درگاه‌های رایانه‌های حساس در ادارات به عنوان راهکاری سریع و کم‌هزینه و در عین حال مؤثر.

**کلمات کلیدی:** فضای سایبر، جرائم رایانه‌ای، فضای مجازی.

## ۱ مقدمه

بشر در طول حیات خود اعصار گوناگونی را پشت سر گذاشته و هریک از آنها را با الهام از تحول عظیمی که در آن عصر پدید آمده و گامی از رشد و تکامل بشری را رقم زده نام‌گذاری کرده است، مانند: عصر آتش، عصر آهن و عصر حاضر که عصر فناوری اطلاعات و ارتباطات نام گرفته است. می‌توان گفت به‌طور کلی تمام فعالیت‌های انسانی از گذشته تاکنون در حال پیشرفت بوده است همواره ابزاری ابداع و اختراع نموده است تا در ارتقاء رفاه و آسایش زندگی خود و خانواده مؤثر گردد، اما در اواخر سده بیستم، عصر فراصنعتی شاهد ظهور پدیده‌ای شگرف، پدیده‌ای که در حقیقت به معنای تولد جهانی دیگر با شرایط و ویژگی‌های جهان کنونی بود که این دنیای جدید، فضای مجازی یا فضای سایبر نام گرفت و هنوز نیم قرن از اختراع اولین

رایانه نمی‌گذرد که سرعت عمل آن از ابتدایی‌ترین ماشین حساب‌های دیجیتال امروزی نیز کمتر بود، اما به هر حال تحولی شگرف در دنیای علم و فناوری محسوب می‌شد و از همین رو رایانه‌ها در این مدت کم به خوبی توانستند جای خود را در تمامی شئون زندگی انسان باز کنند و به نوعی خود را در تمامی پیشرفت‌ها سهیم سازند اما بهره‌برداری روزافزون از سیستم‌های رایانه‌ای زمانی شتاب بیشتری به خود گرفت که امکان متصل گردیدن آنها به یکدیگر در سراسر جهان فراهم شد. این پیشرفت، به وسیله جامعه‌شناسان، دومین انقلاب صنعتی نامیده شده است اما نکته مهم اینجاست که هرچند این فضا با همه گستردگی و جهان شمول بودنش و تأثیرات مثبتی در زندگی انسان‌ها بر جای گذاشته است اما هرگز از نگاه قانون‌مداران علم حقوق خارج نبوده و به محض ظهور این فضا، علم حقوق و ابزارهای آن نیز به بررسی ابعاد این فضا از نگاه حقوقی پرداختند. به عبارت دیگر چون فضای سایبر از همان بدو تولد در دسترس همگان قرار گرفت، هر کس مطابق اغراض و مقاصد خود از آن سود می‌جست و آثار منفی و مخرب فرهنگی هم این محیط بر جای گذاشت که بعضی از این بهره‌برداری‌ها جنبه سوء استفاده به خود گرفت و بالطبع قانون‌گذاران را واداشت که تدابیری بیاندیشند، به همین علت دخالت علم حقوق، ضرورت یافت. این سوء استفاده‌ها که می‌توان گفت که در مجموع جرائم رایانه‌ای نام گرفته‌اند، طیف جدیدی از جرائم هستند. طبیعتاً مجازات‌های قوانین رایانه‌ای، امروزه برای مجازات مجرمین کافی اما کامل نمی‌باشد، چون هر روز جرایم جدیدی به وجود می‌آید که برای مجازات آنها نیاز به قوانین جدید داریم. همان‌گونه که جرایم اینترنتی همیشه در حال به‌روز شدن هستند، بایستی تلاش کرد تا بتوان با نو شدن جرایم، هر ساله قوانینی را که با جرایم جدید متناسب باشد ارائه کرد و از جهتی نیز بایستی سعی شود در زمینه جرایم رایانه‌ای مجازات‌ها بازدارندگی بیشتری داشته باشند تا امنیت و آسایش جامعه در پرتو همکاری مردم و مسئولیت توأماً فراهم گردد.

بشر در طول حیات خود با دوره‌های گوناگونی از تحول و تکامل مواجه بوده است که از اوایل قرن بیستم، زمره‌های محوریت یافتن عنصر دیگری شنیده شد در این عنصر که در همان دوران صنعتی واجد ارزش بودن خود را به اثبات رسانیده بود، به تدریج با پا گذاشتن به سده بیستم موقعیت خود را تثبیت کرد و تا آنجا پیش رفت که به دوران صنعتی پایان داد و بشر را وارد عصر پسا صنعتی یا پسامدرن کرد. این عنصر با ارزش، اطلاعات نام دارد و حدود یک قرن است که بشر تلاش خود را صرف تجلی آن در تمامی عرصه‌های سیاسی، اقتصادی، اجتماعی و فرهنگی کرده است. بی‌تردید هرکاری ابزاری می‌خواهد و ابزار فناوری اطلاعات و ارتباطات، تحقق یک جامعه به‌واقع اطلاعاتی است. دلیل اشاره به عامل ارتباطات، به لحاظ جایگاه ویژه آن در توسعه و تکامل اطلاعات است. ارتباط و به‌تبع آن ابزارهای ارتباطی، از همان ابتدا از عناصر حیاتی محسوب می‌شدند و می‌توان گفت اگر وجود نداشتند، بشر هیچ‌گاه نمی‌توانست به این حد از رشد و بالندگی برسد. دو فناوری در عرصه فناوری اطلاعات و ارتباطات نقش تعیین‌کننده‌ای به عهده داشته‌اند که عبارتند از: رایانه (هدف از اختراع رایانه، تسریع و تسهیل پردازش) و مخابرات اطلاعات بود که به خوبی به ثمر نشست و مخابرات نیز به عنوان مهم‌ترین ابزار ارتباطی در نشر این اطلاعات پردازش شده نقش بسزایی ایفا کرده است. به تدریج با کشف قابلیت‌های شگرف ناشی از تلفیق این دو فناوری، انقلابی در عرصه فناوری اطلاعات و ارتباطات رقم خورد. اوج این انقلاب را می‌توان در ظهور شبکه‌های اطلاع‌رسانی رایانه‌ای جهانی دانست که تحولی بنیادین را در این حوزه رقم زده‌اند. این شبکه‌ها فضایی با ویژگی‌های کاملاً متمایز از دنیای فیزیکی به وجود آورده‌اند

که عده‌ای آن را فضای مجازی نامیدند و برخی هم عنوان فضای سایبر را برای آن برگزیده‌اند. اما ناگفته پیداست که فضای سایبر همانند دیگر عناصر زندگی اجتماعی، از گزند یک پدیده بسیار انعطاف‌پذیر و لاینفک از اجتماع به نام جرم در امان نمانده است. به‌طور کلی، آنچه امروز تحت عنوان رفتار مجرمانه در این گروه جرایم قرار می‌گیرد، دو طیف می‌باشند: گروه اول جرایمی هستند که نظایر آنها در دنیای فیزیکی نیز وجود دارد و فضای سایبر بدون تغییر ارکان مجرمانه‌شان، با امکاناتی که در اختیار مجرمان قرار می‌دهد، ارتکابشان را تسهیل می‌کند. جرایم تحت شمول این حوزه بسیار گسترده‌اند و از جرایم حتی بین‌المللی گرفته تا جرایم علیه اموال و اشخاص را در بر می‌گیرند. نمونه‌ای از این طیف، تشویش اذهان عمومی از طریق سایبر است. اما طیف دیگر این جرایم، به سوءاستفاده‌های منحصر از این فضا مربوط می‌شود که امکان ارتکاب آنها در فضای فیزیکی میسر نیست که جرایمی نظیر دسترسی غیرمجاز به داده‌ها با سیستم‌ها یا پخش برنامه‌های مخرب نظیر ویروس‌ها، جز در فضای سایبر قابلیت ارتکاب ندارند و به همین دلیل به آنها جرایم سایبری محض گفته می‌شوند. بنابراین، برای مقابله با چنین جرایمی و سوء استفاده از آن نیازمند تدوین قوانین جدیدی هستیم که حقوق سایبری نام دارد.

## ۲ ویژگی جرایم رایانه‌ای

در خصوص بیان ویژگی‌های جرایم رایانه‌ای نکته قابل توجه این است که کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند، بدون در نظر گرفتن اینکه این اطلاعات و خدمات در کدام نقطه دنیا واقع شده است. محیط سایبر زمینه فعالیت‌های اقتصادی مهم و ابزار ضروری برای انجام کلیه معاملات تجاری و در سطح بین‌المللی بدون دخالت مستقیم بشر فراهم آورده است. محدوده فعالیت کاربر به مرزهای فیزیکی یک خانه یا یک محل کار و حتی مرزهای یک کشور محدود نبوده و در یک سطح کم هزینه هر کاربر می‌تواند در هر زمانی و در هر مکانی با مردم در هر نقطه‌ای از جهان ملاقات کند و اطلاعات مبادله کند، بدون اینکه از محل واقعی و هویت فرد خبر داشته باشد. از بعد اقتصادی، سایبر را می‌توان یک بازار واحد جهانی دانست که از ثمره‌های موفق جامعه مبتنی بر تکنولوژی مدرن اطلاعاتی می‌باشد که با روند توسعه آن روابط اجتماعی و سنتی و فرهنگی حاکم بر روابط افراد را در سطح ملی دچار تحول نماید در واقع همواره چون ارائه تعریف دقیق و جامع و مانعی از فضای سایبری امکان‌پذیر نمی‌باشد اما با وجود این تفاوت‌ها نباید سه ویژگی اصلی را برای فضای سایبری دور از نظر داشت و آن هم به شرح ذیل است: نخست: پیچیدگی تکنولوژی (عدم توانایی در شناخت ابعاد پیچیده جرایم سایبری و فضای سایبر)؛ دوم: تنوع و گوناگونی جرایم سایبری (به دلیل تحول و توسعه فضای سایبر)؛ سوم: توان مرموز سازی جرایم سایبری در این راستا مراجع قانون گذاری کشورهای مختلف و اسناد بین‌المللی، اعم از ارشادی و الزام آور، هرکدام به فراخور نیازها و تهدیدات پیش رو تعاریف متفاوتی از این جرایم ارائه کرده‌اند که ویژگی‌هایی را نیز به همراه دارند.

### ۳ علت‌شناسی جرایم سایبری

ژان پیناتل در بیان علت جرم می‌گوید: «شرط لازمی که بدون آن رفتار مجرمانه بروز نمی‌دهد» علت‌شناسی از اصول بنیادین دانش جرم‌شناسی محسوب می‌گردد؛ به‌گونه‌ای که اهداف جرم‌شناسی در زمینه پیشگیری و درمان بزه، با شناخت علل ارتكابی آن مقدر می‌باشد. لذا جرم‌شناسان برای مقابله با یک جرم با ترسیم یک رابطه علت و معلولی، سعی در خنثی نمودن علل مؤثر در ایجاد نتیجه مجرمانه می‌نمایند همان‌گونه که در بررسی علل جرایم سنتی با دامنه گسترده‌ای از علل روبرو هستیم، در ارتباط با دنیای جدیدی به نام « فضای سایبر» نیز علاوه بر علل احصاء شده در جرایم سنتی، عوامل متعدد و جدیدی با توجه به ویژگی‌های خاص این فضا در شکل‌گیری جرایم سایبری تأثیرگذار می‌باشند. بنابراین، امروزه در کنار دنیای حقیقی با دنیای مجازی مواجه هستیم که دارای سه ویژگی عمده و اصلی می‌باشند: انعطاف‌پذیری عناصر تشکیل‌دهنده جرم در زمان و مکان، ناشناس ماندن نسبی مرتکبان در فضای مجازی که در واقع شناسایی آنان و محل ارتكاب جرم را دشوار می‌نماید و جهانی بدون گسترده ارتكاب بزه که به بزهکاران اجازه می‌دهد بتوانند جرم را بدون حضور در محل یا از اقصی نقاط جهان انجام دهند [۸]. در این گفتار، تمرکز روی علل کلی ارتكاب جرایم اعم از سنتی و سایبری قرار داده شده و در تبیین این علل ویژگی‌های خاص فضای مجازی به‌عنوان متغیری ویژه و تعیین‌کننده، مد نظر قرار خواهد گرفت.

#### ۱.۳ علل فردی

جنس، سن، بدبینی، خودخواهی، نفرت، کینه، جنون، ثروت، جنون اخلاقی، پرخاشگری، عصبانیت آنی و انتقام از عوامل فردی است که با توجه به وضعیت زیستی - روانی فرد، وی را متمایل به انجام یک رفتار خلاف هنجار می‌کند. برای مثال، آنچه در خصوص سن مرتکبین جرایم سایبری به‌عنوان یکی از علل فردی قابل توجه است، وقوع جرایم مالی در سنین بالا و جرایم علیه عفت و اخلاق عمومی در سنین پایین است. در واقع، نوجوانان سهم عظیمی در جرایم نوع دوم به خود اختصاص داده‌اند. شخص نوجوان پس از ورود به مرحله بلوغ با تغییر و تحولاتی در وضعیت جسمی، روانی و شخصیتی خود مواجه می‌گردد که این تغییرات و وجود محیطی پرجاذبه و قابل دسترس به‌عنوان دنیای مجازی وی را به سوی این دنیای جدید متمایل می‌سازد. در این رابطه سوء استفاده‌کنندگان جنسی از اطفال با استفاده از فضای مجازی که قادر به بارگذاری و توزیع حجم بالایی از مسائل مربوط به پورنوگرافی می‌باشد، گروه‌هایی با افکار و عقاید یکسان تشکیل می‌دهند و به‌دنبال آن به سرعت ارائه سرویس‌های اینترنتی را به تشکیل گروه‌های روسپی‌گری و جنسی در میان کودکان و نوجوانان در دنیای حقیقی تبدیل می‌نمایند. امروزه کودکان و نوجوانان با دسترسی به فضای مجازی و حجم وسیعی از تبلیغات و فیلم‌ها و عکس‌ها و مطالب و شخصیت‌ها آشنا می‌گردند که این وضعیت در کنار آثار مثبتی که دارد، آثار منفی و مخربی نیز به بار آورده است. لذا جوامع جهت اصلاح و تربیت صحیح نسل‌های آینده خود همواره به‌دنبال مقابله با این عوامل بوده است. آنچه به‌عنوان علل گرایش کودکان و نوجوانان به محتویات مبتذل قابل ذکر است، در واقع وضعیت سنی، خواسته‌ها و ارزش‌های مورد تقاضای این قشر، جاذبه این محتویات و عدم وجود جایگزین مشروع می‌باشد. لذا افراد در سنین پایین

به دلیل شرایط خاصی که در آن قرار دارند و بیشتر تحت تأثیر عوامل محیطی قرار می‌گیرند. لذا اتخاذ تدابیر بازدارنده و پیش‌بینی جایگزین‌های مشروع و پرجاذبه در این زمینه می‌تواند کمک‌کننده باشد. از دیگر علل فردی که موجب شکل‌گیری جرایم بالاخص جرایم سایبری می‌گردد، ویژگی‌های روانی - شخصیتی افراد است. کینه‌توزی با یک جنون اخلاقی یا جنون ثروت یا عصبانیت آنی هر یک به نوبه خود، فرآیند ارتکاب جرم را سرعت می‌بخشد. بنابراین همان‌گونه که از مصادیق علل فردی مشخص است برخی ویژگی‌های روانی شخصیتی با تأثیر از محیط اطراف از علل اصلی گرایش به ارتکاب جرایم سایبری محسوب می‌گردد که البته ماهیت فضای سایبر و تساهل انجام اقدامات مجرمانه در آن نیز مزید بر علت است و خودنمایی و سرگرمی از دیگر علل فردی است که طی آن در اکثر موارد اشخاص صرفاً جهت نشان دادن توانایی و استعداد خود مرتکب این جرایم می‌گردند، به گونه‌ای که هک کردن یک سایت یا دسترسی به داده‌های دیگری یا مختل کردن یک داده را امری مطلوب و افتخارآمیز تلقی می‌کنند که البته مقابله با این‌گونه افراد مشکلات خاص خود را دارد.

### ۲.۳ علل اجتماعی

وضعیت فرهنگی حاکم بر فرد و جامعه، وضعیت خانوادگی و گروه هم‌سالان و محیطی که فرد در آن زندگی می‌کند، وضعیت اقتصادی، بی‌اعتقادی به هنجارها، نحوه فعالیت رسانه‌های جمعی و غیره از جمله عوامل اجتماعی هستند که در گرایش فرد به ارتکاب جرم، به‌ویژه جرایم سایبری، تأثیر بسزایی دارند. در این راستا به مهم‌ترین این عوامل اشاره می‌شود.

#### ۱.۲.۳ ضعف فرهنگی

دین و مذهب و اعتقاد به ارزش‌های تعیین شده جامعه از ابزارهای مهم پیشگیری از جرم محسوب می‌گردد تا جایی که به‌طور مثال، در محدوده فضای سایبر، اعتقاد به ارزش‌های دینی، ناخودآگاه فرد را از ارتکاب جرایم سایبری به‌خصوص در زمینه محتویات مبتذل باز خواهد داشت. بنابراین، تضعیف این اعتقادات، بی‌تفاوتی فرد به ارزش‌های جامعه را به همراه داشته و این معضل تأثیر خود را در فضای مجازی که محیطی امن و آرام برای ارتکاب اقدامات معارض با قانون است، بروز می‌نماید. علاوه بر این مورد سطح تحصیلات و آگاهی در عین اینکه تأثیر مثبتی دارد، خود نیز می‌تواند از عوامل اصلی ارتکاب جرایم سایبری محسوب گردد. لذا برخلاف جرایم سنتی که گاهی اوقات بی‌سوادی از علل اصلی ارتکاب آن جرایم محسوب می‌گردد، در جرایم سایبری بی‌سوادی و ناآگاهی از مفاهیم سایبری موجب ارتکاب این جرایم نمی‌گردد بلکه داشتن سواد و تخصص حتی در برخی از جرایم سایبری خاص از علل اصلی ارتکاب آن جرایم خاص محسوب می‌گردد. در کنار این موارد فقدان فرهنگ استفاده صحیح از رایانه و فضای مجازی در کشورهای در حال توسعه و عدم آگاهی از خطرات و آسیب‌های دنیای مجازی می‌تواند از علل دیگر شکل‌گیری محیط مساعد برای ارتکاب جرایم سایبری محسوب گردد.

### ۲.۲.۳ شرایط نامساعد اقتصادی

تورم، فقر اقتصادی، فساد اقتصادی، بیکاری و وضعیت نابسمان زندگی از جمله عللی است که از گذشته تاکنون جوامع انسانی را تحت تأثیر قرار داده و همواره آثار خود را در زمینه سیاسی، اجتماعی، فرهنگی و حقوقی نشان داده است. جرایم اعم از سنتی و سایبری در پاره‌ای از موارد متأثر از شرایط اقتصادی فرد و جامعه قرار خواهند گرفت و به عبارتی دیگر ارتکاب جرم راه‌حلی جهت رهایی از فشاری است که طبق قاعده فشار رابرت مرتون از عوامل اقتصادی بر فرد تحمیل گردیده است تا جایی که امروزه طبق آمار اعلام شده در ایران حدود ۸۰ درصد جرایم رایانه‌ای را جرایم مرتبط با امور مالی و اقتصادی تشکیل می‌دهد. برای مثال، کلاهبرداری و سرقت داده‌ها جهت کسب مال تحت عنوان فیشینگ از جمله جرایم سایبری است که می‌تواند زیربنای اقتصادی داشته باشد. فقر اقتصادی یا جنون ثروت ممکن است فرد را به استفاده از ابزارهای نامشروع جهت کسب ثروت تحریک کند. و در این راستا از فضای مجازی به‌عنوان محیطی امن استفاده کرده و با استفاده از یک رایانه و فقط نشستن در خانه و مقداری تخصص، سیستم‌های رایانه‌ای را مختل کند. بنابراین آنچه در برخی موارد موجب ارتکاب یافتن این جرایم می‌گردد، شرایط نامساعد اقتصادی فرد یا جامعه است؛ چه بسا با ایجاد یک سیاست اقتصادی مناسب از میزان ارتکاب این جرایم کاست.

### ۳.۲.۳ خانواده‌های نابسامان

محیط خانواده محیطی است که فرد در آن به دنیا آمده و در آن به حیات خود ادامه می‌دهد و محققان بر این عقیده‌اند که فرد تحت تأثیر شدید والدین و اعضای خانواده‌اش قرار می‌گیرد و به‌همین دلیل وضع خانوادگی او در بروز رفتارهای خطرناک و ارتکاب جرایم تأثیری مستقیم دارد. این‌گونه تأثیر بر شکل‌گیری منش و شخصیت فرد و در نتیجه رفتارهای آتی آنها بسیار اثرگذار می‌باشد. دوگرف در این باره می‌نویسد: «اثرات سال‌های عمر بر تکوین و تحول آتی شخصیت افراد بسیار بدیهی بوده است و اگر خانواده به وظایف تربیتی عمل کند و اگر روابط بین والدین و فرزند طبیعی باشد و در محیط جو عاطفی محبت حاکم باشد و در نهایت اگر تمام نیازهای طبیعی فرد فراهم گردد، طفل به‌راحتی اجتماعی شده و همچنین در روابط خانوادگی و بیرون از آن رفتار متعادل خواهد داشت اما اگر شرایط و موقعیت به صورت دیگری باشد، یعنی خانواده از نظر تربیتی دچار نقیصه شده و اگر طفل از کمبود شدید عاطفی رنج ببرد و اگر والدین از هم جدا شده باشند، بدیهی است نتایج زیان‌بار آن دیر یا زود در طفل مشاهده خواهد شد. خانواده نقش تعیین‌کننده و قاطعی در انگیزه‌شناسی بزهکاری جوانان تعیین می‌نماید» [۵]. بنابراین خانواده به‌عنوان اولین نهاد اجتماعی که با آن سر و کار دارند، حسب وضعیت و شرایط حاکم بر آن، تأثیر زیادی بر جامعه‌پذیری یا اجتماع‌گریزی دارد. اینگونه تأثیرات منفی، اختصاص به جرم خاصی ندارد و چه‌بسا شرایط حاکم بر یک خانواده به‌گونه‌ای باشد که در آن ارتکاب انحرافات سایبری امری قبیح محسوب نگردد و کودک و نوجوان با نوعی مشوق همراه بشوند. یقیناً فرد حاضر در این‌گونه شرایط، رفتارهای معارضی را بروز خواهد داد که متأثر از شرایط نابهنجار خانوادگی‌اش خواهد بود.



### ۴.۲.۳ همسالان معارض

گروه همسالان از دیگر نهادهای مرتبط با دنیای شخصی افراد می‌باشد که در رشد شخصیتی کودکان اهمیت بسیاری دارد. چرا که کودکان در میان همسالان خود احساس امنیت می‌کنند، برای رفتارهای خود هنجار مناسب می‌یابند و فهم و درک خود را شکل می‌دهند، مهارت بدنی - اجتماعی مناسب را کسب می‌کنند و انگیزه مشارکت و همیاری با دیگران را در خود می‌پروراند. طبق نظریه معاشرت ترجیحی ساترلند، افراد در معاشرت با دوستان و آشنایان و بخصوص کسانی که برای او اهمیت ویژه‌ای دارند، یکسری اقدامات را فرا می‌گیرد و با تجزیه و تحلیل آنها سعی در تقلید و الگوگیری از آنها می‌نماید. بنابراین، نوع گروه همسالانی که در آن، شخص عضویت دارد و ارزش‌ها و رفتارهای حاکم بر آن گروه، تأثیر مهمی در افکار اعضای آن گروه دارد. تا جایی که کودکان و نوجوانان با فراگیری آموزش‌های مخصوص ارتکاب جرم به خصوص جرایم سایبری که نیازمند تخصص برای ارتکاب می‌باشد، پس مرتکب این چنین جرایم می‌گردند. برای مثال در یک گروه که به ارتکاب جرم نشر سی‌دی‌های حاوی محتوای مبتذل مشغول می‌باشند این بسیار امر عادی می‌باشد. بنابراین، افراد با عضویت در این گروه‌ها الگوبرداری می‌کنند و مرتکب آن جرم می‌شوند حتی اگر نفعی برای آنها نداشته باشد.

### ۴ نقش بزه دیده سایبری

در علم جرم‌شناسی بزه‌دیده از دو منظر مورد مطالعه قرار می‌گیرد: ۱- بزه‌دیده‌شناسی اولیه ۲- بزه‌دیده‌شناسی ثانویه. در بزه‌دیده‌شناسی اولیه به بررسی نقش بزه‌دیده، در ارتکاب جرم پرداخته می‌شود. به عبارت دیگر در این نوع فرد بزه‌دیده، خود عاملی برای ارتکاب بزه محسوب می‌گردد. ولی در ثانویه فرد بزه‌دیده به عنوان شخصی می‌باشد که متحمل آسیب‌ها و خسارات مادی و معنوی و عاطفی شده است که سعی در جبران آنها شده است [۸]. فون هانتینگ در سال ۱۹۴۸ با انتشار کتاب «مجرم و قربانی او» بزه‌دیده‌شناسی علمی را پایه‌گذاری کرد و با ارائه سه مفهوم بزه‌کار، قربانی، بزه‌دیدگی مخفی و ارتباط خاص میان بزه‌کار و بزه‌دیده به بررسی تأثیر و نقش بزه‌دیده در ارتکاب جرم می‌پردازد [۷]. در ارتباط با جرایم سایبری نیز نقش بزه‌دیده اهمیت بسیار زیادی دارد و انکارناپذیر است. برای مثال: فردی که از ایمیل خود به‌طور کامل خارج نمی‌شود و امکان دستیابی دیگران به داده‌های شخصی‌اش را با این کار فراهم می‌کند. با اینکه اطلاعات شخصی خود را از طریق فیس‌بوک یا سایر شبکه‌های اجتماعی و حتی چت در اختیار دیگران می‌گذارد و حتی اینکه کامپیوتر شخصی خود را جهت تعمیر به افراد غیرمطمئن می‌سپارد، همه اینها می‌تواند فرد را به‌منزله یک طعمه در اختیار افراد سودجو قرار بدهد. جاذبه فضای سایبر خصایص و ویژگی فضای سایبری می‌تواند بر روی گرایش افراد به ارتکاب بزه بسیار تأثیرگذار باشد. ویژگی‌هایی نظیر تسهیل دسترسی به آخرین اطلاعات، گستره جهانی داشتن فضای سایبر، ریسک پایین دستگیری، ماهیت متفاوت جرایم سایبری جاذبه محتویات فضای اینترنت و آزادی اطلاعات و ارتباطات و خاص بودن بزه‌دیده سایبری، عدم نیاز به ارتباط نزدیک و فیزیکی با مجنی علیه، پراکندگی مجنی علیه سایبری و عدم کشف بسیاری از جرایم علیه افراد در عالم واقعی همگی می‌توانند دست به دست هم داده و ارتکاب افراد به‌سوی رفتار خلاف هنجار را تحریک

کنند. علاوه بر این موارد به این نکته نیز باید اشاره کرد که استفاده از سیستم‌های رایانه‌ای همانند گذشته در انحصار اقشار محدودی نمی‌باشد و چون فراگیر و دارای امکانات بی‌شماری است معمولاً گروه‌های جوان بیش از سایر اقشار در آن جذب می‌شوند. این در حالی است که تدوین‌کنندگان تدابیر پیش‌گیرانه اجتماعی با فضای مجازی رابطه عمیقی ندارند یا نمی‌توانند به اندازه جوانان و نوجوانان به فعالیت‌های شبکه‌ای بپردازند. این شکاف دیجیتال میان متولیان پیشگیری و بزه‌کاران و بزه‌دیدگان باید برطرف شود زیرا در غیر این صورت، به دلیل عدم درک متقابل نمی‌توان به تأثیرگذار بودن تدابیر پیش‌گیرانه امیدوار بود [۲].

## ۵ نتیجه‌گیری

جرائم رایانه‌ای به مثابه پدیده‌ای شگفت‌انگیز که با تولد آن تحولی شگرف در زندگی انسان‌ها پدید آمده است، گرچه برخی از جرائم آن شباهت‌هایی با جرائم سنتی دارد، اما تفاوت‌هایی در روش و ماهیت و نوع جرم دارد که از لحاظ جرم‌شناسی و کیفرشناسی و حقوق کیفری پژوهش‌های نو را می‌طلبد. یعنی می‌توان گفت که باتوجه به پیشرفت روزافزون زوایای مختلف این فضا و کارکردهای متنوع آن، شرایط هر روز فضا را برای ارتکاب اعمال مجرمانه نیز باز می‌کند؛ یعنی این فضا ضمن بر جای گذاشتن آثار مطلوب و توسعه خدمات به عموم مردم ولی از طرفی نیز می‌تواند زمینه بر جای گذاشتن آثار نامطلوب را نیز فراهم آورد. بدین ترتیب، به یقین می‌توان گفت حذف کامل این فضای فناوری ارتباطات و اطلاعات از صحنه زندگی انسان‌ها امکان ندارد ولی از طرفی هم منزه کردن این فضا از لوٹ وجود مجرمین هرگز ممکن نیست پس تنها راه حل این است که جامعه بشری را از ابتدایی‌ترین اقدام یعنی شناسایی علل بروز جرائم تا مکانیزم‌های حاکم بر فضا آگاه و سیر ارتکاب جرائم سایبری را مسدود کنیم. در این راستا اتخاذ تدابیر پیشگیرانه به شرحی که در بخش سوم رفت، بسیار ضروری است. واقعیت این است که مبارزه و کشف این‌گونه جرائم کاری بس دشوار است، چرا که به واسطه ویژگی‌های فضای مجازی که ظرفیت سوء استفاده از آن را بالا می‌برد، ویژگی‌هایی چون بدون مرز بودن فضای مجازی، کم‌هزینه‌گی و پرتیری و پایین بودن احتمال دستگیری یا مجازات، امکان وارد آوردن خسارات بالا بدون آسیب جسمانی مجرم، آسان بودن تهیه و امکانات و عوامل مورد نیاز جرم، بازتاب جهانی موفقیت، امکان جذب حامی و همکار برای ارتکاب جرم از سراسر جهان بدون حضور فیزیکی، امکان جذب منابع مالی و پول‌شویی آسان تر و هرگونه انجام فعالیت‌های مالی الکترونیکی در جهت اهداف مجرمانه با توجه به پیچیدگی جرائم رایانه‌ای، مطالعه و پژوهش بیشتر و نیز تصویب قوانین مورد نیاز در این زمینه بسیار ضروری است.

پیشنهادها: در حال حاضر با عنایت به پیشرفت‌های لحظه‌ای در عرصه رایانه و فضای سایبر ضرورت آموزش بیش از پیش مشخص شده و برای اجرای یک سیاست کیفری مؤثر جهت پیشگیری از جرائم رایانه‌ای به خصوص جاسوسی رایانه‌ای و اینترنتی، این آموزش‌ها باید در مقاطع مختلف زمانی تکرار و روزآمد شوند. ۱- از آنجاکه پلیس به عنوان ضابط دادگستری وظیفه کشف جرائم را بر عهده دارد، در کنار آموزش قضات و سایر مقدمات قضایی، آموزش پلیس نیز باید در سرفصل برنامه‌ریزی‌ها قرار گیرد، چون تعقیب و پیشگیری از جرائم سایبری مستلزم تربیت نیروهای متخصص می‌باشد. البته این توانایی را هم بایستی داشته باشند

که خود را به طور مستمر به روز نگه دارند و گرنه نمی‌توان با این جرایم مقابله کرد. ۲- آموزش‌های عمومی در سطح کارمندان دولت و نظامیان و همچنین مقامات قضایی؛ زیرا آنان برای یک قضاوت صحیح نیاز دارند که شناخت نسبی از ماهیت این فضا و نوع جرایم داشته باشند و برگزاری کلاس‌های تخصصی شدن محاکم این دسته از جرایم توصیه می‌گردد. ۳- تا حد ممکن عدم ذخیره‌سازی داده‌ها و اطلاعات طبقه‌بندی شده به شبکه‌های رایانه ای به خصوص شبکه جهانی اینترنت. ۴- مسدود کردن درگاه‌های رایانه‌های حساس در ادارات به عنوان راهکاری سریع و کم‌هزینه و در عین حال مؤثر؛ در این روش تمامی درگاه‌های سیستم‌های رایانه‌ای از قبیل درایو، CD پورت‌های USB و ... از طریق سرور (شبکه) بسته شده و به این ترتیب کاربر رایانه نمی‌تواند هیچ داده و اطلاعاتی را وارد رایانه کرده و یا از آن خارج کند. در این حالت کاربر تنها به داده‌های مجازی که از سوی مسئولان و به منظور انجام وظیفه روی سیستم او قرار داده شده است، دسترسی خواهد داشت.

## مراجع

- [۱] ابراهیمی، شهرام، جرم شناسی پیشگیری، ۱۳۹۰، جلد اول، چاپ اول، تهران، نشر میزان.
- [۲] جلالی فراهانی، امیرحسین و باقری اصل، رضا. پیش‌گیری اجتماعی از جرایم و انحرافات سایبری، ۱۳۸۶، مجله مجلس و پژوهش، شماره ۵۵.
- [۳] عالی‌پور، حسن، حقوق کیفری فناوری اطلاعات، ۱۳۹۰، چاپ اول، تهران، انتشارات خرسندی.
- [۴] فضل‌ی، مهدی، مسئولیت کیفری در فضای سایبر، ۱۳۸۹، چاپ اول، تهران، انتشارات خرسندی.
- [۵] قاسمی روشن، ابراهیم، عوامل اجتماعی و جرم، ۱۳۷۹، ماهنامه معرفت، شماره ۳۶.
- [۶] کی‌نیا، مهدی، مبانی جرم‌شناسی، ۱۳۸۶، جلد اول، چاپ هشتم، تهران، نشر دانشگاه تهران.
- [۷] مال‌میر، محمود و زرخ، احسان، پیشگیری از بزه‌دیدگی سایبری، ۱۳۸۹، فصلنامه مطالعات پیشگیری از جرم، شماره هفدهم.
- [۸] نجفی ابرندآبادی، علی حسین، تقریرات بزه‌دیده‌شناسی، ۱۳۷۴، تنظیم فاطمه قناد، دوره کارشناسی دانشگاه شهید بهشتی.
- [9] V. Shiva Kumar, Cyber Crime: prevention and detection, Asset, Director. A.P. Police Academy, 2008.
- [10] Michael Kunz and Patrick Wilson, computer crime and computer fraud, university of Maryland Department of criminology and criminal justice, 2004.
- [11] Marc D. Goodman and Susan W. Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, I law info tech, 2010.
- [12] Ales Zavrsnik, Cybercrime Definitional Challenge and Criminological Particularities Masaryk, University journal of law and technology, 2008.



## شبکه‌های اجتماعی مجازی و کنش سیاسی

حمزه عالمی چراغعلی<sup>۱</sup>

استادیار اندیشه سیاسی، مجتمع آموزش عالی شهید محلاتی، قم، ایران  
hz.alemi@gmail.com

### چکیده

این پژوهش رابطه بین شبکه‌های اجتماعی مجازی و کنش سیاسی را با رویکرد کیفی و روش توصیفی - تبیینی بررسی می‌کند. در این پژوهش، نظریات مختلف درباره‌ی کارکردها و ویژگی‌های فضای مجازی به صورت عام و شبکه‌های اجتماعی مجازی به صورت خاص، بررسی شده است. ماحصل این دیدگاه‌ها درباره چگونگی رفتار فرد در فضای مجازی و شبکه‌های اجتماعی مجازی می‌گوید: شبکه‌های اجتماعی مجازی سبب به وجود آمدن گرایش‌های مقاومت افراد در قبال الگوهای سیاسی، اجتماعی و فرهنگی رسمی که میل به تحمیل اراده بر فرد دارند، می‌شود. در مرحله بعد با مطالعه الزامات کنش سیاسی از دیدگاه ژولین فروند، این موضوع بررسی شد که تقویت گرایش‌های مقاومت افراد توسط شبکه‌های مجازی، چه رابطه‌ای با کنش سیاسی آن‌ها دارد؟ آیا شبکه‌های اجتماعی مجازی سبب تقویت کنش سیاسی افراد می‌شوند؟ نتایج حاصل، بیان‌گر این است که: شبکه‌های اجتماعی مجازی کمتر رابطه مثبت با کنش سیاسی دارند. این شبکه‌ها نقش یاری‌دهنده‌ی زیادی در کنش سیاسی ندارند و اتفاقاً هر اندازه کنش سیاسی از حوزه واقعیت به فضای مجازی بیشتر روی آورد، با موانع بیشتری در رسیدن به موفقیت مواجه می‌شود.

**کلمات کلیدی:** فضای مجازی، شبکه‌های اجتماعی مجازی، کنش سیاسی.

### ۱ مقدمه

ظهور و گسترش فناوری‌های اطلاعات و ارتباطات، دوران کنونی را با تغییرات سریع و بنیادین مواجه کرده است. در دوران کنونی فناوری اطلاعات سبب گسترش منطق شبکه‌سازی در همه انواع فرایندها و سازمان‌ها شده و در همین جهت شبکه‌های اجتماعی مجازی به نماد حضور انسان در زندگی مجازی (زندگی دوم) تبدیل شده‌اند. این زندگی مجازی برساخته بشر نمی‌تواند از زندگی واقعی او مجزا باشد و برخی ویژگی‌های زندگی واقعی انسان، در حوزه مجازی رخ می‌نماید و در گام بعد از این حوزه به زندگی واقعی وارد می‌شود. بنابراین می‌توان تأثیر این شبکه‌ها را در حوزه‌های مختلف زندگی واقعی از جمله حوزه سیاست جستجو کرد. در این جهت پژوهش حاضر این سؤال اصلی را دنبال می‌کند که: چه رابطه‌ای بین شبکه‌های اجتماعی

مجازی و کنش سیاسی وجود دارد؟ و آیا شبکه‌های اجتماعی مجازی سبب تقویت کنش سیاسی می‌شوند؟ پاسخ اولیه عبارت است از این‌که:

الف) بین شبکه‌های اجتماعی مجازی و کنش سیاسی رابطه مثبت وجود دارد.

ب) شبکه‌های اجتماعی مجازی سبب تقویت کنش‌های سیاسی افراد می‌شوند.

## ۲ مروری بر پژوهش‌های موجود

بسیاری از پژوهش‌های انجام شده در محدوده‌ی این موضوع، اغلب با رویکردی کمی و روش‌های پیمایشی، شبکه‌های اجتماعی مجازی را عامل مؤثر و مفیدی در حوزه سیاست دانسته‌اند، شهرام‌نیا و دیگران در مقاله «سنجش تأثیر شبکه‌های اجتماعی بر مشارکت سیاسی: مطالعه‌ی موردی دانشجویان دانشگاه مازندران» [۱]، رابطه میان شبکه‌های اجتماعی مجازی و مشارکت سیاسی را مثبت دانسته‌اند. محموداوغلی در مقاله «بررسی تأثیرات شبکه‌های اجتماعی بر کنشگری سیاسی دانشجویان دانشگاه اصفهان» [۲] تأثیر این شبکه‌ها بر کنش سیاسی را تقویت کننده و در دو جهت کنش‌های سازنده و نامتعارف می‌داند. نوری و قلی پور در مقاله «رسانه‌های جدید و کنش جمعی در جامعه سیاسی ایران» نیز گسترش شبکه‌های اجتماعی را مساوی با گسترش کنش‌های جمعی در جامعه ایران دانسته و میان این دو رابطه‌ای مثبت می‌بینند [۳]. در مقابل این پژوهش‌ها، مقاله پیش‌رو با اولویت دادن مبانی نظری بر موارد عینی، بررسی هویت و چیستی دو متغیر شبکه‌های اجتماعی مجازی و کنش سیاسی را مقدم بر بررسی کارکردی این دو می‌داند و از این منظر متمایز از پژوهش‌های انجام شده خواهد بود. در این میان مقاله «واکاوی امر سیاسی در فضای مجازی از منظری آرتی» با رویکردی نظری و کیفی معتقد است شبکه‌های اجتماعی مجازی کمکی به دموکراسی و تقویت کنش سیاسی در عرصه عمومی نمی‌کنند، این مقاله که امر سیاسی را از منظر هانا آرتت بررسی کرده است [۴]، هرچند با مقاله پیش‌رو رویکردی همسو دارد، اما در مقاله حاضر کنش سیاسی به‌صورت دقیق‌تر و با شاخص‌های واضح‌تری بر مبنای دیدگاه ژولین فروند تعریف شده است و از این رو رابطه شبکه‌های اجتماعی مجازی با کنش سیاسی را واضح‌تر تبیین می‌کند.

## ۳ ویژگی‌های بنیادین شبکه‌های ارتباطی مجازی

مطالعه شبکه‌های اجتماعی مجازی فارغ از ویژگی‌ها و کارکردهای فنی آن‌ها نشان می‌دهد که این شکل از فناوری معانی و ویژگی‌های فرهنگی خاصی را منتشر می‌کند. دیوید بل می‌گوید فضای سایبر به‌طور هم‌زمان هم محصول فرهنگ و هم تولیدکننده فرهنگ است [۵]. بسیاری از پژوهشگران این حوزه، ویژگی‌های شبکه‌های مجازی را در دو دسته ویژگی‌های مثبت و منفی تقسیم بندی کرده‌اند که به اختصار در جدول شماره ۱ می‌آید.



جدول ۱: ویژگی‌های مثبت و منفی شبکه‌های اجتماعی مجازی

جنس ویژگی	نوع ویژگی	متفکران و پژوهش‌های طرفدار آن
ویژگی‌های مثبت	تکثر اطلاعات و تضارب آراء	جیمز اسلوین [۶] / مائورا کانوی [۷] / دانا بوید [۸]
	رهایی از سیطره قدرت رسمی	لویسون [۹] / مائورا کانوی [۱۰] / هربرت شیلر و یورگن هابرماس [۱۱] / تامسون [۱۲] / ماریا باکارجیوا [۱۳] / آنتونی گیدنز [۱۴] / بروس بیمبر [۱۵] / اتلینگ، فاریس و پالفری [۱۶]
	سرعت بالا و سهولت در انتقال اطلاعات	فرانسیسکا پولتا [۱۷] / سعیدرضا عاملی [۱۸] / ایمانوئل کاستلز [۱۹] / هیوبرت دریفوس [۲۰]
	فرصت بروز علایق شخصی	جیمز اسلوین [۲۱] / دانا بوید [۸]
ویژگی‌های منفی	فاصله‌گیری از فضای واقعی	شری ترکل [۲۲] / هوارد رین گلد [۲۳]
	دگرگشت ارتباطات واقعی	شری ترکل [۲۴] / زیگموند باومن [۲۵] / هیوبرت دریفوس [۲۶]
	عدم تمرکز و بی‌نظمی	یورگن هابرماس [۲۷] / گلدستین و روتیج [۲۸] / نیکلاس کار [۲۹] / جیمز روزنا [۳۰] / مارک پاستر [۳۱] / ایمانوئل کاستلز [۳۲] / گیدنز [۳۳]
	ایجاد هویت منعطف و سیال	هیوبرت دریفوس [۳۴] / چانگ تزو [۳۵] / دیوید بل [۳۶] / شری ترکل [۲۴] / نورمحمدی [۳۷]

از مطالعه ویژگی‌های شبکه‌های اجتماعی مجازی این جمع‌بندی حاصل می‌شود: «شبکه‌های اجتماعی مجازی و محیطی است که با افزایش آگاهی و فراهم‌سازی زمینه طرح علایق شخصی، سبب به‌وجود آمدن گرایش‌های مقاومت افراد در قبال الگوهای سیاسی، اجتماعی و فرهنگی رسمی که میل به تحمیل اراده بر فرد دارند، می‌شود. فرد در این شبکه‌ها می‌خواهد اجباری که در واقعیت از سوی حکومت یا عرف بر او می‌شود را بشکند و نیروی خود را آزاد کند و نیازهایی که در واقعیت به‌سبب سلطه حکومت و عرف به آن‌ها نرسیده را در فضای مجازی دنبال کند، اما تکثرگرایی و بی‌نظمی در فضای مجازی، تحول زمان و مکان، وجود هویت‌های سیال و دگرگشت روابط انسانی، بین او واقعیات جدایی ایجاد می‌کند.» با شناخت ابعاد کنش سیاسی بیشتر این سؤال شکل می‌گیرد که ایجاد گرایش‌های مقاومت در افراد از یک سو و از سوی دیگر شکاف بین فضای مجازی و واقعی چه تأثیراتی بر کنش سیاسی افراد در واقعیت دارد؟

## ۴ کنش سیاسی

کنش مفهومی است که ابتدا از سوی جامعه‌شناسان طرح شد و جایگاه مهمی در آراء ماکس وبر، امیل دورکیم و تالکوت پارسونز دارد. کنش از نظر ماکس وبر جهت‌گیری رفتاری قابل درک ذهنی است [۳۸]. در نظر او نوع کنش یک فرد را ساختار اجتماعی تعیین می‌کند. در مقابل دورکیم بر وجه تعیین‌کنندگی ساختار اجتماعی تأکید دارد و در موضعی میانه، پارسونز این دو عامل را با یکدیگر در نظر می‌گیرد. به عقیده پارسونز کنش‌گر با داشتن معانی و ارزش‌ها به-هنگام انتخاب هدف تحت «شرایط و وضعیت» اجتماع قرار دارد و این شرایط و وضعیت اجازه نمی‌دهد که کنش‌گر هرگونه که تمایل دارد، تصمیم بگیرد [۳۹].

در میان اندیشمندان سیاسی، هانا آرنت به مسئله کنش سیاسی پرداخته است. آرنت با تقسیم زندگی عمل‌ورزانه قرون وسطی به سه مقوله «زحمت»، «کار» و «عمل»، سیاست را در حوزه عمل انسان تعریف می‌کند. او عمل سیاسی (کنش سیاسی) را عالی‌ترین وجه رفتار انسانی می‌داند. در حالی که زحمت برای رفع نیازهای مادی و بیولوژیکی و کار برای ساختن جهانی آباد است، عمل برای ساختن جهانی آزاد است [۴۰].

در این میان ژولین فروند از جمله متفکران علم سیاست است که تلاش کرده فهم نسبتاً روشنی از امر سیاسی، عمل سیاسی، هدف‌ها و وسیله‌های ویژه امر سیاسی ارائه کند. در کتاب وی با عنوان سیاست چیست؟ [۴۰] می‌توان معنای کنش سیاسی و ابعاد آن را یافت. در اینجا با ملاک قرار دادن دیدگاه فروند، به چستی کنش سیاسی و الزامات ویژه آن می‌پردازیم.

فروند سعی می‌کند چگونگی حرکت گام‌به‌گام فرد در عرصه سیاسی برای رسیدن به اهداف خود را ترسیم کند. او سیاست را جزء فعالیت‌های بنیادین بشر می‌داند که بر داده بنیادین جامعه یا زندگی اجتماعی استوار است. کنش سیاسی در نظر فروند ترکیبی از تصمیم برخاسته از انگیزه و آگاهی، کاربست هوشمندانه وسیله‌ها و پیش‌بینی نتیجه‌هاست. وی در تشریح عمل، وسیله‌ها و اهداف سیاسی، همواره نگاه به محیط اجتماعی دارد. از مجموع مباحث فروند درباره کنش سیاسی این تعریف حاصل می‌شود: «تصمیم و اراده خودآگاه، هوشمندانه و شجاعانه فرد یا گروهی از افراد که با در نظر گرفتن شرایط اجتماعی، برای پیروزی در عرصه سیاسی با شجاعتی هوشمند، امکانات لازم را با پیش‌بینی نتیجه‌های احتمالی در جهت رسیدن به هدف سیاسی مشخص به کار می‌گیرند.» ژولین فروند در هر یک از مراحل سه‌گانه کنش سیاسی یعنی تصمیم آگاهانه، کاربست هوشمندانه وسیله‌ها و پیش‌بینی نتیجه‌ها، لوازم و بایسته‌هایی را برای موفقیت کنش‌گر سیاسی تجویز می‌کند. با توجه به این بایسته‌ها - که نوعی برنامه عملی موفقیت در طی مسیر کنش سیاسی است - به بررسی رابطه نتایج حاصل از رفتار فرد در شبکه‌های اجتماعی مجازی با کنش سیاسی می‌پردازیم.

## ۵ رابطه شبکه‌های اجتماعی مجازی و کنش سیاسی

### ۱.۵ افزایش آگاهی در محیط مجازی و کنش سیاسی

علاوه بر این که در همان مشاهدات اولیه در اینترنت و شبکه‌های اجتماعی مجازی این موضوع قابل تأیید است، گفته شد که محققینی همچون دانا بوید، جیمز اسلوین، تامسون و بندیکت نیز به آن اشاره کرده‌اند. در عین حال این افزایش آگاهی و شناخت در شبکه‌های اجتماعی مجازی به اعتقاد برخی نظریه‌پردازان، قابل اعتماد نیست. استفاده روزنا از نظریه «چگالی اجتماعی» در توضیح «اندیشه‌های انتزاعی و نسبی‌گرایی فرد در فضای مجازی»، نظریه نیکلاس کار در مورد «جابجایی مدام ذهن در اینترنت» و تأثیر آن بر عدم تمرکز فکری و استدلال دریفوس در ناکارآمدی آموزش مجازی از راه دور توسط اینترنت، گویای این است که آگاهی و شناخت برآمده از اینترنت و شبکه‌های اجتماعی مجازی، متزلزل، سطحی و متکثر است. این نوع آگاهی در معرض تغییر و بی‌ثباتی است. در حالی که کنش سیاسی در نظر فروند، نیازمند آگاهی و شناخت منسجم و هوشمندی کنش‌گر در تمامی مراحل تصمیم‌گیری، کاربست وسیله‌ها و پیش‌بینی نتیجه‌هاست. کنش اولین

مواجه آگاهانه و هوشمندانه فرد با وسیله‌های موجود، انتخاب هوشمندانه وسیله‌ها، سازماندهی خردمندانه و کاربست روشن‌بینانه آن‌ها برای رسیدن به اهداف سیاسی است [۴۱]. حال آن‌که به اعتقاد ترکل محیط مجازی منجر به سرگردانی افراد در محیط واقعی می‌شود [۴۲].

فرد نمی‌تواند بدون شناخت واقعیت‌های اجتماعی کنش‌گری موفق باشد. به اعتقاد فروند ارجاع به اجتماع برای هر تصمیم سیاسی تعیین‌کننده است [۴۳] و دریفوس می‌گوید آگاهی از واقعیات وابسته به جسم است و بدن منبع درک ما از واقعیات است، اما در فضای مجازی عدم حضور بدن منجر به نبود درک از واقعیت آدم‌ها و اشیاء می‌شود [۴۴]. ترکل نیز معتقد است فضای مجازی و شبکه‌های اجتماعی مجازی برای این‌که واقعا یکدیگر را بشناسیم و درک کنیم، کارآیی ندارند [۴۵].

بعد از مرحله تصمیم‌گیری، کنش نیازمند میانجی رسیدن به هدف است و وسیله‌ها نقش میانجی را ایفا می‌کنند. وسیله‌ها منابع مادی گذر از طرح به اجرا را تعریف می‌کنند. در این مرحله نیز به‌کارگیری وسیله‌ها برای پیشبرد کنش و رسیدن به هدف نیازمند هوشمندی، نرمش، تجربه و شم پیش‌بینی رویدادها است. روش کاربست وسیله‌ها باید همراه با بازاندیشی و صرفه‌جویی در مصرف منابع باشد و کورکورانه از آنچه دیگران دنبال کرده‌اند پیروی نشود. عدم بازاندیشی در روش استفاده از وسیله‌ها، سبب می‌شود تا فرد همواره آن روش را کارآمد بداند و در نتیجه دچار جزم‌اندیشی شده و در این وضعیت آن روش خود به هدف تبدیل می‌شود. نتیجه این‌که دستیابی به اهداف صورت نمی‌گیرد، در حالی‌که به گفته فروند، وسیله‌ها تنها برای رسیدن به هدف معنادار می‌شوند [۴۶].

فضای مجازی امکان بازاندیشی در مصرف منابع را با مشکل مواجه می‌کند. عدم تاریخ‌نگاری در فضای مجازی زمینه بازخوانی اقدامات گذشته و برنامه‌ریزی بر مبنای تجربه را فراهم نمی‌کند. اسلوین تأیید می‌کند که اینترنت سبب متلاشی‌شدن تجربه می‌شود [۴۷]. کنش سیاسی در شبکه‌های اجتماعی مجازی کمتر وابسته به تجربیات تاریخی است.

پیش‌بینی و ارزیابی نتیجه‌ها نیز مستلزم آگاهی و هوشمندی است. مسئله نتیجه‌ها در کانون کنش جای دارد. برخی از آن‌ها قابل پیش‌بینی هستند و برخی دیگر به‌شکلی غیرقابل پیش‌بینی در هنگام کنش و عمل رخ می‌دهند. برای آن‌دسته از نتیجه‌های قابل پیش‌بینی باید با محاسبه خردمندانه، سرشت آماج مورد نظر، داده‌های آغاز راه، وسیله‌های در دسترس، واکنش‌های احتمالی حریف، در صورت لزوم درجه‌بندی وسیله‌ها، در هم‌کوفتن پایداری‌ها و هم‌چنین وضع روحی، هوشمندی و سازماندهی همکاران و سرانجام وضعیت نوینی که دست‌آورد کار ایجاد می‌کند را پیش‌بینی کرد. اما به‌هنگام رخ‌دادن یک نتیجه غیرقابل پیش‌بینی باید از چنان ابتکار عملی برخوردار بود که بتوان چالاک‌تر از حریف با آن رویارو شد و از آن بهره‌برداری نمود [۴۸].

قابلیت پیش‌بینی در شبکه‌های اجتماعی مجازی نیز به سبب فاصله فضای مجازی از فضای واقعی، آمیخته با تخیلات خواهد بود. کشیده‌شدن دامنه تفکرات در فضای مجازی به موضوع رهاسازی بدن گوشتی و امکان سیر بدون جسم در این محیط، نشانه‌هایی از تخیلات فرد در محیط مجازی است. خودبازنمایی فرد در فضای مجازی، یعنی نشان دادن غیرواقعی خود در این محیط، که ترکل به آن اشاره می‌کند، نشانه‌ای از رفتار خیال‌گونه فرد در محیط مجازی است. عرصه واقعی سیاست، ساختارهای قدرتمند پنهان، اما اثرگذاری دارد که خیال‌پردازی در محیط مجازی مانع محاسبه آن‌ها می‌شود. در این شرایط کنش سیاسی افراد محدود

به رفتارهای مقطعی و هیجانی شده و همچنان که فرزند می‌گوید به رمانتیک عمل برای عمل فرو می‌غلطد و دوام زیادی نخواهد آورد.

## ۲.۵ تکثرگرایی و بی‌نظمی و کنش سیاسی

تکثرگرایی فرد و بی‌نظمی رفتار فرد در محیط مجازی و بازتاب آن در رفتار واقعی، مورد تأیید برخی از نظریه‌پردازان است. دیدگاه روتیچ گلدشتاین درباره تأثیر شبکه‌های مجازی بر افزایش انشعابات داخلی یک گروه، عدم کارایی این شبکه‌ها در شکل‌دادن به توافق عمومی از نظر مارک پاستر، اشاره به بی‌نظمی‌های نوین به‌عنوان پیامد رسانه‌های ارتباطی جدید توسط کاستلز، اعتقاد گیدنز به افزایش بی‌نظمی به‌عنوان پیامد استفاده از رسانه‌های جدید و نتیجه‌گیری هابرماس از تحول زمان و مکان توسط رسانه‌های جدید و تأثیر آن بر ایجاد بی‌نظمی، از جمله این نظریات هستند که پیش‌تر مطالعه شد.

تکثرگرایی و بی‌نظمی موجود در فضای مجازی در مقابل نظم به‌عنوان الزامی ویژه در کنش سیاسی، قرار می‌گیرند. نظم و ترتیب وسیله‌ها و اولویت‌بندی آن‌ها و نیز اولویت‌بندی مسائل پیش‌رو در کنش سیاسی مقولاتی ضروری است. نظم سبب تمایزگذاری و اولویت‌بندی وسیله‌ها و مسائل شده و پیش‌بینی را عینیت می‌بخشد، حصول نتیجه‌ها از این راه ممکن است [۴۹]، تمایزگذاری و گزینش، الزام دیگری در کنش سیاسی است که در تقابل با تکثرگرایی فضای مجازی قرار دارد. در کنش سیاسی، تصمیم با توسل به گزینش، امکان‌ها را محدود می‌کند. به اعتقاد فروند، تصمیم‌گیری به‌معنای گسست با رایزنی است، زیرا در نبود تصمیم، رایزنی را پایانی نیست. تصمیم‌گیری لحظه‌ای است که تردیدها را کنار می‌گذارد و در بین امکان‌های گوناگون، برخی را گزینش می‌کند [۵۰]. بنابراین در وضعیت متکثر و تأیید تمام امکان‌ها، بدون ترجیح یکی بر دیگری، تصمیمی گرفته نمی‌شود و کنشی ایجاد نمی‌گردد. در حالی که به‌گفته دریفوس اینترنت نقطه‌نهایی این گرایش است که هر چیزی را تا حد ممکن انعطاف‌پذیر کنیم و هر قدر از واقعیت را که می‌توانیم دیجیتال نمائیم و به هم پیوند دهیم [۵۱].

بی‌نظمی و تکثرگرایی فضای مجازی، خود ریشه در تحول مفهوم زمان و مکان در عصر اطلاعات و ارتباطات دارد. زمان و مکان موجود در شبکه‌های اجتماعی مجازی، تحت تحولات فناوری ارتباطات و اطلاعات، از معنای واقعی خود خارج شده و حاصل آن زمان بی‌زمان و مکان بی‌مکان است. در حالی که زیست - جهان انسان اجتماعی از زمان خلقت آدمی به شدت مقید به زمان و مکان بوده و ساختار فضا - زمانی، زندگی اجتماعی، چگونگی کنش اجتماعی و روابط اجتماعی فرد را مشخص می‌کند [۵۲]. سیاست همانند دیگر مناسبات اجتماعی در فضا آشکار می‌شود. اندیشیدن درباره سیاست و قدرت تقریباً همواره با فراخواندن مجموعه‌ای از مناسبات فضایی همراه است. این فضاهای واقعی نمودار قدرت اجتماعی و مکانی برای رویدادهای سیاسی و سازنده موضوعات کنش سیاسی هستند [۵۳]. و قدرت سیاسی در فضای واقعی که اشغال می‌کند بازنمایی می‌شود [۵۴]. همچنین مقوله تمایزات مکانی و بار عاطفی مترتب بر آن‌ها به رفتار سیاسی کنشگران عرصه سیاست عمق و گستره خاص می‌بخشد. برخی مکان‌ها کارکرد راهبردی دارند و به کار ویژه جریان‌های سیاسی ماهیت ملی و بین‌المللی می‌بخشند. به طوری که برداشت دیگر ملل درباره کشور خاص تابعی از بروز رفتار سیاسی در فلان مکان خاص است [۵۵].

با این توضیح می‌توان گفت در کنش سیاسی، زمان و مکان در خدمت نوع کنش، انگیزه و اهداف بازیگران آن است. در مقابل زمان بی‌زمان و مکان بی‌مکان محیط مجازی، می‌تواند برساخته کاربران باشد و از این رو متکثر، مبهم و ناپایدار است. همچنین تکثرگرایی فرد در محیط مجازی و بی‌نظمی مؤثر بر وی در این محیط، توافق و همبستگی لازم در کنش سیاسی را با مشکل مواجه می‌کند. روتیج گلدشتاین و مارک پاستر مستقیماً به این موضوع اشاره می‌کنند. ژولین فروند کنش سیاسی را مستلزم سازش و تصمیم قاطع می‌داند که گزینش میان این دو به اوضاع و احوال و موقعیت بستگی دارد، اما در عین حال «سازشی ناجورگاه بهتر از تصمیمی ناشیانه و خشک است.» به گفته فروند در مرحله تصمیم‌گیری و گزینش وسیله‌ها، از آنجا که بخش مهمی از گزینه‌های سیاسی نامعلوم و مبهم است، بهترین راه، سازش است، چرا که زندگی مشترک بدون توافق دوستانه، بدون قراردادها، بدون آشتی‌ها و بدون امتیازدهی دو جانبه، امکان‌ناپذیر است [۵۶].

علاوه بر این تکثرگرایی موجود در فضای مجازی و بی‌نظمی برخاسته از آن سبب از بین رفتن منابع کنش سیاسی می‌شود. به اعتقاد ترکل افراد با درگیر شدن در فضای مجازی، از سیاست در زندگی واقعی دور افتاده‌اند [۵۷]. هوارد رین‌گلد می‌گوید: طبیعت خالی از خطر فضای مجازی سبب کشیده شدن افراد به آن می‌شود و این‌گونه وقت و انرژی شهروندان را که می‌تواند صرف مسائل جامعه واقعی شود، به تحلیل می‌برد [۵۸]. در مقابل کنش سیاسی نیازمند صرف هوشمندانه سرمایه‌هاست. انگیزه و باور به یک هدف، سرمایه‌های کنش سیاسی هستند. شبکه‌های اجتماعی مجازی این سرمایه‌ها را قبل از این که در خدمت کنش درآیند در خدمت گفتگو و ابراز احساس در درون خود قرار می‌دهند و توشه راه کنش را از بین می‌برند [۵۹].

### ۳.۵ رهایی از سیطره قدرت رسمی و کنش سیاسی

گفته شد که یکی از نتایج مهم فضای مجازی و شبکه‌های اجتماعی مجازی بر رفتار فرد، افزایش مقاومت او در قبال سیاست رسمی کشور که نیل به تحمیل اراده بر فرد دارند، است. در مقابل باید توجه داشت که ساختار متکثر فضای مجازی از میزان مقاومت فرد می‌کاهد. مارک پاستر به دلیل تکرر دیدگاه‌های متفاوت در اینترنت و فضای مجازی، آن را در شکل‌دهی به توافق در حوزه عمومی و در نتیجه نیل به دموکراسی ناکارآمد می‌داند [۶۰]. اس. ادای و همکاران وی معتقدند فضای مجازی و شبکه‌های اجتماعی مجازی فرد را با گفتگو و بحث در محیط مجازی سرگرم می‌کنند و بازیگران یک کنش سیاسی را از فعالیت‌های سیاسی خلاق باز می‌دارد، سبب منفعل شدن آنان می‌گردد. با استفاده از شبکه‌های اجتماعی مجازی این امکان به وجود آید که افراد غیرمتعهد تنها با پیوستن به گروه‌های مجازی موجود در فیس‌بوک یا توئیتر، اعتراضات خود را نشان دهند و در عمل تعهدی به حضور جدی در عرصه تظاهرات و اعتراضات خیابانی نداشته باشند [۶۱].

مقاومت سیاسی نیازمند شجاعت در تصمیم‌گیری است. شجاعت عنصر جوهری تصمیم است و تصمیم همانا شجاعت است، چرا که سبب می‌شود تصمیم به سمت هدف‌گیری در جریان افتد و عمل را تا رسیدن به هدف یاری کند. شجاعت سیاسی بر قاطعیت رأیی استوار است که به یاری آن می‌توانیم مسئولیت پیامدهای پیش‌بینی شده و پیش‌بینی نشده عمل سیاسی را بپذیریم. شجاعت به معنای به دست گرفتن سرنوشت است. نشان دادن رفتاری تزلزل‌ناپذیر برگ برنده فوق‌العاده‌ای برای تصمیم‌گیری است، زیرا در اردوی مخالف بی‌تصمیمی و دودلی برمی‌انگیزد. قاطعیت در تصمیم‌گیری سبب غافل‌گیری حریف می‌شود و او را در



وضعیتی فرودست قرار می‌دهد. به گفته توسیدید هراسناک‌ترین چیزها تردید پیاپی در تصمیم‌گیری است. بنابراین شجاعت و قاطعیت از لوازم اصلی تصمیم‌گیری در کنش سیاسی هستند. [۶۲] علاوه بر این شجاعت سبب خطرپذیری شده و غلبه بر موانع می‌شود. تحمل خطر و زیان یکی از ضرورت‌های دیگر رسیدن به پیروزی در کنش سیاسی است، چرا که عرصه سیاسی لاجرم نیازمند نبرد است [۶۳].

فضای مجازی با ساختار متکثر و سرگرم‌سازی افراد نمی‌تواند چنین شجاعت و خطرپذیری را برای نیل به موفقیت در کنش سیاسی فراهم کند. گیدنز معتقد است ارتباطات مجازی بدون خطرپذیری و همراه با احساس امنیت است [۶۴]. و رین‌گلد می‌گوید طبیعت خالی از خطر فضای مجازی سبب کشیده‌شدن افراد به آن می‌شود [۶۵]. بر این اساس حتی می‌توان گفت به نظر می‌رسد کنش‌گران سیاسی اگر بیش از عمل واقعی به عمل مجازی در شبکه‌های اجتماعی روی آورند، همان قاطعیتی که در فرایند کنش کسب کرده‌اند را از دست خواهند داد. محیط و ساختار شبکه‌های اجتماعی مجازی که آمیخته با تکثرگرایی و سرگرم‌سازی است، نقطه مقابل قاطعیت و هوشیاری، یعنی گوهرهای ویژه کنش سیاسی هستند.

#### ۴.۵ هویت در فضای مجازی و کنش سیاسی

فرد در محیط مجازی هویتی منعطف و سیال دارد، ساختار شبکه‌های مجازی با داشتن ویژگی‌هایی همچون انعطاف و تکثرگرایی توانایی کمک به داشتن شخصیت محکم و استواری که کنش سیاسی می‌طلبد را ندارد. دیدگاه‌هایی که درباره رهاسازی بدن گوشتی و امکان سیر در فضای مجازی را دنبال می‌کنند، هرچند هم خیال‌پردازانه باشند، مبتنی بر همین هویت سیال و دیجیتال فرد در محیط مجازی هستند. ترکل، دیوید بل و چان تزو، هر سه به هویت منعطف و دیجیتالی فرد در محیط مجازی اشاره می‌کنند و نگارش کتابی توسط دریفوس در پاسخ به موضوع هوش مصنوعی و دیدگاه‌های رهاسازی بدن در محیط مجازی گویای ویژگی بارز سیالیت هویت در محیط مجازی و آثار آن در درو افتادن فرد از زندگی واقعی است.

در حالی که کنش سیاسی نیازمند هویت باثبات کنش‌گر است؛ شخصیتی که چالش‌های هویتی نداشته باشد و بتواند در لحظات حساس سیاسی، هوشمندی و شجاعت را با هم آمیخته و تصمیم‌های قاطعی بگیرد. عدم تعادل شخصیتی و بی‌هویتی سبب می‌شود تا فرد متزلزل عمل کرده و در مقابل حریف صحنه را ترک کند. همچنین گفته شد از الزامات مهم کنش سیاسی توانایی غلبه بر پایداری‌هایی است که در مسیر آن ایجاد می‌شود. با این توضیح هویت‌های سیال و مبهم در شبکه‌های اجتماعی مجازی اسباب موفقیت کنش سیاسی را چندان برآورده نمی‌کنند. از سوی دیگر بخشی از هویت فرد وابسته به محیط است. هویت مکانی بخشی از زیربنای هویت انسان و برآیند شناخت او درباره جهان (محیط ادراکی و واقعی) است که در آن زندگی می‌کند [۶۶]. در حالی که بی‌مکانی و ابهام در مکان صدور پیام‌ها در شبکه‌های اجتماعی مجازی، در ایجاد یک هویت باثبات برای به سرانجام رساندن کنش سیاسی اختلال ایجاد می‌کند.

برخی پژوهش‌های کمی، شکل‌گیری و رشد هویت‌های قومی در شبکه‌های اجتماعی مجازی را تأیید می‌کنند. بر مبنای یک تحقیق میدانی، شاخص‌های قومی نه تنها در اینترنت روبه زوال نهماده‌اند، بلکه در واقع در سراسر فضای مجازی حاضرند [۶۷]. پژوهش دیگری با مطالعه کیفی وب‌سایت‌ها، وبلاگ‌ها و اتاق‌های گفتگوی قومیت‌های آذری، بلوچ، ترکمن، کرد و عرب خوزستانی، با موضوع «اینترنت و هویت در پنج هویت



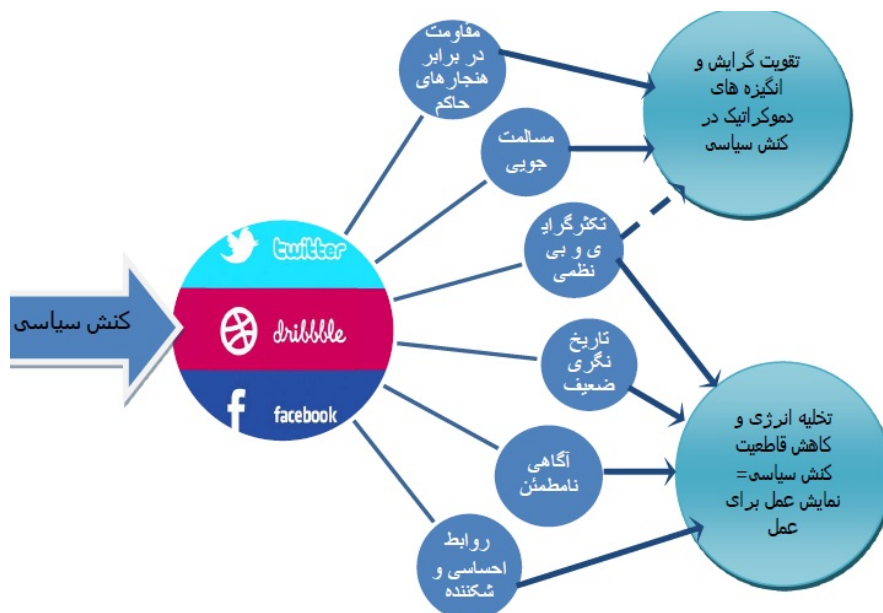
قومی ایران»، به این نتیجه رسیده که کردها تعلقات قومی خود را به نمایش گذاشته و تأکید زیادی بر استفاده از زبان کردی داشته‌اند [۶۸]. با توجه به مجموعه یافته‌های این دو تحقیق و در حالی که می‌گوییم فرد در فضای مجازی هویتی سیال و تغییرپذیر دارد، چگونه این هویت سیال و منعطف می‌تواند در فضای مجازی حول نیازهای حل نشده واقعی انسجام یابد؟

باید گفت اساساً ویژگی فنی و عام اینترنت داشتن ساختار دوگانه است. در فضای مجازی تمرکز وعدم تمرکز، کنترل مرکزی و خودمختاری، یگانگی و چندپارگی و جامعه‌پذیری و فردیت با هم جمع می‌شوند [۶۹]. بر این اساس هویت در شبکه‌های اجتماعی مجازی در جهت حل نیازهای حوزه واقعی انسان تغییر شکل می‌دهد، اما در عین حال نمی‌توان تأثیر تکثرگرایی و بی‌ثباتی فضای مجازی بر شکل‌گیری هویت سیال در این محیط را نادیده انگاشت. ثبات هویتی در محیط مجازی در نقاطی جهت دنبال کردن نیازهای حل نشده واقعی، آیا به معنای تأثیر این موضوع بر شکل‌گیری کنش سیاسی در جهت آن نیازهاست یا تکثرگرایی محیط مجازی مانع از پیوند ایده‌ها در فضای مجازی با کنش سیاسی می‌شود؟

مجموع دیدگاه‌هایی که گویای عدم شکل‌گیری آگاهی عمیق در محیط مجازی، تأثیر تکثرگرایی محیط مجازی و بی‌نظمی رفتاری برآمده از آن بر کنش سیاسی، بی‌زمانی و بی‌مکانی فضای مجازی و تأثیر آن در کنش سیاسی و عدم شکل‌گیری قاطعیت و خطرپذیری جهت کنش سیاسی در محیط مجازی را بیان می‌کنند، مانع از پاسخ سراسر مثبت به این سؤال هستند. برخی از محققین که معتقدند فناوری‌های جدید ارتباطی و شبکه‌های اجتماعی مجازی، به افراد شورشی که شناخت سیاسی کمی دارند، کمک کرده و آن‌ها را در رسیدن به اهداف خود یاری می‌کنند، لوازم دیگری را برای موفقیت افراد در یک جنبش سیاسی ضروری می‌دانند [۷۰]. این لوازم ضرورت رعایت مقتضیات کنش سیاسی را یادآور می‌شوند که بدون آن‌ها امکان موفقیت کنش‌گر فراهم نمی‌شود.

## ۵.۵ دگرگشت ارتباطات انسانی و کنش سیاسی

فضای مجازی و شبکه‌های اجتماعی مجازی علاوه بر گسست توافقات، از نظر برخی همچون ترکل و باومن، سبب انزوا و تنهایی بیشتر انسان می‌شوند و ارتباطات انسانی را از معنای واقعی خود خارج کرده، وضعیت مقطعی و شکننده بر آن‌ها تحمیل می‌کنند. این نوع ارتباطات نمی‌تواند کنش سیاسی را به نتیجه رساند. هدف ویژه امر سیاسی تفاهم درونی و امنیت بیرونی یک اجتماع است و از آنجا که هدف‌های غایی با دیگر فعالیت‌های انسانی همچون فعالیت اقتصادی، فرهنگی، اخلاقی و... در پیوستگی است، بنابراین «سیاست در مجموع زندگی انسان ادغام می‌شود و سیاست نمی‌تواند منزوی، فعالیت برای خود و ناگشوده به روی دیگر اقدامات بشر باشد» [۷۱]. این تعریف از سیاست با ارتباطات شکننده و انزوای افراد در محیط مجازی سازگار نیست. کنش سیاسی جهت دستیابی به اهداف ویژه امر سیاسی، مستلزم ارتباطات واقعی و مؤثر بین اعضای یک گروه است، چرا که نوع کنش سیاسی را اهداف ویژه امر سیاسی و اهداف غایی جامعه بشری معین می‌کنند و ماهیت این اهداف با انزوا در تضاد است.



شکل ۱: تاثیر فضای مجازی بر کنش سیاسی

## ۶ نتیجه گیری

اینترنت و شبکه‌های اجتماعی مجازی سبب افزایش آگاهی و دامنه شناخت فرد و گرایش وی به مقاومت در برابر الگوهای هنجاری حاکم می‌شوند. فضای متکثر و متنوع اینترنت و شبکه‌های اجتماعی مجازی از دیدگاه‌ها، نمادها و نشانه‌های مختلف و فراهم‌شدن زمینه سخن‌گویی افراد مختلف بدون هیچ مانعی، سبب انعطاف‌پذیری بیشتر افراد می‌شود. این ویژگی‌ها سبب گرایش‌های دموکراتیک در افراد، افزایش تحمل‌پذیری آنان و مطرح‌شدن خواسته‌هایی که در حوزه واقعی پاسخ داده نشده‌اند در ادبیات سیاسی حوزه مجازی و واقعی، می‌شود، اما این که این گرایش‌های دموکراتیک و برجسته‌شدن خواسته‌های پاسخ‌داده نشده در ادبیات جامعه، سبب ایجاد کنش سیاسی بر این مبنا می‌شود را نمی‌توان امیدوار بود. فضای مجازی ریشه در فضای واقعی دارد و ابتدا باید کنشی در حیطه واقعیت رخ بدهد تا آن‌گاه در فضای مجازی تبلور یابد. فضای مجازی نمی‌تواند آغازگر یک کنش سیاسی باشد، بدون این که در عرصه واقعیت اتفاقی رخ داده باشد. از سوی دیگر هرگاه در عرصه واقعی کنش سیاسی رخ دهد و این کنش در شبکه‌های اجتماعی مجازی بازتاب یابد، در این وضعیت شبکه‌های اجتماعی مجازی هرچند آرمان‌ها و اهداف این کنش را زنده نگه می‌دارند، اما همزمان موانعی را پیش روی آن ایجاد می‌کنند. تکرارگری و بی‌نظمی فضای مجازی، آگاهی نامطمئن، تضعیف تاریخ‌نگری و تجربیات تاریخی، روابط احساسی و شکننده سبب می‌شود تا از میزان قاطعیت و انرژی کنش‌گران سیاسی که فضای مجازی را برای بازتاب کنش سیاسی خود انتخاب کرده‌اند، کاسته شود و کنش سیاسی در نمایش عمل برای عمل خلاصه گردد. مجموع نتایج به دست آمده را می‌توان در شکل ۱ نشان داد.

بنابراین فرضیات پژوهش تا حد زیادی نیازمند تعدیل و اصلاح هستند. شبکه‌های اجتماعی مجازی کمتر رابطه مثبت با کنش سیاسی دارند. این شبکه‌ها نقش یاری‌دهنده زیادی در کنش‌های سیاسی ندارند و اتفاقاً هر اندازه کنش سیاسی از حوزه واقعیت به فضای مجازی بیشتر روی آورد، با موانع بیشتری در رسیدن به موفقیت مواجه می‌شود.

## مراجع

- [۱] شهرام‌نیا، امیرمسعود، ابراهیمی‌پور، حوا، محموداوغلی، رضا و ملکان، مجید. سنجش تأثیر شبکه‌های اجتماعی بر مشارکت سیاسی: مطالعه موردی دانشجویان دانشگاه مازندران. فصلنامه جامعه‌شناسی کاربردی، (۶۵): ۱۹-۳۲، ۱۳۹۶.
- [۲] محموداوغلی، رضا. بررسی تأثیرات شبکه‌های اجتماعی بر کنشگری سیاسی دانشجویان دانشگاه اصفهان. مجله علمی پژوهشی مطالعات توسعه اجتماعی فرهنگی، (۴): ۱۴۵-۱۶۸، ۱۳۹۵.
- [۳] نوری، مختار و قلی‌پور، مجتبی. رسانه‌های جمعی و کنش جمعی در جامعه سیاسی ایران. فصلنامه جستارهای سیاسی معاصر، (۲): ۳۳-۵۳، ۱۳۹۷.
- [۴] نجف‌پور، سارا و قلی‌پور، مجتبی. واکاوی امر سیاسی در فضای مجازی از منظری آرنتی. دوفصلنامه سیاست نظری، (۲۶): ۲۸۷-۳۱۹، ۱۳۹۸.
- [۵] بل، دیوید. درآمدی بر فرهنگ‌های سایبر، ترجمه مسعود کوثری و حسین حسینی. جامعه‌شناسان، ۱۳۸۹، ۱۵.
- [۶] اسلویین، جیمز. اینترنت و جامعه، ترجمه عباس گیلوری و علی رادباوه. نشر کتابدار، ۱۳۸۰، ۱۳.
- [۷] کانوی، مائورا. «بهره‌برداری تروریست‌ها از اینترنت و چالش‌های مدیریت فضای اطلاعات» در انقلاب، اطلاعات، امنیت و فناوری‌های جدید، ترجمه علیرضا طیب. پژوهشکده مطالعات راهبردی، ۱۳۸۹، ۱۴۲.
- [8] [www.blogrunner.com/snapshot/d/9/2/twitter\\_pointless\\_babble\\_or\\_peripheral\\_awareness\\_social](http://www.blogrunner.com/snapshot/d/9/2/twitter_pointless_babble_or_peripheral_awareness_social)
- [۹] لوینسون، پل. جدیدتر از رسانه‌های خیلی جدید. مجله جهانی رسانه، (۱۰): ۶، ۱۳۸۹.
- [۱۰] کانوی، مائورا. همان، ۱۱۴.
- [۱۱] بهرامی، کمیل. نظریه رسانه‌ها (جامعه‌شناسی ارتباطات). کویر، ۱۳۸۸، ۹۴-۹۵.
- [۱۲] تامپسون، جان ب. رسانه‌ها و مدرنیته (نظریه اجتماعی رسانه‌ها)، ترجمه مسعود اوحدی. سروش، ۱۳۸۹، ۳۲۳.
- [۱۳] بل، دیوید. همان، ۹۳-۹۴.
- [۱۴] بهرامی، کمیل. همان، ۲۸۶-۲۸۷.
- [15] Bimber, B. The internet and political transformation: Populism, community, and accelerated pluralism. [www.calstatela.edu/faculty/blawson/bimber%201998.pdf](http://www.calstatela.edu/faculty/blawson/bimber%201998.pdf), *The University of Chicago Press*, 1998.
- [16] Etling, Bruce, Faris, Robert, and Palfrey, John. Political change in the digital age: The fragility and promise of online organizing. [http://muse.jhu.edu/journals/sais\\_review/summary/v030/30.2.etling.html](http://muse.jhu.edu/journals/sais_review/summary/v030/30.2.etling.html), 2010.
- [17] Polleta, Francesca. "free spaces" in collective action. *Theory and Society*, 28(1):1-38, 1999.

- [۱۸] عاملی، سیدسعیدرضا. دو فضایی شدن کره زمین و توسعه واقعی - مجازی. مجموعه مقالات ارزیابی فضای مجازی ایرانی، دانشگاه تهران، ۱۳۸۵، ۷-۱۲.
- [۱۹] کاستلز، مانوئل. عصر اطلاعات: اقتصاد، جامعه و فرهنگ (جلد اول)، ترجمه احد علیقلیان و افشین خاکباز. ویراستار پایا، علی. طرح نو، ۱۳۸۰، ۵۳۷.
- [۲۰] دریفوس، هیوبرت. نگاهی فلسفی به اینترنت. گام نو، ۱۳۸۳، ۱۹.
- [۲۱] اسلوین، جیمز. همان، ۱۳.
- [۲۲] بل، دیوید. همان، ۶۷-۷۵.
- [۲۳] دریفوس، هیوبرت. همان، ۱۲۱.
- [24] Turkle, Sherry. *Alone Together: Why We Expect More from Technology and Less from Each Other*. Basic Books, 2011.
- [۲۵] بهرامی، کمیل. همان، ۲۹۳-۲۹۴.
- [۲۶] دریفوس، هیوبرت. همان، ۲۲.
- [۲۷] اسلوین، جیمز. همان، ۱۴.
- [28] Goldstein, Joshua and Rotich, Juliana. Digitally networked technology in kenya's 2007-2008 post-election crisis. *The Berkman Center for Technology and Society, Harvard University*, [http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein&Rotich\\_Digitally\\_Networked\\_Technology\\_Kenyas\\_Crisis.pdf](http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein&Rotich_Digitally_Networked_Technology_Kenyas_Crisis.pdf), 2008.
- [۲۹] رجبی، داود. قاب جادو (آسیب‌های اینترنتی در غرب). مرکز پژوهش‌های صدا و سیما، ۱۳۸۹، ۱۰۳.
- [۳۰] روزنا، جیمز. «اطلاعات، هوش مصنوعی و توسعه مهارت‌های تحلیلی نخبگانی اعتلا یافته و مردمانی توانمندتر» در انقلاب اطلاعات، امنیت و فناوری‌های جدید، ترجمه علیرضا طیب. پژوهشکده مطالعات راهبردی، ۱۳۸۹، ۷۳.
- [۳۱] مهدی‌زاده، سیدمحمد. اینترنت و حوزه عمومی. فصلنامه مطالعاتی و تحقیقاتی وسایل ارتباط جمعی (رسانه)، سال ۱۵، شماره ۵۹، ۱۳۸۳، ۱۲۵.
- [۳۲] اسلوین، جیمز، همان، ۴۸.
- [۳۳] بهرامی، کمیل. همان، ۲۸۶-۲۸۷.
- [۳۴] دریفوس، هیوبرت. همان، ۲۸.
- [۳۵] حافظ‌نیا، محمدرضا. جغرافیای سیاسی فضای مجازی. سمت، ۱۳۹۱، ۱۳.
- [۳۶] بل، دیوید. همان، ۱۹۰-۲۱۳.
- [۳۷] نورمحمدی، مرتضی. چالش‌های فرهنگ و هویت در فضای مجازی. پگاه حوزه، شماره ۲۶۱، ۱۳۸۸، ۳۱.
- [۳۸] وبر، ماکس. اقتصاد و جامعه، ترجمه عباس منوچهری و دیگران. مولی، ۱۳۷۴، ۳-۴.
- [۳۹] همیلتون، پیترو. تالکوت پارسونز، ترجمه علی برزگر. نشر مرن‌دیز، ۱۳۷۴، ۸۷.
- [۴۰] فروند، ژولین. سیاست چیست؟، ترجمه عبدالوهاب احمدی. آگاه، ۱۳۸۴.
- [۴۱] همان، ۴۴.

- [۴۲] بل، دیوید. همان، ۷۶-۷۹.
- [۴۳] فروند، ژولین. همان، ۴۳.
- [۴۴] دریفوس، هیوبرت. همان، ۱۱.
- [۴۵] بل، دیوید. همان، ۷۶-۷۹.
- [۴۶] فروند، ژولین. همان، ۸۳-۸۵.
- [۴۷] اسلوین، جیمز. همان، ۴۷-۴۸.
- [۴۸] فروند، ژولین. همان، ۹۱.
- [۴۹] همان، ۸۸-۸۹.
- [۵۰] همان، ۴۱.
- [۵۱] دریفوس، هیوبرت. همان، ۴.
- [۵۲] عاملی، سیدسعیدرضا. همان، ۷-۱۲. ۱۳۸۵.
- [۵۳] کاویانی، مراد و عزیزی، علی. نقش هویت مکانی در بروز گُش سیاسی مطالعه موردی: میدان و خیابان انقلاب شهر تهران. نشریه تحقیقات کاربردی علوم جغرافیایی، ۱۷(۲۰):۱۵۸، ۱۳۹۰.
- [۵۴] همان، ۱۵۷.
- [۵۵] همان، ۱۵۶.
- [۵۶] فروند، ژولین. همان، ۹۹-۱۰۱.
- [۵۷] بل، دیوید. همان، ۹۷-۷۵.
- [۵۸] دریفوس، هیوبرت. همان، ۱۲۱.
- [۵۹] همان، ۸۳.
- [۶۰] مهدی‌زاده، سیدمحمد. همان، ۱۲۵.
- [۶۱] ماه‌پیشانیان، مهسا. آسیب‌شناسی نقش شبکه‌های اجتماعی مجازی در جنبش بیداری اسلامی مصر. نهضت نرم‌افزاری، صفحات ۵۱-۵۰، ۱۳۹۱.
- [۶۲] فروند، ژولین. همان، ۴۳-۴۷.
- [۶۳] همان، ۲۸-۳۰.
- [۶۴] اسلوین، جیمز. همان، ۱۶.
- [۶۵] دریفوس، هیوبرت. همان.
- [۶۶] کاویانی، مراد و عزیزی، علی. همان، ۱۵۵.
- [۶۷] حکیمی، رؤیا. نقش شبکه‌های اجتماعی بر هویت (مطالعه ای موردی روی فیس بوک و کاربران کرد). مجله جهانی رسانه، (۱۱)، ۱۳۹۰.
- [۶۸] فکوهی، ناصر و عیاری، آذرنوش. اینترنت و هویت در پنج هویت قومی ایرانی. مجله جهانی رسانه، ۱۳۸۸.
- [۶۹] ون‌دایک، جان. «سیاست‌گذاری در جامعه شبکه‌ای»، ترجمه پیروز ایزدی. فصلنامه مطالعاتی و تحقیقاتی وسایل ارتباط جمعی (رسانه)، (۵):۸۲، ۱۳۸۲.

[70] Etling, Bruce, Faris, Robert M., and Palfrey, John Gorham. Political change in the digital age: The fragility and promise of online organizing. *The Berkman Klein Center for Internet & Society at Harvard University*, [http://muse.jhu.edu/journals/sais\\_review/summary/v030/30.2.etling.html](http://muse.jhu.edu/journals/sais_review/summary/v030/30.2.etling.html), 2010.

[۷۱] فروند، ژولین. همان، ۱۲۹-۱۲۶.



## ترسیم نقشه‌ی هم‌واژگانی و تحلیل موضوعی مقالات حوزه داده‌کاوی در پایگاه اسکوپوس با استفاده از نرم‌افزار وی.او.اس. ویور

آرام مجیری<sup>۱</sup>، محسن حاجی زین العابدینی<sup>۲</sup>

<sup>۱</sup> دانشجوی دکتری، گروه علم اطلاعات و دانش‌شناسی، دانشگاه شیراز  
aram.mojiri76@gmail.com

<sup>۲</sup> استادیار، گروه علم اطلاعات و دانش‌شناسی، دانشگاه شهید بهشتی، تهران  
zabedini@gmail.com

### چکیده

هدف از این پژوهش ترسیم نقشه هم‌واژگانی و تحلیل موضوعی مقالات حوزه داده‌کاوی که در پایگاه اسکوپوس نمایه شده‌اند، است. این پژوهش از نوع توصیفی بوده و با رویکرد علم‌سنجی انجام گرفته است. جامعه آماری مورد پژوهش، مقالات پایگاه اسکوپوس بین سال‌های ۲۰۱۵ تا ۲۰۲۰ هستند. داده‌ها در نرم‌افزار وی.او.اس.ویور و اکسل مورد تحلیل و بررسی قرار گرفتند و جستجو در بین مقالاتی که دارای دو عبارت "Data Mining" و "Data Text" بودند انجام شد. تعداد مقالات بازیابی شده ۱۸۹۴ بود که برای انسجام در کار از ۱۰۳ مقاله‌ای که حد آستانه هم‌رخدادی کلید واژگان آن ۶ بود استفاده شد و در آخر مورد بررسی قرار گرفتند. تعداد خوشه‌های ایجاد شده توسط نرم‌افزار، هفت خوشه بود و خوشه‌ی اول که بزرگ‌ترین و مهم‌ترین خوشه است، ۱۷ مورد را شامل شد. طبق نتایج به دست آمده می‌توان گفت که ارتباط بین داده‌کاوی و متن‌کاوی بسیار زیاد است. در این مقاله مؤثرترین موضوعات در این حوزه مشخص شده‌اند که دو مورد از آن‌ها word embeddings و web mining هستند. هم‌چنین دو مورد از موضوعات مهم بر اساس هم‌رخدادی موضوعی شامل opinion mining و network analysis. دو مورد از پرتکرارترین کلمات عبارتند از text mining و data mining.

**کلمات کلیدی:** داده‌کاوی، ترسیم نقشه‌ی هم‌واژگانی، تحلیل موضوعی، پایگاه اسکوپوس، نرم‌افزار وی.او.اس.ویور.

### ۱ مقدمه

در عصر حاضر، ذخیره سازی اطلاعات بسیار ارزان است؛ به طوری که حجم بزرگی از داده‌های گوناگون در همه جا پراکنده است. طرفداران داده‌کاوی این نوید را می‌دهند که کوه‌های عظیم داده‌ها در دل خود اطلاعاتی

دارند که می‌تواند ارزشمند باشد و برای بهره برداری از این مخازن عظیم تنها کاری که باید انجام شود اقدام به بیرون کشیدن آن اطلاعات ارزشمند است. بنابراین اصطلاح داده‌کاوی برای گردآوری ناهمگن ابزارها به منظور استخراج اطلاعات بالقوه ارزشمند از درون سلسله کوه‌های عظیم داده‌ها به کار می‌رود. در واقع داده‌کاوی اشاره به استخراج و یا کاوش دانش از میان حجم عظیمی از داده یا انبار داده‌ها دارد [۱][۲] به عبارت دیگر داده‌کاوی علم استخراج اطلاعات مفید از پایگاه‌های داده یا مجموعه داده‌ای است [۳].

در طی چند دهه گذشته با پیشرفت روز افزون کاربرد پایگاه داده‌ها، حجم داده‌های ثبت شده به طور متوسط هر ۵ سال دو برابر شده است. در این میان، سازمان‌هایی موفق هستند که بتوانند حداقل ۷% داده‌هایشان را تحلیل کنند [۴]. حوزه علم‌سنجی در جهت سهولت بخشیدن دسترسی به اطلاعات و کمک به جستجوگران دانش از طریق پردازش، استخراج و مرتب سازی اطلاعات به ترسیم ساختار فکری دانش می‌پردازد و با هدف بررسی ساختار دانش در حوزه‌های علمی از روش‌ها و فنون مختلف مانند هم استنادی، هم واژگانی و هم نویسنده‌گی، امکان تحلیل مسیر یابی و نمایش دانش را فراهم می‌کند [۵].

شاخص‌های علمی پژوهشی، جایگاه کشورها را تعیین می‌کند. در واقع علم و پژوهش نشان‌دهنده‌ی قدرت است. در نتیجه فاصله بین کشورها و جایگاه کشورها از نظر تأثیرگذاری و مقبولیت به نسبت سطح علمی و پژوهش‌ها، تعیین می‌شود. همین‌طور توسعه مرزهای علم و دانش تأثیر مستقیمی بر روی رشد اقتصادی کشور دارد [۶]. یکی از کارآمدترین شیوه‌های بررسی وضعیت کلی پژوهش، استفاده از مطالعات علم‌سنجی است و علم‌سنجی، علم اندازه‌گیری و تجزیه و تحلیل فعالیت‌های مکتوب علمی است [۷]. تحلیل هم‌واژگانی نیز یکی از روش‌های علم‌سنجی است و بر این فرض استوار است که کاربرد واژه‌های مشترک در دو یا چند متن، حاکی از نزدیکی آن متون به یکدیگر است. این روش ابزار قدرتمندی در ردیابی علوم است و به واسطه آن می‌توان ساختار، مفاهیم و مؤلفه‌های حوزه‌های علمی را شناسایی و برای آن سیاست‌گذاری کرد. با این روش می‌توان الگوها و رویدادهای مفهومی، ساختار علمی، شبکه مفهومی، روابط سلسله مراتبی مفاهیم و مقولات مفهومی را کشف و ترسیم نمود؛ در نتیجه ردیابی توسعه و پیشرفت حوزه‌های علمی ممکن خواهد شد [۸].

هدف از این پژوهش، آن است که با استفاده از نرم افزار وی.او.اس.ویور نقشه هم‌واژگانی مقالات حوزه داده‌کاوی ترسیم شود و همچنین به تحلیل موضوعی مقالات این حوزه که در پایگاه اسکوپوس در سال‌های بین ۲۰۱۵ تا ۲۰۲۰ نمایه شده‌اند، پرداخته است.

در این پژوهش سعی شده است به پرسش‌های زیر پاسخ داده شود:

- شبکه هم‌واژگانی مقالات به چه صورتی است؟
- مهم‌ترین موضوعات حوزه داده‌کاوی کدام‌اند؟
- مؤثرترین موضوعات این حوزه کدام‌اند؟
- موضوعات مهم بر اساس هم‌رخدادی موضوعی کدام‌اند؟

## • پرتکرارترین کلمات در مقالات این حوزه کدام اند؟

مطالبی که در بخش‌های آینده در مقاله بیان می‌شود شامل پیشینه‌ی پژوهش، روش پژوهش، یافته‌ها و نتیجه‌گیری است.

## ۲ مروری بر کارهای دیگران

در این زمینه پژوهش‌های بسیاری انجام شده است که این پژوهش بعضی از فعالیت‌های اخیر را مورد بررسی قرار داده است.

مکی زاده و دیگران در سال ۱۳۹۵ در حوزه درمان افسردگی، پژوهشی با استفاده از تحلیل هم‌رخدادی واژگان و فن تحلیل شبکه و بهره‌گیری از نرم‌افزارهای راور ماتریس، یو سی نت و نت دراور با هدف کشف زمینه‌های موضوعی پرکاربرد و نو ظهور انجام دادند. آنان به این نتیجه رسیدند که در حوزه درمان افسردگی، دو حوزه دارودرمانی و روانشناسی پرکاربردترین موضوعات هستند؛ از دیگر نتایج این پژوهش مشخص کردن حوزه‌های مطالعاتی جدید در این حوزه بوده است [۹].

فیض‌آبادی و وزیری در سال ۱۳۹۶ در مطالعه‌ای به ترسیم ساختار حوزه‌های علمی مطالعات دمانس با استفاده از روش تحلیل هم‌رخدادی واژگان پرداختند. یافته‌های آن‌ها نشان دادند که تعداد مقالات از ۱۴ مقاله در سال ۱۹۸۳ به ۱۱۳۰ مقاله در سال ۲۰۱۴ رسیده است. تعداد ۱۴۴۱۷ مقاله بازیابی شده ۵۵۸۹۲ کلیدواژه داشت. نتایج حاصل از تحلیل هم‌وقوعی کلیدواژه‌ها نشان می‌دهند که این مفاهیم در پنج دسته کلی *Alzheimer disease, dementia, mild cognitive impairment, cognition* و *frail elderly* قرار می‌گیرند. همچنین نتایج هم‌رخدادی واژگان در بازه زمانی ۵ ساله نیز نشان دادند که طی سال‌های اخیر، علاوه بر کلیدواژه‌های آلزایمر و دمانس، واژه‌های *memory, aging, cognition* و *caregivers* رشد زیادی داشته‌اند [۱۰].

رئیس‌زاده و کرمعلی در سال ۱۳۹۷ به ترسیم نقشه علمی مقالات حوزه ترومای نظامی با استفاده از تحلیل هم‌واژگانی در مدلاین پرداختند. یافته‌ها نشان دادند که رشد تولیدات علمی مربوط به حوزه ترومای نظام، در بازه زمانی ۲۰۱۷-۲۰۰۰ سیر صعودی داشته و با نرخ رشد نسبتاً ثابتی بوده است. نتایج تحلیل هم‌واژگانی در مقالات بیانگر تمرکز موضوعات در زمینه‌های PTSD نوع زخم، مدیریت مجروحان، شرایط رزم و تجارت جنگ‌هایی عراق و افغانستان بوده است [۱۱].

کرمبخش و محمودی در سال ۱۳۹۸ به پژوهشی با عنوان مروری بر تولیدات علمی ایران در حوزه روانشناسی و روان‌پزشکی نظامی بر اساس پایگاه داده اسکوپوس یک مطالعه علم‌سنجی تا سال ۲۰۱۸ پرداختند. در این پژوهش مطالعه مروری با رویکرد علم‌سنجی انجام شد و کلیدواژه‌های مرتبط با حوزه روانشناسی و روان‌پزشکی نظامی تعیین گردید. سپس پایگاه استنادی اسکوپوس به عنوان مرجع معتبر علمی برای جستجوی تولیدات علمی ایران انتخاب شد و با رعایت دستورالعمل این پایگاه فرمول جستجو با ترکیب کلیدواژه‌ها تنظیم گردید. منابع انتشار یافته تا تاریخ ۱۰ شهریور ۲۹۳۰ استخراج و تحلیل داده‌های آماری صورت گرفت. یافته‌ها حاکی از آن بود که تولیدات روانشناسی و روان‌پزشکی نظامی در دنیا ۹۱۲۲۳

مورد بوده که آمریکا با تولید ۱۱۹۲۱ مورد رتبه اول و انگلستان با ۹۹۲۷ مورد در جایگاه دوم قرار دارد و سهم ایران نیز ۹۲۷ مورد (رتبه ۲۱) است. بهترین دانشگاه در ایران در این حوزه دانشگاه علوم پزشکی بقیه الله با انتشار ۱۹ مقاله و بیشترین سهم در پذیرش و انتشار مقالات در بین مجلات مربوط به مجله طب نظامی با انتشار ۹۱ مقاله است همچنین بیشترین ارجاع به مقالات این حوزه مربوط به مقاله چاپ شده در مجله *toxicology and pharmacology clinical and Basic* در سال ۱۷۷۱ میلادی است [۱۲].

محمدلو و بتولی در سال ۱۳۹۹ پژوهشی با عنوان مطالعه علم‌سنجی و تحلیل محتوای تولیدات علمی با موضوع "سلب اعتبار مقالات" در پایگاه استنادی اسکوپوس انجام دادند. در این پژوهش جامعه آماری، تولیدات علمی با موضوع "سلب اعتبار مقالات" بود که تا ابتدای اگوست ۲۰۱۹ در اسکوپوس نمایه شده‌اند. از ۲۶۲۸ مقاله بازیابی شده، ۱۴۰ مقاله مرتبط با موضوع، جهت بررسی انتخاب گردید. مدارک منتخب از نظر سال انتشار، نام کشور، نویسندگان، زبان و موضوع مورد بررسی قرار گرفت. نتایج، حاکی از افزایش قابل ملاحظه تعداد مقالات از سال ۲۰۱۴ به بعد است. ۱۵۹ نویسنده از ۳۶ کشور و ۱۶۰ دانشگاه / سازمان در نگارش این مقالات مشارکت داشتند. دلایل سلب اعتبار و موضوعات مقالات سلب اعتبار شده بررسی شد. همچنین تأثیر سلب اعتبار بر اعتبار نویسندگان، تعداد تولید علمی و تعداد استناد، وضعیت درآمد، جنسیت و زبان نویسندگان، همکاری بین‌المللی، روند سلب اعتبار مقالات، نوع مطالعه، دارا بودن اعلان سلب اعتبار، ضریب تأثیر مجله و مدت زمان بین انتشار تا سلب اعتبار نیز تحلیل شد. در نهایت به نقش دانشگاه‌ها جهت آگاه‌سازی پژوهشگران، آموزش امانت‌داری پژوهش و حساس کردن آن‌ها نسبت به بدرفتاری علمی اشاره شده بود [۱۳].

خاصه و دیگران در سال ۱۴۰۰ به تحلیل علم‌سنجی و دیداری سازی برون‌داد علمی فصلنامه کتابداری و اطلاع رسانی طی سال‌های ۱۳۸۸ تا ۱۳۹۷ پرداختند. در این پژوهش همه ۳۷۰ عنوان مقاله منتشر شده در این فصلنامه در سال‌های ۱۳۸۸ تا ۱۳۹۷ در پایگاه استنادی علوم ایران جستجو و استخراج شد و داده‌ها پس از اصلاحات ضروری داده‌ها در انواع نرم افزارهای تحلیل و نگاشت علمی مانند نت در او، یوسی.نت و وی.او.اس.ویور وارد و خروجی‌های حاصل تحلیل شد. یافته‌ها نشان داد که توزیع جغرافیایی مؤسسات تولیدکننده و وضعیت نویسندگان پرکار از نظر تولید مقاله و اثرگذار به لحاظ دریافت استناد و شاخص اچ در فصلنامه مناسب بود. الگوی تألیف گروهی و مرکزیت‌های رتبه، بینایی و نزدیکی نویسندگان حاکی از تعامل مؤثر پژوهشگران در نگارش آثار بود. تحلیل هم‌رخدادی کلیدواژگان پرسیامد نشان‌دهنده توجه به مباحث جدید حوزه و مسائل مهم کتابخانه‌ها بود. خوشه‌های موضوعی ترسیم شده هم نشان از برجسته بودن موضوع علم‌سنجی و سازمان‌دهی دانش و مسائل مرتبط با مدیریت کتابخانه‌ها داشت. هرچند فصلنامه توانسته است، به‌ویژه در حوزه کتابخانه‌ها و اطلاع رسانی اثرگذار باشد، لازم است با دسترس‌پذیر شدن بیشتر و در نظر گرفتن تمهیداتی دیگر، نسبت کل استناد به مقاله را افزایش دهد و سهم موضوعات نوپدید در تدوین مقالات آن بیشتر شود [۱۴].

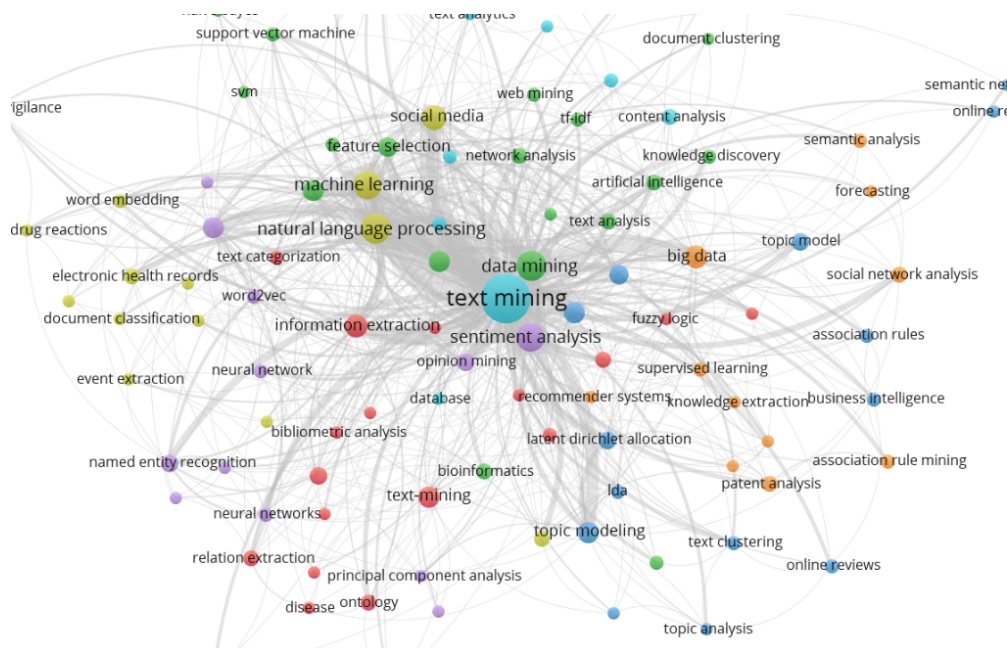
با مطالعه و بررسی‌های انجام‌شده مشخص شد که تا به حال مقاله‌ای به ترسیم نقشه هم‌واژگانی و تحلیل موضوعی مقالات حوزه داده‌کاوی در پایگاه اسکوپوس نپرداخته است.

### ۳ روش پژوهش

پژوهش حاضر از نوع توصیفی و با رویکرد علم‌سنجی بوده است. جامعه آماری مورد پژوهش، مقالات پایگاه اسکوپوس بین سال‌های ۲۰۱۵ تا ۲۰۲۰ است که در تاریخ ۱۳-۰۳-۱۴۰۰ اطلاعات مورد نیاز از این پایگاه استخراج شده و داده‌ها در نرم افزار وی.او.اس. ویور و اکسل مورد تحلیل و بررسی قرار گرفته‌اند. روش کار در این پژوهش به این صورت است که در زمان جستجو از روش جستجوی پیشرفته پایگاه اسکوپوس استفاده شد و جستجو در بین مقالاتی که دارای دو عبارت "Data Mining" و "Data Text" که در سال‌های بین ۲۰۱۵ تا ۲۰۲۰ منتشر شده‌اند لحاظ گردید. همین‌طور مطالعه بر روی مقالاتی که در این پایگاه به زبان انگلیسی بودند انجام شد. تعداد مقالات بازایی شده ۱۸۹۴ مقاله بود که برای انسجام در کار از ۱۰۳ مقاله‌ای که حد آستانه هم‌رخدای کلید واژگان آن ۶ بود استفاده شد. این مقالات در نرم افزارهای گفته شده تحلیل و بررسی شدند و نتایج حاصل در بخش یافته‌ها به طور کامل بیان شده است.

### ۴ یافته‌های پژوهش

در این بخش سعی شده است به پرسش‌های مورد نظر در رابطه با مقالات حوزه داده‌کاوی پاسخ داده شود: برای پاسخ به پرسش اول با استفاده از نرم افزار وی.او.اس. ویور نقشه هم‌واژگانی مقالات این حوزه به صورت شکل ۱ است.



شکل ۱: ترسیم نقشه هم‌واژگانی مقالات حوزه داده‌کاوی

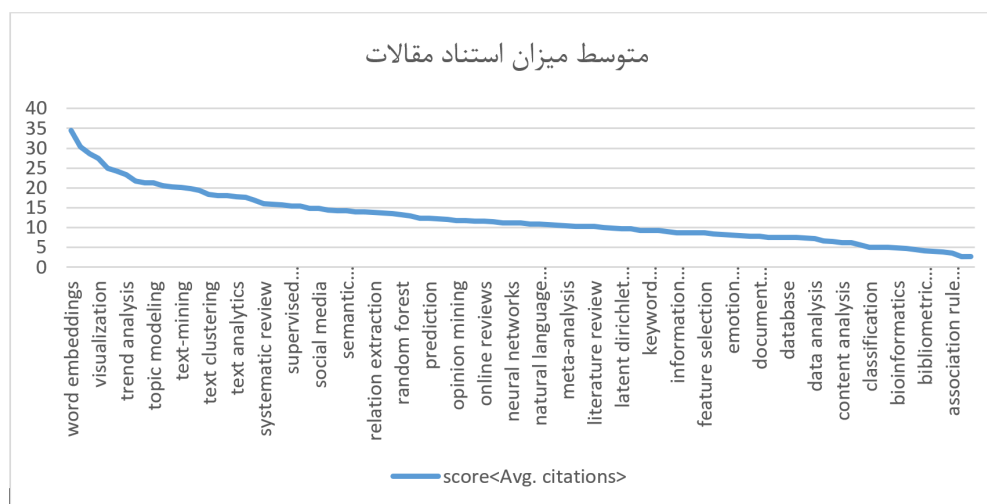
طبق شکل ۱، رنگ‌های مختلف نشان دهنده خوشه‌های مختلف ایجاد شده است و همان‌طور که ملاحظه



می‌شود هرچه ارتباط بین موضوعات بیشتر باشد لینک بین آن‌ها پررنگ‌تر و به هم نزدیک‌تر هستند و همین‌طور هرچه اهمیت یک واژه در شبکه بیشتر باشد سایز گره‌ها بزرگ‌تر نشان داده می‌شوند؛ پس می‌توان متوجه شد که دو واژه اصلی و موضوعات مهم این حوزه، داده‌کاوی و متن‌کاوی هستند و فاصله نزدیک این دو نسبت به یکدیگر نشان دهنده ارتباط زیاد این دو موضوع با یکدیگر است.

برای پاسخ به پرسش دوم تعداد خوشه‌های ایجاد شده توسط نرم افزار، هفت خوشه است که تعداد آیتم‌های موجود در هرکدام از این خوشه‌ها به ترتیب از بزرگ‌ترین خوشه تا کوچک‌ترین آن ۱۷، ۱۷، ۱۶، ۱۵، ۱۳، ۱۳، ۱۱ مورد است. که خوشه اول بزرگ‌ترین و مهم‌ترین خوشه است که شامل ۱۷ مورد: in-formation extraction, ontology, biomedical text mining, text-mining, feature extraction, relation extraction, keyword, bibliometric analysis, text categorization, visualization, trend analysis, systematic review, semantic similarity, text summarization, extraction, fuzzy logic, meta-analysis, visual analytics است. پس مهم‌ترین موضوعات موجود در مقالات حوزه داده‌کاوی به صورت گفته شده است. زیرا اغلب، مهم‌ترین موضوعات در اولین خوشه قرار می‌گیرند.

سومین پرسش مطرح شده که باید به آن پاسخ داد درمورد مؤثرترین موضوعات این حوزه است که برای پاسخ به این پرسش باید به تعداد دفعاتی که به یک مقاله استناد شده است و آن موضوع مورد نظر در آن مقاله وجود داشته است توجه کرد. شکل ۲ خلاصه‌ای از این واژگان و تعداد دفعات استناد را نشان داده است که با توجه به ترتیبی که در نرم افزار اکسل بود چهار مورد از مؤثرترین موضوعات شامل word embeddings, web mining, visualization و visual analytics است.

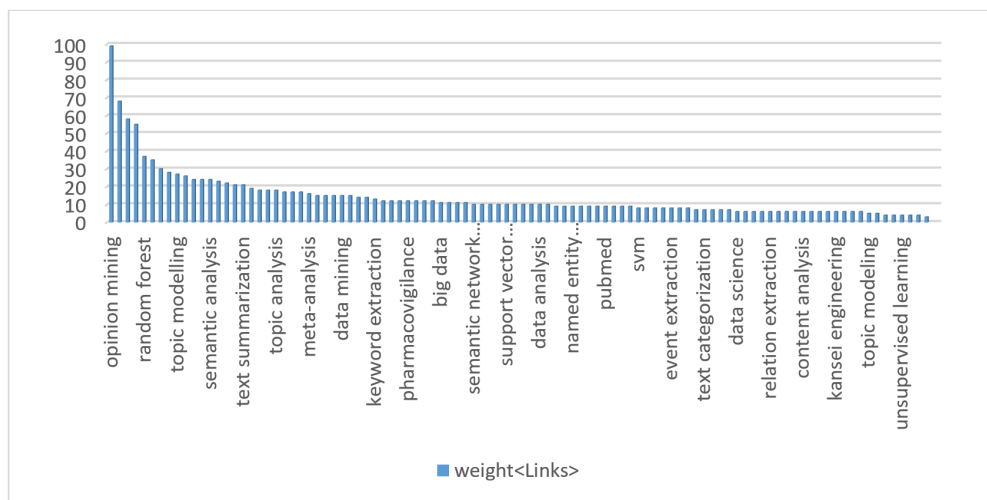


شکل ۲: مؤثرترین موضوعات حوزه داده‌کاوی

چهارمین پرسش مطرح شده این بود که موضوعات مهم بر اساس هم‌رخدادی موضوعی کدام هستند که برای پی بردن به این مسئله، میزان ارتباط یک موضوع با موضوعات دیگر مورد بررسی قرار گرفته شد. به



عبارتی هر چه ارتباط یک موضوع با موضوعات دیگر بیشتر باشد، اهمیت آن موضوع بر اساس هم‌رخدادی را نشان می‌دهد. شکل ۳ نشان دهنده این موضوعات هستند؛ که چهار موردی که بیشترین هم‌رخدادی را شامل می‌شوند عبارت است از: social, text classification, network analysis, opinion mining. network analysis که میزان هم‌رخدادی این موضوع با دیگر موضوعات به ترتیب برابر است با ۶۸، ۹۹، ۵۵ و ۵۸.



شکل ۳: موضوعات مهم بر اساس هم‌رخدادی موضوعی

آخرین پرسش، تعیین پرتکرارترین کلمات موجود در مقالات است؛ که برای پاسخ به این پرسش کلماتی که بیشترین تکرار را در کلیدواژه نویسندگان دارا هستند انتخاب شده‌اند. ده مورد از پرتکرارترین کلمات در جدول زیر آمده است:

جدول ۱: پرتکرارترین واژگان مقالات

تعداد تکرار	واژگان
958	text mining
169	data mining
149	language processing Natural
129	machine learning
124	sentiment analysis
81	social media
56	information extraction
54	big data
45	classification
44	deep learning

جدول ۱ پربسامدترین و پرتکرارترین موضوعات را به ما نشان داده است؛ که باید توجه کرد که هرچه بسامد یک موضوع بیشتر باشد، اهمیت آن در شبکه بیشتر می‌شود. در نتیجه می‌توان گفت موضوعات متن‌کاوی و داده‌کاوی از اهمیت بالایی برخوردار هستند.

## ۵ نتیجه‌گیری

در دنیای امروز داده‌کاوی به یکی از موضوعات مهم و پرکاربرد تبدیل شده است که می‌توان آن را در زمینه‌های مختلف بکار برد؛ با استفاده از داده‌های بسیار بزرگ، الگوها و مدل‌هایی در اختیار ما قرار می‌گیرند که می‌توان با آن‌ها تا حدودی آینده را پیش بینی کرد. نتیجه کاربرد پذیری داده‌کاوی در زمینه‌های مختلف، اهمیت روز افزون آن و معطوف شدن تمرکز بر روی این حوزه است. به این دلیل که در رشته علم اطلاعات نیز با داده‌ها و اطلاعات سروکار داریم، در این رشته نیز داده‌کاوی مورد توجه قرار گرفته است و از آن استفاده می‌شود و این امر باعث شد تا این پژوهش بر روی حوزه داده‌کاوی با رویکرد علم‌سنجی انجام گیرد و نقشه هم‌واژگانی مقالات این حوزه ترسیم شود و بر روی موضوعات و واژگان آن تحلیل و بررسی‌هایی صورت گرفت.

طبق نتایج به دست آمده می‌توان گفت که ارتباط بین داده‌کاوی و متن‌کاوی بسیار زیاد است، زیرا طبق شکل ۱ این دو موضوع در کنار یکدیگر قرار گرفته‌اند و همین‌طور اهمیت این دو موضوع در شبکه طبق بزرگ بودن سایز گره این دو موضوع، زیاد است. مؤثرترین موضوعات در این حوزه مشخص شده‌اند که دو مورد از آن‌ها word embeddings و web mining هستند. همچنین دو مورد از موضوعات مهم بر اساس هم‌رخدادی موضوعی شامل opinion mining و network analysis و دو مورد از پرتکرارترین کلمات عبارت‌اند از text mining و data mining هستند.

## مراجع

- [1] Hand, D. "what is data mining?" transl. h. gudarzi. *Reviews of official statistics of Iran*, 2002.
- [2] Devyudi, R. K. and Pai, R. P. Baj. Review on the applications of data mining in librarianship and information, transl. i. jafarpour. *book of the moon*, 2011.
- [3] Hand, D., Mannila, H., and Smyth, S. Padhraic. *Principles of Data Mining*. Cambridge, MTT Press, 2001.
- [4] Fayyad, U., Piatetsky-Shapiro, G., and Smyth, P. From data mining to knowledge discovery in databases. *AI Magazine*, 1996.
- [5] Chakoli, A. Nowrozi. Role and place of scientometric studies in development. *Journal of Information Processing and Management*, 2012.
- [6] Mesgarpour, B., Etemadi, A., Fotuhi, A., Karbaizadeh, A., and Yousefian, M. Pharmaceutical science research trends in iran compared to middle eastern and north african countries: a scientometric study. *Health Information Management*, 2009.

- [7] Zamani, G. H., Khalkhabali, I. Azizi, and Hayati, D. Progress of iran's science in agriculture and natural resources: A scientometric study. *Science and Extension and Agriculture of Iran*, 2008.
- [8] Ahmadi, H. and Asareh, F. Review on the functions of synonymous analysis. *National Studies in Library and Information Organization*, 2016.
- [9] Makizadeh, F., Hazeri, A., Hosseininasab, S. H., and Soheili, F. Thematic analysis and drawing of a scientific map of articles related to the field of depression treatment. *Health Management Quarterly*, 2015.
- [10] Feizabadi, M. and Vaziri, A. Mapping the structure of the scientific fields of dementia studies using the method of vocabulary co-occurrence analysis. *Journal of Sabzevar University of Medical Sciences*, 2016.
- [11] Raiszadeh, M. and Karamali, M. Scientific mapping of articles in the field of military intelligence using synonym analysis in medline. *Military Medicine Journal*, 2017.
- [12] Karambakhsh, A. and Tarahi, M. A review of iran's scientific productions in the field of military psychology and psychiatry based on the scopus database: a scientometric study until 2018. *Journal of Military Medicine*, 2018.
- [13] Mohammadlou, A. and Batoli, Z. Scientometric study and content analysis of scientific productions with the topic of "disqualification of articles" in the scopus citation database. *Faiz Publication*, 2019.
- [14] Khaase, A., Mokhtari, H., and Aghaei, N. Scientometric analysis and visualization of the scientific output of the library and information quarterly during the years 2009 to 2018. *Library and Information*, 2021.



## تحلیل راهبردی اقدامات مقررات حفاظت از داده‌های عمومی (ارائه چارچوب مفهومی اقدامات کلان حفاظت از داده در کشور)

رحیم خانی زاد<sup>۱</sup>، ابوزر عرب سرخی<sup>۲</sup>

<sup>۱</sup> استادیار، دانشگاه علم و صنعت ایران، تهران  
khanizad@iust.ac.ir

<sup>۲</sup> استادیار، پژوهشگاه فناوری اطلاعات و ارتباطات، تهران  
abouzar\_arab@itrc.ac.ir

### چکیده

توسعه روزافزون فناوری‌های اطلاعاتی و رشد صعودی دارایی‌های اطلاعاتی منتشر شده در فضای سایبر علاوه بر ایجاد فرصت‌های بزرگ برای استفاده از آن در حوزه‌های مختلف، موجب بروز تهدیدات امنیتی متنوع و متفاوتی از سمت بازیگران مختلف هم در فضای فردی و هم در ابعاد اجتماعی، ملی و بین‌المللی شده است. کشور ایران نیز به دلیل موقعیت خاصی که در منطقه و جهان دارد، از لحاظ بین‌المللی نیز در معرض خطرات و تهدیدات اطلاعاتی خاص خود قرار گرفته است و در این شرایط نیازمند تقویت ساختارهای حکمرانی اطلاعاتی از جنس حفظ و مدیریت امنیت داده‌ها و اطلاعات کشور در این حوزه است. از این رو در مقاله حاضر مؤلف به دنبال آن است تا ضمن مطالعه و مقایسه رهیافت‌ها، راهبردها و خط مشی‌های ملی کشورهای مختلف نظیر ایالات متحده آمریکا، کانادا، اتحادیه اروپا، آلمان، کره جنوبی و... در زمینه تدوین و بهره‌برداری از مقررات حفاظت از داده‌های عمومی، نسبت به شناسایی گزینه‌های راهبردی و ارائه چارچوب مفهومی اقدامات کلان در کشور حرکت نماید. این پژوهش امکان شناسایی رفتار مؤثر و کارا با پدیده‌های نوظهور را فراهم می‌آورد. در این راستا، شناسایی و مطالعه نظام‌مند اسناد راهبردی کشورها با بهره‌گیری از روش تحلیل محتوای کیفی متعارف انجام شد. در ادامه، به منظور ارزیابی و پایایی‌گذاری محتوا، با محاسبه ضریب توافق کاپای کوهن معادل ۶۲.۰۰ به دست آمد. بر اساس نتایج تحقیق، مقوله‌هایی چون جمع‌آوری و اعلام، اعلان نقض در اطلاعات، محدودیت پردازش و استفاده، محدودیت در جمع‌آوری داده، حق تعریف اطلاعات و داده‌های شخصی، حق اعلام جمع‌آوری، مسئولیت‌پذیری، اعلان نقض در داده‌ها، حفظ حریم خصوصی آنلاین و پردازش اطلاعات شخصی حساس، به‌عنوان مهم‌ترین درس‌های آموخته و محورهای چارچوب مفهومی اقدامات کلان پیشنهادی جهت تدوین راهبردهای ملی در زمینه توسعه مقررات حفاظت از داده‌های عمومی شناسایی شدند.

**کلمات کلیدی:** راهبردهای ملی توسعه مقررات حفاظت از داده‌های عمومی، تحلیل فراگیر راهبردها، تحلیل محتوا.

## ۱ مقدمه

شرکت‌ها، سازمان‌ها و کسب‌وکارهای مختلف هر کدام به دلایلی نظیر ارائه کالاها و خدمات، اعطای مجوز، شناسایی وضعیت و هویت افراد به‌نحوی با داده‌ها و اطلاعات افراد سر و کار دارند. از سوی دیگر افراد در سطوح مختلف با توجه به نوع فعالیت و مجوزهایی که از سوی مراجع مختلف صادر می‌شوند، سطحی از اعتماد در حفظ حریم خصوصی را برای این نهادهای حقوقی قائل هستند. این امر نه تنها از جنبه حفظ حریم و اطلاعات خصوصی، بلکه از جنبه اعتماد عمومی و اجتماعی نیز دارای اهمیت است که حاکمیت بتواند نه تنها اعتماد افراد، بلکه اعتماد به ساختارهای سازمان‌محور تحت حمایت و حاکمیت خود را از استفاده بجا و بدون سوء استفاده از داده‌ها و اطلاعاتشان در هر سطحی مطمئن سازد. از سوی دیگر، ماهیت هر جایی، هر زمانی و گستردگی کاربردهای فناوری‌های مبتنی بر داده و اطلاعات از یک سو و پراکندگی و گستردگی شرکت‌ها، سازمان‌ها و نهادهایی که با اطلاعات عمومی در ارتباط هستند از سوی دیگر، موجب شده است که نظارت بر چنین امری (حفاظت از داده‌ها) به مقوله‌ای چالش‌برانگیز و در عین حال اجتناب‌ناپذیر تبدیل شود. این امر لزوم طراحی ساز و کارهای متنوع برای حفاظت از داده‌های عمومی را دوجندان کرده و با توجه به شیوع و پیشرفت آن در طول زمان، اهمیت و فوریت آن را نیز افزایش داده است.

### ۱.۱ حریم خصوصی و حفاظت از داده‌های شخصی

«حریم خصوصی» به توانایی فرد یا گروهی اشاره دارد که می‌تواند خود یا اطلاعاتی را در مورد خود حفظ نماید و از این طریق اطلاعات خود را به هر صورتی که مایل باشد، بیان کند [۱]. زمانی که موضوعی برای شخص (یا اشخاصی) ماهیتی خصوصی دارد، معمولاً بدان معنی است که آن موضوع به‌طور ذاتی خاص یا حساس برای وی (آن‌ها) است [۱]. دامنه حریم خصوصی تا حدودی با امنیت هم‌پوشانی دارد؛ به‌طوری که می‌تواند مفاهیم استفاده مناسب و نیز حفاظت از اطلاعات را نیز در بر گیرد. عدم نقض غیرقانونی حریم خصوصی توسط دولت‌ها، شرکت‌ها و یا افراد بخشی از قوانین حفظ حریم خصوصی در بسیاری از کشورها است [۲] و در برخی موارد، در قانون اساسی کشورها نیز آمده است و چون این قوانین ذیل حقوق بشر تعریف می‌گردند، معمولاً قوانین سخت‌گیرانه‌ای نیز به‌شمار می‌آیند [۳].

### ۲.۱ اهداف حفاظت از داده‌های عمومی

برای حفاظت از داده‌ها سه هدف اصلی را می‌توان متصور بود [۴]:

۱. ارائه و تدوین آیین‌نامه و قوانینی برای حمایت از اشخاص حقیقی در رابطه با پردازش داده‌های شخصی و نیز قوانینی در خصوص حرکت آزاد داده‌های شخصی<sup>۱</sup>.
۲. حمایت از حقوق و آزادی‌های اساسی اشخاص حقیقی به‌ویژه در حوزه حمایت از داده‌های شخصی آن‌ها.

<sup>۱</sup>Free Movement of Personal Data



۳. کمک به نقل و انتقال آزاد اطلاعات شخصی بدون محدودیت و با رعایت مباحث مرتبط با حمایت از اشخاص حقیقی و نیز توجه به پردازش داده‌های شخصی.

باید به این موضوع توجه داشت که ساز و کارهای متنوعی برای این موضوع در کشورهای مختلف به کار گرفته شده است که بخشی از آن‌ها معرف خروجی‌های متنوع و کاربردی شده در سطح آزمایشگاه‌های معتبر و آکادمیک بوده که می‌تواند در شناسایی راهکارها و فناوری‌های لازم برای حفاظت از داده‌های عمومی بسیار مؤثر باشد.

### ۳.۱ دامنه کاربرد قوانین و مقررات حفاظت از داده‌ها

در اسناد مختلف در خصوص دامنه کاربرد مقررات حفاظت از داده‌ها، عناوین متعددی اشاره شده است که فصل مشترک آن‌ها را می‌توان در موارد زیر خلاصه کرد [۵]:

الف) هر نوع پردازش داده‌های شخصی، با استفاده از روش‌های خودکار و یا غیرخودکار که تمام یا بخشی از یک سامانه بوده و تمام یا بخشی (به‌طور کامل یا جزئی) از داده‌های شخصی را مورد پردازش قرار دهد.

ب) برای پردازش داده‌های شخصی توسط نهادها، ارگان‌ها و سازمان‌های خاص لازم است تا آیین‌نامه‌های جداگانه‌ای طراحی و اعمال شده و با مقررات کلی حفاظت از داده‌ها سازگار شود.

ج) لازم است برای ارائه‌دهندگان خدمات واسطه‌ای<sup>۲</sup> نیز آیین‌نامه‌های جداگانه‌ای طراحی و ارائه شده و با مقررات کلی حفاظت از داده‌ها سازگار شود.

البته قوانین و مقررات در این حوزه در برخی از موارد استثناء نیز قائل شده‌اند که از مهم‌ترین آن‌ها به شرح زیر هستند [۶]:

- چنانچه فعالیتی خارج از چارچوب‌های جغرافیایی شمول مقررات باشد.
- توسط سازمان‌ها و نهادهایی انجام گیرد که از سوی قانون مجوز آن را دارا می‌باشند.
- توسط اشخاص با ویژگی‌های خاص و برای مصارف صرفاً شخصی و محدود انجام شود.
- توسط مقامات ذی‌صلاح و به‌منظور پیشگیری، تحقیق، کشف یا پیگرد قانونی از جرائم کیفری یا اجرای مجازات‌های کیفری - از جمله حراست و جلوگیری از تهدیدات برای امنیت ملی و عمومی - انجام شود.

<sup>2</sup>Intermediary Service Providers

## ۲ تعاریف و مفاهیم مرتبط با حفاظت از داده‌ها

بررسی منابع و مراجع مختلف، محقق را به مجموعه‌ای از مفاهیم کلیدی در فضای مقررات عمومی حفاظت از داده‌ها می‌رساند که در ادامه مورد بررسی قرار خواهند گرفت.

**اطلاعات شخصی:** «داده‌های شخصی»<sup>۳</sup> به معنای هرگونه اطلاعات مربوط به یک شخص<sup>۴</sup> مشخص یا قابل شناسایی<sup>۵</sup> (موضوع داده) است [۷]. شخص حقیقی قابل شناسایی معرف فردی است که می‌تواند به‌طور مستقیم یا غیرمستقیم، به ویژه با مراجعه به شناسه‌ای - نظیر نام، شماره شناسایی، داده‌های مکانی، شناسه آنلاین یا یک یا چند عامل خاص جسمی یا فیزیولوژیکی، هویت ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی - مربوط به خود را احراز هویت نماید. این تعریف گسترده و کاملاً فراگیر است که شامل موارد زیر است:

الف) هرگونه اطلاعات مربوط به یک شخص مشخص (یعنی اطلاعات شخصی شده).

ب) اطلاعات مربوط به شخصی که بر اساس انواع شناسه‌ها قابل شناسایی باشد.

ارائه این تعریف برای افراد «مشخص» نسبتاً ساده است. به عنوان مثال، چنانچه شخصی گواهی‌نامه رانندگی، مجوز کار، استعلام سوابق کیفری و... را داشته باشد، یک هویت مشخص مانند مدرسه، کارفرما یا صاحبخانه فرد (به عنوان کنترل کننده) به راحتی می‌تواند آن را شناسایی کند. بدین ترتیب هر نوع داده‌ای از شما، مثل تاریخ تولد، آدرس، شماره تلفن، حقوق و دستمزد و هزینه اجاره خانه شما، داده‌های شخصی محافظت شده تحت GDPR را تشکیل می‌دهند.

**پردازش:** پردازش به معنای مجموعه‌ای از عملیات است که بر روی داده‌های شخصی انجام می‌شود. جمع‌آوری، ضبط، سازماندهی، ساختاردهی، ذخیره‌سازی، سازگاری یا تغییر، بازیابی، نتیجه‌گیری، استفاده، افشاء از طریق انتقال، انتشار، تراز یا ترکیب، ایجاد محدودیت، پاک کردن و یا از بین بردن از عمده عملیات رایج پردازشی محسوب می‌شوند.

**محدودسازی پردازش:** این مفهوم به معنی علامت‌گذاری بر روی داده‌های شخصی ذخیره شده با هدف محدود کردن پردازش آن‌ها در آینده است.

**کنترل کننده:** این مفهوم به معنای شخص حقیقی یا حقوقی، مرجع عمومی، سازمان یا یک نهاد دیگر است که به تنهایی یا به‌طور مشترک با دیگران، اهداف و ابزارهای پردازش داده‌های شخصی را تعیین می‌کند. در مواردی که اهداف و وسایل پردازش براساس قانون کشور تعیین شده باشد، لازم است کنترل کننده خود را با معیارهای مشخص شده تطبیق دهد [۱۰].

<sup>3</sup>Personal Data

<sup>4</sup>Natural Person

<sup>5</sup>Identifiable

**پردازش‌گر:** این مفهوم به معنای یک شخص حقیقی یا حقوقی، مقامات دولتی، سازمان یا یک نهاد دیگر است که داده‌های شخصی را از طرف کنترل‌کننده پردازش می‌کند [۱۰].

**شخص ثالث:** این مفهوم به معنای شخص حقیقی یا حقوقی، مرجع عمومی، نمایندگی یا ارگان‌های دیگر (به غیر از موضوع داده، کنترل‌کننده و پردازش‌گر) و اشخاصی است که تحت اختیار مستقیم کنترل‌کننده و یا پردازش‌گر، مجاز به پردازش داده‌های شخصی هستند [۱۱].

**رضایت:** رضایت<sup>۶</sup> از موضوع داده‌ها به معنای هرگونه نشان دادن آزادانه و آگاهانه و بدون ابهام در مورد استفاده از داده‌ها است که توسط فرد با یک بیانیه یا با امضای یک تأییدیه روشن، توافقی را برای پردازش داده‌های شخصی فرد ایجاد می‌کند.

**داده‌های ژنتیکی:** این مفهوم به معنی داده‌های شخصی مربوط به ویژگی‌های ژنتیکی ارثی یا اکتسابی یک فرد حقیقی است که اطلاعات خاصی را در مورد فیزیولوژی یا سلامتی - به‌ویژه از تجزیه و تحلیل نمونه بیولوژیکی - آن شخص ارائه می‌دهد [۱۱].

**داده‌های بیومتریک:** این مفهوم به معنای داده‌های شخصی ناشی از پردازش فنی خاص مربوط به خصوصیات جسمی، فیزیولوژیکی یا رفتاری یک شخص حقیقی است که به شناسایی منحصر به فرد آن شخص - مانند تصاویر صورت یا داده‌های انگشت‌نگاری<sup>۷</sup> - منجر می‌شود.

**اطلاعات مربوط به سلامتی:** این مفهوم به معنای داده‌های شخصی مربوط به سلامت جسمی یا روانی یک شخص - از جمله خدمات مراقبت‌های بهداشتی ارائه‌شده به شخص - است که اطلاعاتی را پیرامون وضعیت سلامتی وی نشان می‌دهد.

**مرکز اصلی تأسیس:** مرکز اصلی تأسیس<sup>۸</sup> در مورد کنترل‌کننده‌ها و پردازش‌گرها بدین معنی است:

الف) در مورد یک کنترل‌کننده با استقرار در بیش از یک کشور و دارای محل استقرار در کشور، محل مدیریت مرکزی آن در کشور مرجع ملاک تصمیم و مسئول در مورد اهداف و ابزارهای پردازش داده‌های شخصی خواهد بود، مگر اینکه آن را به یکی از شعب خود واگذار کرده باشد که در این صورت نیز مسئول تصمیمات، شعبه اصلی خواهد بود [۱۲].

ب) در مورد یک پردازنده با استقرار در بیش از یک کشور و دارای محل استقرار در کشور، محل مدیریت مرکزی آن در کشور مرجع ملاک تصمیم و مسئول در مورد اهداف و ابزارهای پردازش داده‌های شخصی خواهد بود، مگر اینکه آن را به یکی از شعب خود واگذار کرده باشد که در این صورت نیز مسئول تصمیمات، شعبه اصلی خواهد بود.

<sup>6</sup>Consent

<sup>7</sup>Dactyloscopy

<sup>8</sup>Main Establishment

**بناگاه اقتصادی:** این مفهوم به معنای شخص حقیقی یا حقوقی است که - صرف نظر از شکل قانونی آن - از طریق مشارکت و یا ایجاد انجمن‌هایی ایجاد می‌شود که به‌طور منظم در یک فعالیت اقتصادی مشغول فعالیت اقتصادی هستند.

**گروه شرکت:** مفهوم گروه شرکت<sup>۹</sup> به معنای یک شرکت کنترل کننده و شرکت‌های تحت حمایت و متعهد به آن می‌باشد [۱۳].

**مرجع نظارت:** این مفهوم به معنای یک مرجع عمومی مستقل است که به موجب قانون تأسیس شده و وظیفه نظارت بر اجرای قوانین و مقررات حفاظت از داده‌ها را برعهده دارد.

**مرجع نظارتی مرتبط:** این مفهوم به معنای یک مرجع نظارتی است که دغدغه اصلی آن به دلایل زیر پردازش اطلاعات شخصی در موارد خاص است:

الف) کنترل کننده یا پردازشگر در قلمرو کشور دیگری تأسیس شده است.

ب) تعداد افراد قابل ملاحظه‌ای تحت تأثیر پردازش و کنترل داده در یک شرکت خاص باشند.

**پردازش مرزی:** پردازش مرزی<sup>۱۰</sup> در شرایط زیر معنی می‌شود:

a) پردازش داده‌های شخصی که در چارچوب فعالیت‌های یک شرکت یا بناگاه اقتصادی که خارج از کشور فعالیت می‌کند و یا علاوه بر فعالیت در کشور، در سایر کشورها نیز فعال است.

b) پردازش داده‌های شخصی که در قالب یک کنترل کننده و یا پردازشگر در داخل کشور فعالیت می‌کند ولی فعالیت‌های آن تأثیر قابل ملاحظه‌ای بر فعالیت‌های خارج از کشور دارد.

**اعتراض مربوط و مستدل:** این مفهوم به معنی اعتراض به تصمیماتی است که منجر به نقض قوانین و آیین‌نامه‌ها در حوزه حفاظت از داده‌ها، تداخل مقررات این حوزه با سایر حوزه‌ها و یا اختیارات پیش‌بینی شده در رابطه با کنترل کننده‌ها و پردازش‌گرها و نحوه فعالیت آن‌ها می‌شود.

**خدمات جامعه اطلاعاتی:** خدمات در جامعه اطلاعاتی یعنی هر خدمتی که به‌طور معمول در یک بناگاه اقتصادی برای سود / پاداش انجام می‌شود و از راه دور، از طریق وسایل الکترونیکی و به درخواست فرد دریافت کننده خدمات انجام می‌شود [۱۴].

در اینجا «از راه دور» بدان معنی است که این خدمات در اکثر موارد بدون حضور همزمان طرفین ارائه می‌شود. همچنین «از طریق الکترونیکی» به این معنی است که این سرویس در ابتدا با استفاده از تجهیزات الکترونیکی برای پردازش و ذخیره‌سازی داده‌ها در مقصد دریافت می‌شود و به‌طور کامل از طریق رابط سیمی،

<sup>9</sup>Group of Undertakings

<sup>10</sup>Cross-Border Processing

از طریق رادیو، به صورت نوری، الکترومغناطیسی و یا با هر وسیله دیگری منتقل و دریافت می‌شود. علاوه بر موارد فوق، «در صورت درخواست فرد دریافت‌کننده خدمات» نیز بدان معنی است که این خدمات از طریق انتقال داده به درخواست فردی ارائه می‌شود.

**سازمان بین‌المللی:** این مفهوم به معنای سازمان و نهادهای فرعی آن است که براساس قوانین بین‌المللی عمومی فعالیت می‌کند و یا هر نهادی که توسط دو یا چند کشور بوجود آمده باشد یا براساس قوانین آن‌ها ایجاد شده باشد.

**موضوع داده:** موضوع داده<sup>۱۱</sup> به هر فرد مشخصی اطلاق می‌شود که به‌طور مستقیم یا غیرمستقیم از طریق یک شناسه - نظیر نام، شماره شناسنامه، داده‌های محل یا از طریق فاکتورهای اختصاصی جسمی، فیزیولوژیکی، ژنتیکی، روانی، اقتصادی، فرهنگی و یا هویت اجتماعی - شناسایی می‌شود [۱۴]. موضوع و افراد داده می‌توانند مشتریان، پیمانکاران، فروشندگان و حتی کارمندان یک سازمان باشند.

**دسته‌بندی‌های ویژه از اطلاعات شخصی:** برخی از داده‌ها از حساسیت‌های خاصی در استفاده و پردازش برخوردار هستند که در اینجا دسته‌بندی شده‌اند و محافظت از آن‌ها نیز تابع شرایط خاصی خواهد بود. به عبارت دیگر، انواع داده‌های شخصی زیر ممکن است به محافظت خاصی نیاز داشته باشند:

- نژاد و قومیت
- عقاید سیاسی، مذهبی یا فلسفی (از جمله عضویت در اتحادیه‌ها)
- سلامتی، زندگی فردی و گرایش جنسی
- داده‌های ژنتیکی و بیومتریک (به‌منظور شناسایی منحصر به فرد)

البته برای استفاده از این داده‌ها نیز شرایط خاصی را می‌توان طراحی کرد که رضایت شخصی، استفاده در مراحل شغلی قانونی، استفاده در شرایط پزشکی خاص و نیز استفاده برای تحقیق و توسعه از جمله این موارد هستند.

**رضایت در استفاده از داده:** «رضایت» از پردازش و بهره‌برداری از داده‌ها به‌معنای هرگونه نشان دادن آزادانه و آگاهانه و بدون ابهام در مورد استفاده از داده‌ها است که توسط فرد با یک بیانیه یا با امضای یک تأییدیه روشن، توافقی را برای پردازش داده‌های شخصی فرد ایجاد می‌کند.

<sup>11</sup>Data Subject

**بهره‌گیری مشروع از داده:** یکی از مفاهیم اساسی در پردازش داده‌ها، بهره‌برداری مشروع<sup>۱۲</sup> است که در بسیاری از موارد با ابهام مواجه می‌شود. برای این منظور در اینجا توضیح داده می‌شود که پردازش داده‌های فرد فقط در صورتی مجاز است که حداقل یکی از موارد زیر اعمال شود:

۱. موضوع داده به پردازش اطلاعات شخصی خود برای یک یا چند هدف خاص رضایت داده باشد.
۲. پردازش داده‌های فرد برای انجام امور قراردادی و یا پیمانکاری که سوابق داده‌ها در آن اهمیت دارد و یا برای انجام مراحل قبل از ورود به قرارداد لازم باشد.
۳. پردازش داده‌ها برای سنجش رعایت تعهد قانونی ضروری باشد.
۴. پردازش و بهره‌گیری از داده‌های فرد برای محافظت از منافع حیاتی وی و یا شخص حقیقی دیگری ضروری باشد.
۵. پردازش و بهره‌گیری از داده‌ها برای انجام اموری که به نفع مردم باشد و یا جزو وظایف رسمی کنترل‌کننده و بهره‌بردار باشد، ضروری است.
۶. پردازش و بهره‌گیری از داده‌ها برای اهداف و منافع مشروعی که توسط کنترل‌کننده و بهره‌بردار و یا شخص ثالث دنبال می‌شود، ضروری باشد.

**مرجع محافظت از داده:** مراجع محافظت از داده<sup>۱۳</sup> معرف مقام رسمی مستقلی هستند که از طریق اختیارات تحقیق و تصحیح، بر اعمال قانون حمایت از داده‌ها نظارت می‌کنند. آن‌ها مشاوره تخصصی را در مورد مسائل مربوط به حمایت از داده‌ها ارائه می‌دهند و به شکایاتی که ممکن است قانون را نقض کرده باشند، رسیدگی می‌کنند. مرجع حفاظت از داده تضمین می‌کند که داده‌های شخصی به درستی نگهداری و با دقت محافظت می‌شوند، و نیز حفظ حریم خصوصی آینده‌ی کاربران را نیز تضمین می‌کند.

**مدیر حفاظت از داده:** کنترل‌کننده و پردازش‌گر داده‌ها باید از یک نفر به عنوان «مدیر حفاظت از داده»<sup>۱۴</sup> استفاده کنند. بهره‌گیری از این مدیر در موارد زیر ضروری است:

- الف) پردازش داده‌ها توسط یک مقام یا نهاد عمومی انجام می‌شود.
- ب) فعالیت‌های اصلی کنترل‌کننده یا پردازش‌گر شامل عملیات پردازش باشد که به دلیل ماهیت، دامنه و یا اهداف آن‌ها، نیاز به نظارت منظم بر داده‌ها در مقیاس بزرگ دارند.
- ج) فعالیت‌های اصلی کنترل‌کننده یا پردازش‌گر شامل پردازش داده‌های شخصی در مقیاس وسیعی از دسته‌بندی‌های خاص و مربوط به محکومیت‌ها و جرائم کیفری باشد.

<sup>12</sup>Legitimate Interest

<sup>13</sup>Data Protection Authority

<sup>14</sup>Data Protection Officer



**نقض داده:** نقض داده‌ها<sup>۱۵</sup> معرف یک مسئله امنیتی است که منجر به تخریب تصادفی یا غیرقانونی، از بین رفتن، تغییر، افشای غیرمجاز یا دسترسی به داده‌های محافظت‌شده می‌شود. اساساً هر چیزی که بر محرمانه بودن، صحت یا دسترسی‌پذیری داده‌ها تأثیر بگذارد، نقض داده خوانده می‌شود. در برخی از قوانین حفاظت از داده‌ها، سازمان‌ها از نظر قانونی موظف هستند تا ظرف مدت زمان خاصی از نقض داده‌ها اطلاع یافته و آن‌را به مرجع حفاظت از داده‌ها گزارش دهند [۱۴].

### ۳ مقررات و قوانین در ایران در حوزه حفاظت از داده‌ها

در بسیاری از کشورها از جمله در ایران قوانین و مقررات خاصی برای حفاظت از اطلاعات و داده‌های فردی و عمومی تدوین، طراحی و ارائه شده است که لازمه اجرای آن ایجاد امکانات فناورانه در جهت پیشگیری، رصد و پایش و اقدام متناسب در حوزه حفاظت از داده‌ها است.

چنین شرایطی توجه تصمیم‌سازان و سیاست‌گذاران دولتی را بیش از پیش به موضوع حفاظت از داده‌ها معطوف داشته است و دولت‌ها نیز نقش مهمی در این روند ایفا خواهند کرد. دولت به عنوان یک تسهیل‌کننده به ایجاد یک محیط مساعد برای بازیگران صنعت - از طریق اصلاحات رگولاتوری، ایجاد مهارت و ظرفیت‌سازی، استانداردسازی، توسعه قابلیت همکاری، زیرساخت‌ها و نیز اقدامات امنیتی - می‌پردازد [۱۰]. در همین راستا همکاری صنعت و دولت برای حصول اطمینان از ایجاد یک محیط مساعد برای توسعه مناسب و کارآمد قوانین و مقررات حفاظت از داده و اجرای آن امری اجتناب‌ناپذیر است. در جدول ۱ برخی از قوانین و مقررات ایران اشاره شده که با این حوزه ارتباط دارند.

از این‌رو بررسی مجموعه راهبردها و گام‌های کشورهای پیشرو و در حال توسعه و نیز استخراج اقدامات ضروری برای توسعه قوانین و مقررات در این حوزه ضروری به نظر می‌رسد تا از این طریق دید جامعی نسبت به آنچه که دولت‌ها در کشورهای مختلف انجام می‌دهند به دست آید [۶]. البته مطالعه تجارب مفید و انتقال خط‌مشی‌ها و راهبردهای کاربردی‌پذیر برای کشور صرفاً از طریق کپی‌برداری امکان‌پذیر نیست؛ چرا که اصول حاکم بر تصمیمات در سطح ملی و شرایط سیاسی، اقتصادی، اجتماعی و فناورانه از یک کشور به کشور دیگر متفاوت است. همین امر موجب گردیده تا کشورهای مختلف رویکردهای بعضاً متفاوتی را در مواجهه با این پدیده اتخاذ نمایند.

### ۴ کلیات تحقیق

#### ۱.۴ ضرورت انجام تحقیق

باتوجه به مجموعه موارد فوق، بدون داشتن درک و آگاهی از خط‌مشی‌ها و راهبردهای توسعه قوانین و مقررات حفاظت از داده‌ها در کشورهای توسعه‌یافته و در حال توسعه (نظیر جمهوری اسلامی ایران) احتمال تحمیل هزینه‌های فرصت به تصمیم‌سازان این حوزه در کشور افزایش می‌یابد. بنابراین نیاز است تا یک چارچوب

<sup>15</sup>Data Breach

## جدول ۱: برخی از قوانین و مقررات مرتبط با حفاظت از داده‌ها در ایران

ردیف	عنوان	موضوع کلیدی مطرح شده
۱	قانون انتشار و دسترسی آزاد به اطلاعات	بند «ب» ماده ۱ قانون - اطلاعات شخصی معرف اطلاعات فردی نظیر نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور است.
۲	ماده ۱۳۰ قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (۱۳۸۳)	لایحه «حفظ و ارتقاء حقوق شهروندی و حمایت از حریم خصوصی افراد، در راستای اجرای اصل بیستم (۲۰) قانون اساسی جمهوری اسلامی ایران» توسط قوه قضائیه تدوین می‌شود.
۳	مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای مصوب شورای عالی انقلاب فرهنگی (۱۳۸۰)	وظایف ISPها دربرگیرنده حریم خصوصی کاربران و تعیین جرایم افشاء است.
۴	قانون برنامه پنج‌ساله پنجم توسعه جمهوری اسلامی ایران (۱۳۹۴-۱۳۹۰)	تبصره ماده ۲۰۶ - عدم افشاء اطلاعات بند الف ماده ۳۵ - صیانت از اطلاعات پزشکی
۵	بند ۱ منشور حقوق شهروندی	تفکیک حریم عمومی از حریم خصوصی و نهادینه کردن خدمت در هر دو حریم که متأسفانه جزئیاتی پیرامون آن اشاره نشده است.
۶	بند «ب» اساسنامه سازمان بیمه سلامت ایران	تشکیل و صیانت از پرونده الکترونیکی سلامت افراد مدنظر است.
۷	بند ۴ ماده ۱۲ دستورالعمل تشکیل بانک اطلاعات هویت ژنتیک ایران	دستورالعمل حفاظت از اطلاعات ژنتیکی در آزمایشگاه‌ها را مدنظر قرار داده است.
۸	مصوبه شورای عالی اداری در خصوص منشور حقوق شهروندی (۱۳۹۵)	تمهیدات فنی و قانونی لازم را برای حفظ حریم خصوصی افراد و تأمین امنیت داده‌های شخصی آنان توسط قوه قضائیه مدنظر قرار گیرد.

مفهومی برای شناسایی و بیان گزینه‌های راهبردی کشور در مواجهه با این حوزه ارائه شود. براین اساس، ضرورت‌های انجام تحقیق حاضر به شرح زیر هستند:

- درک بهتر رهیافت‌ها و راهبردهای مرتبط با توسعه قوانین و مقررات حفاظت از داده‌ها در کشورهای مختلف جهان
- تصمیم‌سازی در حوزه توسعه قوانین و مقررات حفاظت از داده‌ها در کشور مبتنی بر درس‌های آموخته و بهترین تجارب منتشر شده در سایر کشورها
- ارائه یک سازوکار پشتیبان تصمیم‌گیری جهت شناسایی و تبیین راهبردهای توسعه قوانین و مقررات حفاظت از داده‌ها در کشور

## ۲.۴ سؤالات تحقیق

بر اساس مجموعه موارد مطرح‌شده، سؤال اصلی این پژوهش عبارت است از:

- چارچوب مفهومی برای شناسایی و تبیین راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها در کشور دارای چه ابعادی است؟
- پاسخ به سؤال فوق مستلزم پاسخگویی به سؤالات فرعی زیر است:

- ابعاد / گزینه‌های راهبردی توسعه قوانین و مقررات حفاظت از داده‌ها در سایر کشورها چیست؟
- چارچوب مفهومی مناسب برای شناسایی و تبیین راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها در کشور کدام است؟
- اهمیت هر یک از ابعاد / گزینه‌های راهبردی در چارچوب پیشنهادی به چه میزان است؟

## ۳.۴ اهداف تحقیق

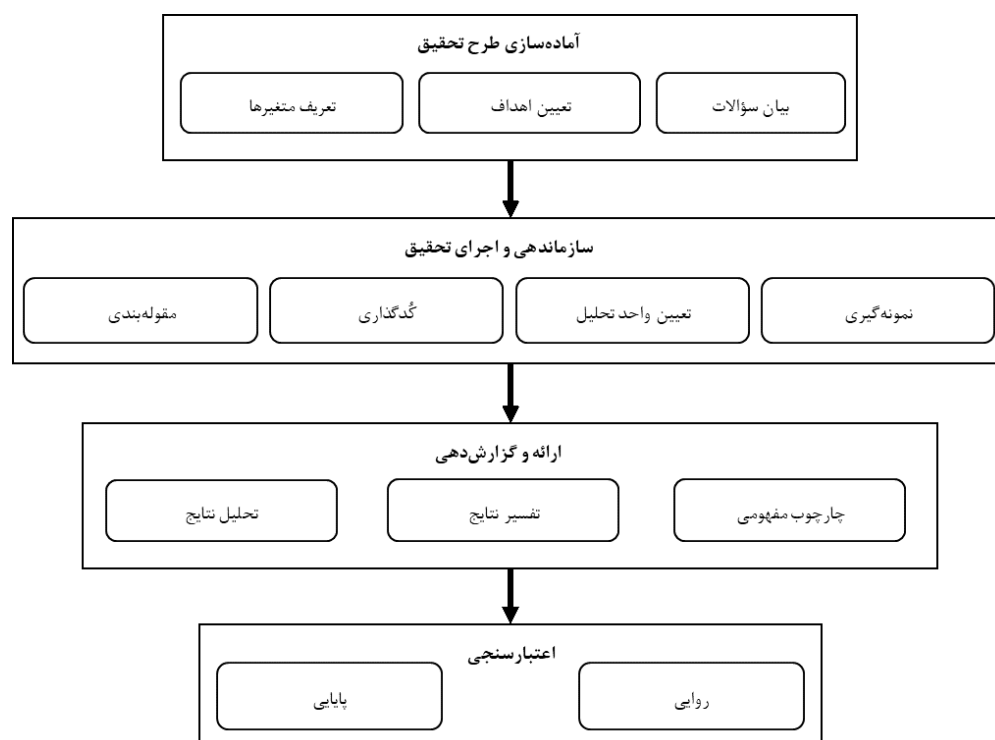
هدف اصلی در این پژوهش مطالعه مقایسه‌ای راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها باهدف «ارائه یک چارچوب مفهومی برای شناسایی و تبیین راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها» است. اهداف فرعی شامل موارد ذیل می‌باشد:

- بررسی رهیافت و نگرش کشورهای مختلف نسبت به قوانین و مقررات حفاظت از داده‌ها
- شناسایی و تحلیل ابعاد / گزینه‌های راهبردی توسعه قوانین و مقررات حفاظت از داده‌ها در سایر کشورها
- بررسی و انتخاب یک چارچوب کاربردپذیر جهت شناسایی و تبیین راهبردهای ملی توسعه قوانین و مقررات حفاظت از داده‌ها مبتنی بر درس‌های آموخته

## ۵ چارچوب پیشبرد تحقیق

محقق در راستای ارائه یک چارچوب مفهومی اقدامات کلان توسعه قوانین و مقررات حفاظت از داده‌ها نسبت به بررسی مقایسه‌ای راهبردهای منطقه‌ای، ملی و بخشی این حوزه در قالب یک چارچوب نظام‌مند تحقیق اقدام نموده است. این چارچوب در قالب شکل ۱.۵ ارائه شده است [۱۵].

در گام اول و براساس مسئله تحقیق تعریف‌شده، محقق به بیان اهداف، سوالات و متغیرهای تحقیق می‌پردازد. لازم به ذکر است که متغیرهای تحقیق حاضر همان راهبردها و اقدامات کلان ملی توسعه قوانین و مقررات حفاظت از داده‌ها در کشورهای مختلف هستند. در گام دوم تحقیق، نمونه‌گیری (براساس روش‌های نمونه‌گیری هدفمند و در دسترس)، تعیین واحد تحلیل و زمینه (براساس کلمات، عبارات و مضامین معرف گزاره‌های راهبردی هدف تحقیق) و نیز گدگذاری و مقوله‌بندی (براساس دستورالعمل گدگذاری دو مرحله‌ای باز و مبتنی بر رویکرد استقرایی و داده‌رانده) در دستورکار محقق قرار می‌گیرد. در گام سوم، محقق نسبت به ارائه چارچوب مفهومی پیشنهادی (براساس گدگذاری و مقوله‌بندی برخاسته از داده) و نیز تحلیل و بررسی یافته‌ها (براساس تحلیل فراوانی کدها و مقوله‌ها، تحلیل‌های درون و بین موردی و نیز بررسی‌های مقایسه‌ای) می‌پردازد. در گام چهارم نیز محقق به بررسی اعتبار چارچوب پیشنهادی خواهد پرداخت.



شکل ۱: چارچوب پیشبرد تحقیق

## ۱.۵ روش تحقیق

در این پژوهش از روش تحلیل محتوای کیفی استفاده شده است که یکی از روش‌های انجام پژوهش کیفی است. تحلیل محتوای کیفی در جایی که تحلیل کمی به محدودیت‌هایی می‌رسد، نمود می‌یابد. بنابراین تحلیل محتوای کیفی را می‌توان روش تحقیقی برای تفسیر ذهنی محتوایی داده‌های متنی - از طریق فرایندهای طبقه‌بندی نظام‌مند گُذبندی و تم‌سازی یا طراحی الگوهای شناخته‌شده - دانست [۱۵].

با تحلیل کیفی می‌توان یک رویکرد تجربی روش‌شناسانه و کنترل‌شده مرحله به مرحله را با رعایت عناصر مورد مطالعه در نظر گرفت. عینیت نتایج به‌وسیله وجود یک فرآیند گُذبندی نظام‌مند تضمین می‌شود. این روش، تیم و الگوهای که آشکار و یا پنهان هستند را به‌صورت محتوای آشکار می‌آزماید [۱۶].

هم‌اکنون سه رویکرد: سنتی (متعارف) [۱۶]، هدایت‌شده [۱۷]، جامع [۱۸] برای کاربرد تحلیل محتوا مطرح است. در تحلیل محتوای به روش متعارف طبقات به‌گونه مستقیم از متن داده‌ها استخراج می‌شوند. ستون فقرات تحقیق حاضر مبتنی بر روش تحلیل محتوای متعارف بنا نهاده شده است. در این روش، محقق به دنبال تفسیر ذهنی محتوای متنی از طریق فرآیندهای طبقه‌بندی نظام‌مند، گُذگذاری، مقوله‌بندی و نیز ارائه یک چارچوب مفهومی شناخته‌شده است [۱۸]. پیش‌فرض محقق پیرامون استفاده از این روش تحقیق، جدید بودن پدیده مورد مطالعه (یعنی قوانین و مقررات حفاظت از داده‌ها) و محدود بودن منابع نظری پیرامون آن است. در این شرایط، محقق از به‌کارگیری مقوله‌های از پیش تعریف‌شده پرهیز می‌نماید و به دنبال به‌کارگیری رویکردی داده‌رانده برای شناسایی مقوله‌ها است. براساس روش پایه انتخابی (تحلیل محتوای متعارف)، محقق مجموعه‌ای از فعالیت‌های مستقل اما به‌هم‌پیوسته را در قالب چهار گام برای پیشبرد تحقیق حاضر پیش‌بینی نموده است. این گام‌ها در قالب شکل ارائه شده است.

البته محقق برای غنابخشی به یافته‌های تحقیق از مجموعه‌ای از روش‌ها و تکنیک‌های تحقیق در مرحله سوم (ارائه و گزارش‌دهی) استفاده نموده است. در این گام و برای تحلیل یافته‌های تحقیق - مبتنی بر چارچوب مفهومی پیشنهادی - از تکنیک‌های بررسی درون‌موردی و بین‌موردی و نیز بررسی مقایسه‌ای راهبردی استفاده شده است. در بررسی مقایسه‌ای راهبردی، محقق به دنبال هدف‌هایی فراتر از توصیف بوده و این کار متضمن دآوری و ارزش‌گذاری آزمودنی‌ها است. در این نگاه، محقق برای بهبود یافته‌ها از بررسی مقایسه‌ای می‌تواند با هدف تصمیم‌گیری در سطح ملی و بخش بهره‌برداری نماید [۱۵]. علاوه بر این، در تحلیل‌های درون‌موردی و بین‌موردی - مبتنی بر ساختار حاکم بررسی موردی چندگانه مطرح‌شده در تحقیق حاضر - محقق به دنبال مقایسه دیدگاه‌های حاکم در کشورهای مختلف و نیز دلیل پرداخت یا عدم پرداخت به برخی از نمونه‌های موردی مبتنی بر شرایط آن کشور است [۱۵].

<sup>16</sup>Conventional

<sup>17</sup>Directed

<sup>18</sup>Summative

## ۲.۵ جامعه و نمونه آماری تحقیق

جامعه آماری تحقیق حاضر متشکل از گزارش‌های منطقه‌ای (قاره‌ای و بین قاره‌ای)، ملی و بخشی منتشر شده در زمینه راهبردهای توسعه قوانین و مقررات حفاظت از داده‌ها است. محقق برای تأمین جامعیت تحقیق حاضر نسبت به انتخاب هدفمند اسناد فوق اقدام نموده است؛ به گونه‌ای که کلیه اسناد راهبردی (منطقه‌ای، ملی و بخشی) مشتمل بر ۳۸ نمونه موردی دسترس‌پذیر تا سال ۲۰۲۱ در قالب روش سرشماری جمع‌آوری و مورد تحلیل عمیق قرار گرفته‌اند. علاوه بر این، جهت سنجش روایی اسناد مورد بررسی پیل خبرگی ۶ نفره با حضور اعضای هیات علمی و خبرگان حوزه فناوری در پژوهشگاه ارتباطات و فناوری اطلاعات، دانشگاه تهران، دانشگاه شهید بهشتی و دانشگاه علم و صنعت - که در مجموع سابقه انجام ۶ پروژه راهبردی، کاربردی و توسعه‌ای در زمینه قوانین و مقررات حفاظت از داده‌ها طی ۳ سال گذشته را داشته‌اند - تشکیل گردید.

## ۳.۵ روش گردآوری و تحلیل داده‌های تحقیق

واحد تحلیل در این پژوهش، کل متن اسناد شناسایی شده است. پس از انتخاب واحد تحلیل، به تدوین مقوله‌ها و زیرمقوله‌های اسناد پرداخته شده و متغیرهای پژوهش از این طریق شناسایی شده‌اند. جهت تحلیل اسناد مقوله، اختصاص داده شده است. هر یک از مقوله‌ها دارای یک یا چند واحد است. با شناسایی راهبردهای کلیدی در متن اسناد و گدگذاری داده‌ها امکان بررسی و تحلیل راهبردها فراهم شده است. در این روش دو عنصر اصلی مطرح هستند: واحد تحلیل و مقوله تحلیل.

واحد تحلیل معرف کوچک‌ترین جزء پیکره‌ی متن است که برای رسیدن به هدف تحقیق، اندازه‌گیری و شمارش می‌شود. واحد تحلیل می‌تواند در برگیرنده کلمه، جمله، پاراگراف و ... باشد که این واحدها وابسته به نوع متن و هدف پژوهش انتخاب می‌شوند.

هنگامی که واحدها معین شدند باید مشخص گردد که واحدهای استخراج و شمارش شده چگونه دسته‌بندی می‌شوند. عناوین این دسته‌بندی‌ها معرف مقوله تحلیل هستند. در نهایت واحدها براساس مقوله‌های تحلیل دسته‌بندی می‌شوند تا مراحل شمارش و تحلیل اطلاعات صورت گیرد [۱۵].

## ۶ بررسی اقدامات راهبردی تدوین مقررات حفاظت از داده‌های عمومی در واحدهای تحلیل

همانطور که پیش از این اشاره شد، واحد تحلیل در این پژوهش کلیه اسناد راهبردی (منطقه‌ای، ملی و بخشی) مشتمل بر ۳۸ نمونه موردی دسترس‌پذیر تا سال ۲۰۲۱ است. در ادامه و به منظور بررسی تفصیلی موضوع نسبت به ارائه خلاصه کلی از اهداف کلیدی و برنامه‌های پیش‌بینی شده در ۵ نمونه منتخب اقدام می‌گردد.

### ۱.۶ ایالات متحده آمریکا

ایالات متحده آمریکا یکی از معدود کشورهای جهان است که نهاد دولتی برای محافظت از داده‌های فدرال ندارد. با این وجود ایالات متحده رهبر جهانی در زمینه حفظ حریم خصوصی در جهان از جنس کارکردی



و ساختاری محسوب می‌شود. قانون گزارش اعتباری منصفانه<sup>۱۹</sup>، مصوب سال ۱۹۷۰ در آن زمان به عنوان اولین قانون مدرن برای حفظ حریم خصوصی، پاسخی به اتوماسیون روبه‌رشد داده‌های شخصی در ایالات متحده تلقی شد.

اما امروز اروپا در حمایت از داده‌های مصرف‌کننده از ایالات متحده پیشی گرفته و آیین‌نامه حمایت از داده‌های عمومی که از سال ۲۰۱۸ به اجرا در آمد، حقوق اساسی افراد را تقویت می‌کند و مصرف‌کنندگان را مجدداً بر سرنوشت داده‌های شخصی خود مسلط می‌کند و این حقوق را به اشخاص می‌دهد که در صورت نقض (در مدت ۷۲ ساعت) اطلاع‌رسانی کنند و از حقوق مصوب در این قانون بهره‌مند گردند [۱۹]. در این شرایط، در کشور آمریکا قوانین متعددی تدوین و ارائه شده است که در جدول ۲ به برخی از آن‌ها اشاره می‌شود.

## ۲.۶ اقدامات کانادا

کانادا مدت‌هاست که با تصویب «قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی<sup>۲۴</sup>» (PIPEDA) در اوایل سال ۲۰۰۰ در صدر کشورهای مدعی محافظت از داده‌ها قرار داشته است. این قانون اولیه براساس ۱۰ اصل مندرج در الگوی محافظت از اطلاعات شخصی تنظیم شده و مسئولیت‌پذیری، اخذ رضایت و محدودیت در جمع‌آوری داده‌ها را دربر می‌گیرد. امروزه، این اصول همچنین در آیین‌نامه حفاظت از داده‌های عمومی اتحادیه اروپا (GDPR) نیز دیده می‌شود [۲۰].

در PIPEDA به ۱۰ اصل اساسی حفاظت از داده‌ها اشاره شده است. در عین حال سازمان‌ها در هر زمان مسئولیت حفاظت از اطلاعات شخصی را برعهده دارند و موظف هستند که اطمینان حاصل کنند که هرگونه جمع‌آوری، استفاده یا افشای اطلاعات شخصی فقط برای اهدافی انجام می‌شود که فرد - با توجه به شرایط موجود - آن را مناسب می‌داند. این اصول در جدول ۳ آمده است.

## ۳.۶ اقدامات اتحادیه اروپا

مقررات حفاظت از داده‌های عمومی اتحادیه اروپا<sup>۲۵</sup> (GDPR) معرف مقرراتی است که در مورد حفاظت از داده و محرمانگی همه اشخاص و خروج داده در اتحادیه اروپا و منطقه اقتصادی اروپا وضع شده است. هدف این مقررات اساساً اعطای کنترل داده‌ها به شهروندان و ساکنان این منطقه و ساده‌سازی محیط مقررات‌گذاری برای کسب‌وکارهای بین‌المللی از طریق یکسان‌سازی مقررات است [۱۰].

این مقررات جایگزین قانون حفاظت از داده اتحادیه اروپا (95/46/EC) شده است و شامل احکام و الزاماتی مرتبط با پردازش اطلاعات شخصی قابل تشخیص در اتحادیه اروپا می‌شود و در خصوص همه کسب‌وکارهایی مطرح می‌شود که با این منطقه اقتصادی مرادبه کاری دارند (صرفنظر از مکان استقرارشان). بدین ترتیب، فرآیندهای کسب‌وکار که اطلاعات شخصی را اداره می‌کنند باید مبتنی بر «حفاظت اطلاعات

<sup>19</sup>Fair Credit Reporting Act

<sup>24</sup>Personal Information Protection and Electronic Documents Act

<sup>25</sup>General Data Protection Regulation

## جدول ۲: برخی از قوانین و مقررات ایالات متحده آمریکا در حوزه حفاظت از داده‌ها

ردیف	عنوان	موضوع مورد توجه
۱	قانون گرام لیچ بیلی <sup>۲۰</sup>	حمایت از اطلاعات شخصی در دست بانک‌ها، شرکت‌های بیمه و سایر شرکت‌های حوزه خدمات مالی
۲	قانون گزارش اعتباری منصفانه <sup>۲۱</sup>	محدودسازی استفاده از اطلاعات دارای اعتبار مربوط به اعتبار فردی، جایگاه اعتباری، ظرفیت اعتباری، شخصیت و شهرت عمومی
۳	استانداردهای امنیت داده‌های صنعت کارت پرداخت (PCI-DSS)	مجموعه‌ای از استانداردهای امنیتی که توسط شرکت‌های بزرگ کارت اعتباری به منظور محافظت از داده‌های دارندگان کارت‌های پرداخت تهیه شده است.
۴	قانون قابلیت انتقال و پاسخگویی بیمه سلامت (HIPAA)	بهبود بهره‌وری در مراقبت‌های بهداشتی و نتایج مراقبت از بیمار با تشویق جریان آزاد اطلاعات بهداشتی در ایالات متحده و حراست از حریم خصوصی اطلاعات بهداشتی فرد
۵	قانون حمایت از مصرف‌کنندگان تلفن	آیین‌نامه‌های مرتبط با تماس‌ها و پیام‌های متنی تلفن‌های همراه و قوانین مربوط به تماس با تلفن‌های ثابت برای اهداف بازاریابی یا استفاده از سیستم‌های شماره‌گیری خودکار یا پیام‌های از پیش ضبط‌شده
۶	قانون آموزش حقوق و حفظ حریم خصوصی خانواده	ایجاد حق بازرسی و تجدید نظر در سوابق دانش آموزان و ممنوعیت افشای این سوابق یا سایر اطلاعات شخصی دانش‌آموزان، بدون رضایت وی و یا خانواده وی
۷	قانون حریم خصوصی مصرف‌کننده در کالیفرنیا	لایحه‌ای برای حفظ حقوق حریم شخصی و حمایت از مصرف‌کننده افراد مقیم ایالت کالیفرنیا
۸	قانون حفاظت از حریم خصوصی ویدیو	قانون حذف اطلاعات شناسایی شخصی در ویدئوها در شرکت‌های اجاره ویدیو حداکثر یک سال پس از آن که اطلاعات دیگر برای هدف جمع‌آوری شده آن ضروری نیست.
۹	قانون اوراق بهادار فدرال	قوانین کنترل اوراق بهادار فدرال در عرضه و فروش اوراق بهادار و تجارت اوراق بهادار، فعالیت‌های متخصصان خاص در صنعت، شرکت‌های سرمایه‌گذاری، پیشنهادات مناقصه، اظهارنامه‌های حقوقی و مقررات شرکت‌های عمومی کاربرد دارند.
۱۰	قانون حفاظت از حریم خصوصی آنلاین کودکان (COPPA)	حفاظت از داده‌ها و حریم خصوصی کودکان در فضای اینترنت
۱۱	قانون حفظ حریم خصوصی ارتباطات الکترونیکی <sup>۲۲</sup> (ECPA)	محافظت از ارتباطات برخط، شفاهی و الکترونیکی در زمان برقراری ارتباطات، حمل و نقل و ذخیره آنها را مدنظر قرار می‌دهد.
۱۲	قانون تقلب و سوءاستفاده رایانه‌ای <sup>۲۳</sup> (CFAA)	قانونی برای حفاظت از سیستم‌های کامپیوتری در مقابل قانون‌شکنی و حملات سایبری
۱۳	قانون کمیسیون تجارت فدرال (قانون FTC)	قانونی برای جلوگیری از استفاده از روش‌های ناعادلانه رقابت و اعمال یا اقدامات ناعادلانه یا فریبنده مؤثر بر تجارت
۱۴	قانون حمایت مالی از مصرف‌کننده (CFPA)	قانون ایجاد نقطه پاسخگویی برای اجرای قوانین مالی مصرف‌کننده فدرال و حمایت از مصرف‌کنندگان در بازار مالی
۱۵	چارچوب سیاست حفظ حریم خصوصی داده‌های پیشنهادی دولت ترامپ	مجموعه‌ای از اهداف حفظ حریم خصوصی «کاربر محور» برای حمایت از مصرف‌کنندگان در مقابل اقدامات نهادهای دولتی مرتبط با حریم خصوصی

## جدول ۳: اصول ده‌گانه PIPEDA

اصل	توضیحات
مسئولیت‌پذیری	یک سازمان مسئول اطلاعات شخصی تحت کنترل خود است و باید برای حصول اطمینان از پیروی از PIPEDA، یک افسر حفظ حریم خصوصی را استخدام کند.
شناسایی اهداف	سازمان‌ها باید اهدافی را شناسایی کنند که برای جمع‌آوری داده‌های شخصی آن‌ها اقدام می‌کنند.
رضایت	رضایت افراد برای جمع‌آوری، استفاده یا افشای اطلاعات شخصی مورد نیاز است. برخی از معافیت‌ها در مورد این اصل اعمال می‌شود. به‌عنوان مثال در مواردی که دلایل قانونی، پزشکی یا امنیتی مطرح است ممکن است اخذ رضایت غیرممکن یا غیرعملی باشد.
محدودیت سازمان	اطلاعات باید با استفاده از روش‌های منصفانه و قانونی جمع‌آوری شوند و فقط به داده‌های مورد نیاز برای هدف مشخص‌شده توسط سازمان محدود شود.
محدودیت استفاده، افشاء و نگهداری اطلاعات	اطلاعات شخصی فقط برای اهدافی که برای آن جمع‌آوری شده است می‌تواند مورد استفاده یا افشاء قرار گیرد و باید صرفاً برای مدت زمان مورد نیاز برای انجام این اهداف نگه داشته شود، مگر اینکه فرد رضایت داده یا به‌صورتی قانونی مجاز باشد.
دقت	اطلاعات شخصی باید تا حد امکان دقیق، کامل و به‌روز باشد تا به درستی اهداف استفاده را برآورده سازد.
محافظت	اطلاعات شخصی باید از طریق ضمانت امنیتی مناسب در برابر از دست دادن یا سرقت و همچنین دسترسی غیرمجاز، افشاء، کپی، استفاده و یا اصلاح محافظت شوند.
صراحت	سازمان‌ها باید در مورد سیاست‌ها و شیوه‌های مربوط به مدیریت داده‌های شخصی آزاد باشند و اطمینان حاصل کنند که چنین اطلاعاتی به‌راحتی در قالب کاملاً قابل فهم در دسترس افراد قرار می‌گیرد.
دسترسی فردی	در صورت درخواست فرد باید از وجود، استفاده و افشای اطلاعات شخصی خود مطلع شده و به آن دسترسی پیدا کند. اشخاص حق دارند صحت و کامل بودن اطلاعات را به چالش کشیده و در صورت لزوم اصلاح کنند.
چالش انطباق PEPEDA	فرد می‌تواند انطباق یک سازمان با اصول PEPEDA را به چالش کشیده و چالش خود را به مسئول امور حفظ حریم خصوصی شرکت - که مسئولیت انطباق با PEPEDA را بر عهده دارد - ارائه کند.

از طریق طراحی و به‌طور پیش فرض» باشند؛ یعنی اطلاعات شخصی باید با استفاده از مستعارسازی یا بی‌نام‌سازی ذخیره شود و حداکثر محرمانگی به‌طور پیش‌فرض در نظر گرفته شود؛ به‌گونه‌ای که داده‌ها بدون رضایت صریح به‌طور عمومی در دسترس نباشد و بدون اطلاعات اضافی جداگانه برای تعیین هویت اشخاص قابل استفاده نباشد. براین اساس هیچ‌گونه اطلاعات شخصی نمی‌تواند پردازش شود، مگر آنکه تحت مبنای قانونی که به وسیله مقررات مشخص شده، انجام شود یا آنکه کنترل‌کننده یا پردازنده داده‌ها اجازه صریح مختارانه صاحب داده‌ها را دریافت کرده باشد. صاحب داده‌ها می‌تواند در هر زمانی این اجازه را لغو کند [۱۰].

این قانون در ۱۴ آوریل ۲۰۱۶ وضع شد و بعد از سپری شدن دو سال به عنوان دوره گذار، از ۲۵ می ۲۰۱۸ به اجرا درآمد. اعمال این قانون نیازمند تصویب قانون جداگانه در کشورهای عضو اتحادیه نمی‌باشد و به‌طور خودکار در همه آن‌ها لازم‌الاجرا است.

#### ۴.۶ اقدامات کره جنوبی

مشابه ساختار مقررات عمومی حفاظت از داده مصوب اتحادیه اروپا در کشور کره جنوبی نیز قانونی در رابطه با محافظت از اطلاعات شخصی (قانون حمایت از اطلاعات شخصی<sup>۲۶</sup> (PIPA))، از سپتامبر ۲۰۱۱ تصویب و اجرا گردید. بدین ترتیب که «قانون حمایت از اطلاعات شخصی» کره جنوبی در ۲۹ مارس ۲۰۱۱ به تصویب مجلس قانونگذاری این کشور رسید و در ۳۱ مارس ۲۰۱۲ توسط دولت این کشور اجرایی شد. این قانون سخت‌گیرانه‌ترین و جامع‌ترین قانون حفاظت از حریم خصوصی کاربران در فضای مجازی در میان کشورهای دنیا شناخته می‌شود (گرینلیف و پارک، ۲۰۱۲). این قانون شامل تمامی سازمان‌های بخش دولتی نیز می‌شود و علاوه بر جامع بودن، دارای ویژگی‌های زیر است [۲۱]:

- کمیسیون حفاظت از اطلاعات شخصی که ۱۵ عضو مستقل دارد.
- الزام بنگاه‌های تجاری و سازمان‌های دولتی به نصب مأموران حافظ انطباق با قوانین حریم خصوصی.
- لزوم اطلاع‌رسانی به افراد آسیب‌دیده و نیز نهادهای نظارتی در صورت بروز هرگونه مسائل امنیتی و نشر داده‌های شخصی افراد.
- لزوم انجام ارزیابی آثار حریم خصوصی برای سامانه‌های بخش دولتی آسیب‌پذیر.
- الزام سازمان‌ها به اخذ رضایت آشکار افراد برای مقاصد بازاریابی با استفاده از پایگاه‌های داده خود سازمان‌ها.

<sup>26</sup>Personal Information Protection Act

## ۵.۶ اقدامات روسیه

در ۲۲ ژوئیه ۲۰۱۴ بود که اصلاحات قابل توجهی در قانون روسیه به تصویب رسید و در تاریخ ۱ سپتامبر ۲۰۱۵ لازم‌الاجرا گردید. این اصلاحات به کلیه اپراتورهایی که از داده‌های شخصی استفاده می‌کنند، الزام می‌کند که هرگونه اطلاعات شخصی افراد روس را در پایگاه‌های داده مستقر در روسیه ذخیره و پردازش کنند. مجازات نقض این شرط می‌تواند منجر به مسدود کردن وبسایت‌ها و کسب‌وکار شود. پیگیری حقوقی متخلفان از قانون حفاظت از داده‌های شخصی توسط سرویس فدرال با نظارت بر محتوا، ارتباطات و فناوری‌ها ایجاد می‌شود و این سرویس ممکن است برای مسدود کردن وبسایت‌ها اقدام کند.

تیم واکنش اضطراری به حوادث رایانه‌ای بخش مالی<sup>۲۷</sup> به‌عنوان زیرمجموعه‌ای از اداره کل امنیت و حفاظت از اطلاعات بانک روسیه تأسیس شده است و به‌عنوان مرکز دارای صلاحیت تبادل اطلاعات بین بانک روسیه، بانک‌ها و مؤسسات مالی غیربانکی (NBFIs)، شرکت‌های یکپارچه‌ساز، فروشندگان آنتی‌ویروس و ارائه‌دهندگان خدمات ارتباطاتی و اپراتورها و به‌طور خاص برای اجرای قانون در سراسر جامعه فعالیت می‌کند و مقام نظارت بر امنیت سایبری در سراسر صنعت روسیه را برعهده دارد.

## ۷ یافته‌های تحقیق

پس از تعیین متن اسناد راهبردی شناسایی شده - به‌عنوان واحد تحلیل - محقق نسبت به تدوین مقوله‌ها و زیرمقوله‌های اسناد پرداخته و متغیرهای پژوهش از این طریق شناسایی شده‌است. این نتایج در قالب جدول ۴ ملاحظه می‌شود. جهت تحلیل اسناد ۳۸ مقوله اختصاص داده شده است. هر یک از مقوله‌ها دارای یک یا چند واحد ثبت است. با شناسایی پیام‌ها و گزاره‌های کلیدی موجود در مقاله‌ها و گدگذاری داده‌ها امکان بررسی و تحلیل فراهم شده‌است. در بررسی واحدهای تحلیل، ۴۲۵ زیرمقوله شناسایی گردید. سپس در جلسات خبرگی این زیرمقوله‌ها مورد بازبینی قرار گرفته، گدگذاری شده و در ۳۸ مقوله سازماندهی شده‌اند. نتایج این فعالیت در قالب جدول ۴ ارائه شده‌است.

جدول ۴: گدگذاری داده واحدهای تحلیل

ردیف	مقوله	فراوانی
۱	حق تعریف اطلاعات و داده‌های شخصی	۳۳
۲	مسئولیت‌پذیری	۳۳
۳	محدودیت در پردازش اضافه‌تر	۳۱
۴	حفظ کیفیت اطلاعات	۳۱
۵	حق اعلام جمع‌آوری	۳۰
۶	حق حمل و نقل داده‌ها	۳۰
۷	حق اعلان نقض اطلاعات	۳۰
۸	محدودیت پردازش و استفاده	۳۰
۹	اعلان نقض در داده‌ها	۳۰
۱۰	اطلاعات شخصی حساس	۳۰
۱۱	مشخص نمودن هدف از پردازش	۲۹

<sup>27</sup>FinCERT

ردیف	مقوله	فراوانی
۱۲	الزام مسئول حفظ داده‌ها	۲۸
۱۳	حفظ محدودیت‌های انتقال داده‌های مرزی	۲۸
۱۴	عدم استفاده در بازاریابی مستقیم	۲۸
۱۵	حق تعریف داده‌های حساس	۲۷
۱۶	محدودیت در جمع‌آوری داده	۲۷
۱۷	انجام اقدامات امنیتی و استفاده از اشخاص ثالث	۲۷
۱۸	حق انتقال اطلاعات	۲۴
۱۹	مشارکت دادن و ایجاد دسترسی برای موضوع داده	۲۴
۲۰	حفظ حریم خصوصی آنلاین	۲۴
۲۱	باز بودن داده‌ها	۲۳
۲۲	حق درخواست دسترسی	۲۱
۲۳	استفاده و افشای داده	۱۸
۲۴	حفظ امنیت داده‌ها	۱۸
۲۵	حق حفظ حریم خصوصی آنلاین	۱۸
۲۶	نگهداری و از بین بردن داده‌ها	۱۷
۲۷	انتقال اطلاعات	۱۷
۲۸	حفظ کیفیت اطلاعات	۱۷
۲۹	محدودیت پردازش و استفاده	۱۷
۳۰	مشخص بودن هدف از جمع‌آوری داده‌ها	۱۷
۳۱	عدم پردازش بیش از توافق اولیه	۱۶
۳۲	مشخص بودن و اعلام نحوه جمع‌آوری	۱۵
۳۳	اعلام تغییر در داده‌های جمع‌آوری شده	۱۵
۳۴	عدم جمع‌آوری بیش از توافق اولیه	۱۵
۳۵	حق درخواست تعلیق پردازش	۱۵
۳۶	باز بودن داده‌ها	۱۴
۳۷	حق فراموش شدن	۱۴
۳۸	مأمور محافظت از داده	۱۳

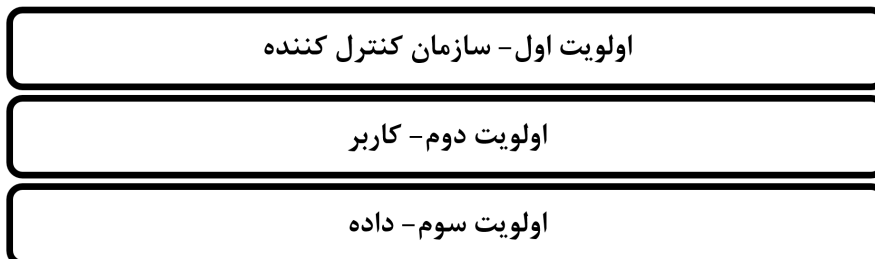
در ادامه، با شناسایی گزاره‌های راهبردی کلیدی در متن اسناد و گذراری داده‌ها امکان بررسی و تحلیل راهبردها فراهم شده است. همانطور که در جدول ۵ مشاهده می‌شود، ۳۸ مقوله شناسایی شده در قالب ۳ موضوع راهبردی اصلی دسته‌بندی شده است و فراوانی موضوعات راهبردی نشان داده شده است. باید توجه داشت که موضوعات راهبردی معرف محورهای تعریف اصول و الزامات کلان، راهبردها و خط‌مشی‌های حفاظت از داده در اسناد و مقررات سایر کشورها بوده است.

## ۸ ارزیابی و صحت‌سنجی یافته‌های تحقیق

یکی از بهترین روش‌ها برای سنجش روایی، کسب نظر خبرگان است. در این پژوهش و برای تأیید اسناد ورودی جهت تحلیل محتوا از یک پنل خبرگی ۶ نفره با حضور اعضای هیات علمی و خبرگان حوزه فناوری در پژوهشگاه ارتباطات و فناوری اطلاعات، دانشگاه تهران، دانشگاه شهید بهشتی و دانشگاه علم و صنعت استفاده شده است. این افراد طی سال‌های ۱۳۹۷ تا ۱۳۹۸ مسئولیت مجری‌گری و راهبری ۶ پروژه کاربردی و راهبردی در حوزه تنظیم‌گری در حوزه ارتباطات و فناوری اطلاعات را برعهده داشته‌اند. در این راستا، جلسات مستمری تشکیل و اعتبار اسناد ورودی برای انجام تحلیل به تأیید خبرگان رسیده است.







شکل ۲: اولویت و تمرکز موضوعات راهبردی در اسناد مطالعه شده

جدول ۶: مقوله مورد تمرکز و راهبرد مرتبط

اولویت	گزاره راهبردی (مقوله)	فراوانی	موضوع راهبردی مربوطه
۱	حق تعریف اطلاعات و داده‌های شخصی	۳۳	کاربر
۲	مسئولیت‌پذیری	۳۳	سازمان کنترل کننده
۳	محدودیت در پردازش اضافه‌تر	۳۱	سازمان کنترل کننده
۴	حفظ کیفیت اطلاعات	۳۱	سازمان کنترل کننده
۵	حق اعلام جمع‌آوری	۳۰	کاربر
۶	حق حمل و نقل داده‌ها	۳۰	کاربر
۷	حق اعلان نقض اطلاعات	۳۰	کاربر
۸	محدودیت پردازش و استفاده	۳۰	سازمان کنترل کننده
۹	اعلان نقض در داده‌ها	۳۰	داده
۱۰	پردازش اطلاعات شخصی حساس	۳۰	سازمان کنترل کننده

همچنین با توجه به نتایج به دست آمده، اولویت و تمرکز موضوعات راهبردی - براساس مجموع فراوانی گزاره‌های راهبردی (مقوله‌ها) در اسناد - به ترتیب در قالب شکل ۲ به تصویر کشیده شده است. به منظور بررسی رویکرد مورد تمرکز در اسناد راهبردی ملی، محقق مقوله‌ها/ گزاره‌های راهبردی برجسته در هر نمونه موردی را به تفکیک واحدهای تحلیل در قالب جدول ۸ ارائه نموده است. با بررسی رویکرد کشورها در موضوعات راهبردی شناسایی شده در اسناد و بررسی نتایج تحلیل کیفی مندرج در جدول ۸، مشاهده می‌شود که گزاره‌های راهبردی (مقوله‌های) ذیل بیش از ۵۰ درصد واحدهای تحلیل تکرار و مورد تاکید بوده است. تکرارپذیری این مقوله‌ها بیانگر اهمیت این موضوعات در امر برنامه‌ریزی و اخذ استراتژی‌های در امر توسعه قوانین و مقررات حفاظت از داده‌ها در کشورهای مختلف را نشان می‌دهد. تحلیل بین‌موردی و درون‌موردی راهبردهای توسعه قوانین و مقررات حفاظت از داده‌های عمومی در نمایی متفاوت و به تفکیک واحدهای تحلیل در قالب جدول (۵) ارائه شده است. بررسی میزان تکرار و توجه به راهبردها در کشورهای مختلف بیانگر آن است که میزان توجه به مقوله‌ها در کشورهای مختلف، متفاوت است.

بررسی مقوله‌های ۳۸ گانه در کشورهای منتخب که به بیش از ۲۰ مورد از مقوله‌ها توجه کرده‌اند، نشان می‌دهد اکثر کشورها به رعایت مقوله‌ها در قوانین و مقررات حفاظت داده کشور خود اهمیت داده‌اند. در عین حال مقوله استفاده از مأمور حفاظت از داده که ناظر به اجرای دقیق در سمت کنترل کننده‌ها است، به علت

ایجاد بار اجرایی کمتر مورد توجه بوده است و در واقع فقط ۷ مورد از کشورها و یا به عبارت دیگر نیمی از کشورهای منتخب به آن توجه کرده‌اند.

جدول ۷: گزاره‌های راهبردی / مقوله مورد تمرکز به تفکیک واحدهای تحلیل

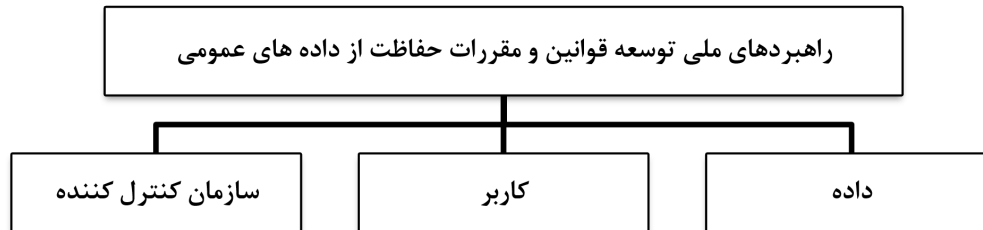
واحد تحلیل	مقوله مورد تمرکز	واحد تحلیل	مقوله مورد تمرکز
امریکا	<ul style="list-style-type: none"> <li>• حق تعریف اطلاعات و داده‌های شخصی</li> <li>• مسئولیت‌پذیری</li> <li>• محدودیت پردازش و استفاده</li> <li>• حق اعلان نقض اطلاعات</li> <li>• اعلان نقض در داده‌ها</li> <li>• حق حمل و نقل داده‌ها</li> <li>• محدودیت در پردازش اضافه‌تر</li> <li>• حق اعلام جمع‌آوری</li> </ul>	کانادا	<ul style="list-style-type: none"> <li>• محدودیت پردازش و استفاده</li> <li>• مسئولیت‌پذیری</li> <li>• پردازش اطلاعات شخصی حساس</li> <li>• محدودیت پردازش و استفاده</li> <li>• اعلان نقض در داده‌ها</li> <li>• حق حمل و نقل داده‌ها</li> <li>• محدودیت در پردازش اضافه‌تر</li> <li>• حق اعلام جمع‌آوری</li> </ul>
اتحادیه اروپا	<ul style="list-style-type: none"> <li>• حق تعریف اطلاعات و داده‌های شخصی</li> <li>• مسئولیت‌پذیری</li> <li>• محدودیت پردازش و استفاده</li> <li>• حق اعلان نقض اطلاعات</li> <li>• محدودیت پردازش و استفاده</li> <li>• اعلان نقض در داده‌ها</li> <li>• حق حمل و نقل داده‌ها</li> <li>• محدودیت در پردازش اضافه‌تر</li> <li>• حق اعلام جمع‌آوری</li> </ul>	کره جنوبی	<ul style="list-style-type: none"> <li>• حق تعریف اطلاعات و داده‌های شخصی</li> <li>• مسئولیت‌پذیری</li> <li>• محدودیت پردازش و استفاده</li> <li>• حق اعلان نقض اطلاعات</li> <li>• محدودیت پردازش و استفاده</li> <li>• اعلان نقض در داده‌ها</li> <li>• حق حمل و نقل داده‌ها</li> <li>• محدودیت در پردازش اضافه‌تر</li> <li>• حق اعلام جمع‌آوری</li> </ul>
روسیه	<ul style="list-style-type: none"> <li>• محدودیت پردازش و استفاده</li> <li>• مسئولیت‌پذیری</li> <li>• پردازش اطلاعات شخصی حساس</li> <li>• حق حمل و نقل داده‌ها</li> <li>• حق اعلام جمع‌آوری</li> </ul>	ژاپن	<ul style="list-style-type: none"> <li>• مسئولیت‌پذیری</li> <li>• محدودیت پردازش و استفاده</li> <li>• اعلان نقض در داده‌ها</li> <li>• حق اعلام جمع‌آوری</li> </ul>

واحد تحلیل	مقوله مورد تمرکز	واحد تحلیل	مقوله مورد تمرکز
اسپانیا	<ul style="list-style-type: none"> <li>مسئولیت پذیری</li> <li>حق تعریف اطلاعات و داده‌های شخصی</li> <li>محدودیت پردازش و استفاده</li> <li>حق حمل و نقل داده‌ها</li> <li>حق اعلام جمع‌آوری</li> </ul>	سنگاپور	<ul style="list-style-type: none"> <li>مسئولیت پذیری</li> <li>حق تعریف اطلاعات و داده‌های شخصی</li> <li>محدودیت پردازش و استفاده</li> <li>اعلان نقض در داده‌ها</li> <li>حق حمل و نقل داده‌ها</li> <li>حق اعلام جمع‌آوری</li> </ul>
تایوان	<ul style="list-style-type: none"> <li>مسئولیت پذیری</li> <li>پردازش اطلاعات شخصی حساس</li> <li>اعلان نقض در داده‌ها</li> <li>محدودیت پردازش و استفاده</li> <li>حق اعلام جمع‌آوری</li> </ul>	هند	<ul style="list-style-type: none"> <li>مسئولیت پذیری</li> <li>محدودیت پردازش و استفاده</li> <li>اعلان نقض در داده‌ها</li> <li>حق حمل و نقل داده‌ها</li> <li>حق اعلام جمع‌آوری</li> </ul>
فرانسه	<ul style="list-style-type: none"> <li>مسئولیت پذیری</li> <li>حق اعلان نقض اطلاعات شخصی</li> <li>محدودیت پردازش و استفاده</li> <li>اعلان نقض در داده‌ها</li> <li>حق حمل و نقل داده‌ها</li> <li>حق اعلام جمع‌آوری</li> </ul>	نروژ	<ul style="list-style-type: none"> <li>حق تعریف اطلاعات و داده‌های شخصی</li> <li>محدودیت پردازش و استفاده</li> <li>حق حمل و نقل داده‌ها</li> <li>حق اعلام جمع‌آوری</li> </ul>
نیجریه	<ul style="list-style-type: none"> <li>حق تعریف اطلاعات و داده‌های شخصی</li> <li>مسئولیت پذیری</li> <li>محدودیت پردازش و استفاده</li> <li>اعلان نقض در داده‌ها</li> <li>حق اعلام جمع‌آوری</li> </ul>	استرالیا	<ul style="list-style-type: none"> <li>حق اعلان نقض اطلاعات</li> <li>محدودیت پردازش و استفاده</li> <li>حق اعلام جمع‌آوری</li> </ul>

در بخش‌های مختلف بیشترین توجه کشورها به جمع‌آوری و اعلام، اعلان نقض در اطلاعات، محدودیت پردازش و استفاده، محدودیت در جمع‌آوری داده، حق تعریف اطلاعات و داده‌های شخصی، حق اعلام جمع‌آوری، مسئولیت‌پذیری، اعلان نقض در داده‌ها، حفظ حریم خصوصی آنلاین و پردازش اطلاعات شخصی حساس معطوف بوده‌است.

در حوزه توجه به مقوله‌هایی که در دسته‌بندی «داده» قرار می‌گیرند، بیشترین توجه به جمع‌آوری و اعلام (۱۴ مورد)، اعلان نقض در اطلاعات (۱۳ مورد)، محدودیت پردازش و استفاده (۱۴ مورد) و محدودیت در جمع‌آوری داده (۱۴ مورد) بوده‌است. در این بخش کمترین توجه به مقوله نگهداری و از بین بردن داده‌ها





شکل ۳: چارچوب مفهومی اقدامات کلان

در قالب یک مدل مرجع دسته‌بندی شده است. در ادامه یافته‌های تحلیل مورد واکاوی قرار گرفت تا مورد توافق و اجتماع خبرگان قرار گیرد. نتایج این پژوهش و اشباع نظری تحت عنوان «چارچوب مفهومی اقدامات کلان» در قالب شکل ۳ ارائه شده است.

همانطور که مشاهده می‌شود نتایج برآمده از تحلیل اسناد، به سه موضوع راهبردی بنیادی برای سیاست‌گذاری منتج شد که ملاحظات سیاست‌گذاران و نیز اقتضات و نیازهای توسعه قوانین و مقررات حفاظت از داده‌های عمومی در کشورهای مختلف را پوشش می‌دهد. در این بین تحلیل یافته‌ها براساس تحلیل محتوای انجام‌شده اهمیت توجه به مقوله‌هایی چون جمع‌آوری و اعلام، اعلان نقض در اطلاعات، محدودیت پردازش و استفاده، محدودیت در جمع‌آوری داده، حق تعریف اطلاعات و داده‌های شخصی، حق اعلام جمع‌آوری، مسئولیت‌پذیری، اعلان نقض در داده‌ها، حفظ حریم خصوصی آنلاین و پردازش اطلاعات شخصی حساس را نشان می‌دهد.

آنچه بیش از مدل تبیین شده حایز اهمیت است، نحوه اجرایی ساختن این موضوعات راهبردی است که افزون بر پاره‌ای رویکردهای شناختی و ملاحظات فناورانه، مستلزم توجه به بلوغ ساختاری و سیاست‌گذارانه در حوزه فناوری است که چالش عمده بسیاری از کشورهای توسعه‌یافته در این زمینه محسوب می‌شود. وزن این موضوعات از یک کشور به کشور دیگر دستخوش تغییر می‌شود. به‌عنوان مثال، در کشور ایران به‌واسطه وجود قوانین و مقررات خاص و ساختار حاکمیتی خاص کشور، مطمئناً مقوله‌های تحقیق و توسعه و نیز تنظیم و اعمال مقررات (با نگاه رگولاتوری و سازماندهی اکوسیستم) در اولویت قرار خواهند گرفت. در واقع، چارچوب مفهومی پیشنهادی - برگرفته از بررسی مقایسه‌ای راهنمای ملی توسعه قوانین و مقررات حفاظت از داده‌های عمومی - می‌تواند در نقش ساختار پشتیبان تصمیم و نیز پرتفوی خط‌مشی‌های کلان، راهبردها و نیز اقدامات کلان برای تدوین نقشه‌راه و نیز سیاست‌گذاری‌های این حوزه کاربرد داشته باشد.

بنابراین، فرموله نمودن نقشه راهبردی تدوین قوانین و مقررات حفاظت از داده‌های عمومی کشور و تدوین حوزه‌های کاربردپذیر می‌تواند به‌عنوان فعالیت‌های آتی پیشنهادی پژوهش حاضر مدنظر قرار گیرند.

## مراجع

- [1] Tamburri, D. A. Design principles for the general data protection regulation (GDPR): A formal concept analysis and its evaluation. *Information Systems*, 2019.



- [2] Slepchuk, Alec N. and Milne, George R. Informing the design of better privacy policies. *Privacy and disclosure, online and in social interactions*, 2019.
- [3] Sana, S. and Tahar, K. Sensitive and private data analysis: A systematic review. *ICFNDS*, 2019.
- [4] Purtova, N. The law of everything. broad concept of personal data and future of eu data protection law. *Law, Innovation and Technology*, 2018.
- [5] Van O., I. and U. V., Helena. Does the GDPR enhance consumers' control over personal data? an analysis from a behavioural perspective. *Journal of Consumer Policy*. Springer., 2018.
- [6] Gauthier, Ch. The impact of the eu general data protection regulation on scientific research. *Ecancermedicalscience*, 2017.
- [7] Clarke, R. Privacy impact assessment: Its origins and development. *Computer law and security review*, 2009.
- [8] Clarke, R. An Evaluation of Privacy Impact Assessment Guidance Documents. *International Data Privacy Law*, 1(2): 111-120, 2011.
- [9] Commission Nationale de l'Informatique et des Libertes (CNIL). Privacy Impact Assessment (PIA) Methodology, 2015. URL: <https://www.cnil.fr/en/PIA-privacy-impact-assessment-en>
- [10] European Commission. Special Eurobarometer 423 Cyber Security. Report 978 DR-01-15-143-EN-N, European Commission, 2015.
- [11] ISO/IEC 29134 information technology – security techniques — privacy impact assessment – guidelines.
- [12] Oetzel, M.C. and Spiekermann, S. A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, 2014.
- [13] Office of the Australian Information Commissioner. *Guide to undertaking privacy impact assessments*, 2014.  
URL: <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments>
- [14] Markos, E., Milne, GR., and Peltier, JW. Information sensitivity and willingness to provide continua: a comparative privacy study of the united states and brazil. *JPublic Policy Mark*, 2017.
- [15] Saadatmand, F. A. S. Configurations of platform organizations: Implications for complementor engagement. 2019.
- [16] Zhang, Yan. Qualitative analysis of content. 1966.
- [17] H. H.-F. a. S. SE. Three approaches to qualitative content analysis. 2005.
- [18] Ghorra-Gobin, C. The comparative social science approach. 2008.
- [19] Shejy, G. Data privacy and security in social networks. *Smart Innovation, Systems and Technologies*, 2020.

- [20] Hsieh, Hsiu-Fang and Shannon, Sarah E. Three approaches to qualitative content analysis. *Qual Health Res.*, 2005.
- [21] Ko, M. J. and Lim, T. H. *Journal of the Korean Medical Association*, 2020.
- [22] P. and Baxter, J. S. Qualitative case study methodology. *Study design and implementation for novice researchers*, 2008.

## کتابخانه‌ها در متاورس

فاطمه محمدخانی<sup>۱</sup>، محسن حاجی زین العابدینی<sup>۲</sup>

<sup>۱</sup> دانشجوی کارشناسی ارشد مدیریت اطلاعات دانشگاه شهید بهشتی  
fateme.98.fm@gmail.com

<sup>۲</sup> عضو هیئت علمی گروه علم اطلاعات و دانش‌شناسی دانشگاه شهید بهشتی  
zabedini@gmail.com

### چکیده

[هدف] این پژوهش به منظور آشنایی با متاورس و کاربرد آن برای کتابداران و کتابخانه‌ها نوشته شده است. [روش‌شناسی] مقاله با روش مروری به گردآوری مقالات و اطلاعات درباره متاورس، نقش و خدماتی که کتابخانه‌ها می‌توانند در متاورس به آن بپردازند پرداخته است. برای نوشتن این مقاله جستجوی کلیدواژه‌های مرتبط با حوزه پژوهش در گوگل اسکالر، ریسرچ گیت، سوبلیکا، امرالد و ... انجام شد. [یافته‌ها] کتابداران در استفاده از فضای مجازی پیشگام بوده‌اند و آگاهی از ابزارها و بسترهای جدید همواره برای متخصصان اطلاعات مهم بوده است. کتابخانه‌ها به عنوان مرکز اصلی ترویج اطلاعات و علم می‌توانند برای هم‌گامی با نسل دیجیتال و برآورده کردن نیازهای آنها از مزایا و امکانات متاورس استفاده کنند. با از میان رفتن حضور فیزیکی، کاربران که در محیط متاورس آواتارهایی ساخته‌اند می‌توانند آزادانه به هر جا سفر کنند و از مکان‌های مختلف دیدن کنند. کتابخانه‌ها نیز می‌توانند از این امکان بهره‌جویند، از جمله فعالیت‌هایی که می‌توان به آن پرداخت: پذیرای حضور مجازی کاربران حتی در سطح بین‌الملل باشند، منابع خود را به اشتراک بگذارند، همایش‌ها و کارگاه‌های آموزشی برگزار کنند. [اصالت] متاورس پدیده‌ای نوظهور است که تحقیقات انگشت‌شماری درباره‌ی آن در حوزه کتابخانه و کتابداری انجام شده است با توجه به تحقیقات اندک در این حوزه این پژوهش از آن نظر حائز اهمیت است که کتابخانه‌ها برای هم‌گامی با سرعت پیشرفت فناوری و پررنگ کردن نقش خود در آن نیاز به حضور در متاورس دارند.

**کلمات کلیدی:** متاورس، کتابخانه‌ها در متاورس، واقعیت افزوده، واقعیت مجازی.

### ۱ مقدمه

تغییر سریع و مستمر تکنولوژیکی که مشخصه جامعه اطلاعاتی است که در آن قرار داریم، تأثیر قابل توجهی بر روشی که کتابداران برای کسب‌وکار خود پیش می‌برند، دارد. کتابداران در حال حاضر کمتر محدود به حضور

فیزیکی برای ارائه خدمات هستند، زیرا نقش‌هایشان آنها را عمیق‌تر به محیط‌های مجازی می‌برد (کروگر<sup>۱</sup>، ۲۰۰۵) [۴]. نوآوری‌های علوم کامپیوتر به دلیل تغییراتی که تعاملات انسانی، ارتباطات و تراکنش‌های اجتماعی ایجاد کرده‌اند، نقش مهمی را در زندگی روزمره ایفا می‌کنند. از دیدگاه کاربران نهایی، سه موج اصلی نوآوری در فناوری به ترتیب حول محور معرفی رایانه‌های شخصی، اینترنت و دستگاه‌های تلفن همراه ثبت شده است. در حال حاضر، موج چهارم نوآوری محاسباتی حول فناوری‌های فضایی و فراگیر مانند واقعیت مجازی (VR)<sup>۲</sup> و واقعیت افزوده (AR)<sup>۳</sup> در حال گسترش است. انتظار می‌رود این موج الگوی محاسباتی فراگیر بعدی را تشکیل دهد که پتانسیل تغییر آموزش (آن‌لاین)، تجارت، کار از راه دور و سرگرمی را دارد. این پارادایم جدید متاورس است (میستاکیدیس<sup>۴</sup>، ۲۰۲۲) [۱۱]. ریشه کلمه «متاورس» ترکیبی از کلمه یونانی «Meta» که پیشوندی به معنای «فراتر یا پس از» و کلمه انگلیسی «Universe» به معنای «جهان هستی» است. بنابراین می‌توان متاورس را فراتر از جهان هستی ترجمه کرد (فرخی و شهامت، ۱۴۰۰) [۲]. اولین بار این اصطلاح از «سقوط برف» استفنسون (۱۹۹۲)<sup>۵</sup> استفاده شده است، که یک سیاره‌ای مجازی شبیه‌سازی شده را به تصویر می‌کشد که یک فضای خطی محدود با املاک و مستغلات متعلق به یک نهاد شرکتی واحد است که در آن انسان‌ها با یکدیگر و با ربات‌ها از طریق آواتارها<sup>۶</sup> در خیابان تعامل دارند (چوهان<sup>۷</sup>، ۲۰۲۲) [۸]. در حقیقت، متاورس راهی واحد برای تعامل افراد و اشیاء در یک ظرفیت مجازی و فضایی است. مجموعه‌ای از جهان‌های مجازی، که شامل جهان فیزیکی ما می‌شود، متاورس را تشکیل می‌دهند (هیوز<sup>۸</sup>، ۲۰۲۲) [۹].

## ۲ پیشینه پژوهش داخل کشور

حسینی و میرحسینی (۱۳۹۵) [۱] در مقاله «آینده فن‌آوری در کتابخانه‌های عمومی (چالش‌ها و فرصت‌ها) با ذکر تکنولوژی‌های جدید مورد استفاده در کتابخانه این‌گونه بیان داشتند که مدیران کتابخانه و کتابداران موظفند برنامه‌ای استراتژیک برای رویارویی با مسائل و چالش‌های حاصل از فن‌آوری اطلاعات در کتابخانه‌های خود در نظر بگیرند. اجرای این برنامه مستلزم بکارگیری تمام ظرفیت‌ها و توانمندی‌های موجود و انتخاب بهترین روش برای پاسخگویی به تغییرات محیطی و هماهنگ شدن سازمان با آن و همچنین همکاری کلیه کتابداران و کارکنان کتابخانه می‌باشد. فرخی و شهامت (۱۴۰۰) [۲] در مقاله «نقش و کاربست متاورس در فرایند یادگیری» به‌طور خلاصه به بیان تعریف متاورس و کاربردهای آن می‌پردازند و سپس نقش متاورس در یادگیری و آموزش و ویژگی‌های مثبت یادگیری و آموزش در متاورس را بیان می‌کنند.

<sup>1</sup>Kruger, Hilda

<sup>2</sup>Virtual Reality

<sup>3</sup>Augmented Reality

<sup>4</sup>Stylianios Mystakidis

<sup>5</sup>Stephenson's Snow Crash (1992)

<sup>۶</sup>آواتار: کلمه‌ای در زبان سانسکریت است که نشان‌دهنده تجلی خدایی به شکل انسان است. مثلاً در محیط‌های اجتماعی VR، هر کاربر در دنیای مجازی به‌شکل یک شخصیت یا آواتار قابل مشاهده است.

<sup>7</sup>Usman W. Chohan

<sup>8</sup>Hughes

### ۳ پیشینه پژوهش خارج کشور

مقاله "I, Librarian" کروگر (۲۰۰۵) [۴] سناریویی از تغییرات فناوری را ارائه می‌دهد، اینکه چگونه این تغییرات بر نقش کتابداران در آینده تأثیر می‌گذارد. یکی از نگرانی‌های اصلی این مقاله، ارتباط مداوم متخصصان اطلاعات به‌عنوان واسطه‌های اطلاعاتی در جامعه آینده ما است. هیل و وانس و جونز<sup>۹</sup> (۲۰۱۰) [۶] در مقاله «کتابخانه‌های متاورس: جوامع به‌عنوان منابع» به بررسی هدف و پتانسیل کتابخانه‌های دنیای مجازی و کتابداران برای کمک به یادگیرندگان در محیط‌های مجازی اطلاعات مورد نیاز از جمله شبیه‌سازی‌ها، محتوای با کیفیت بالا و جوامع پرداخته است. چوهان (۲۰۲۲) [۸] در مقاله «متاورس یا متاکورس» ابتدا به تعریف متاورس پرداخته است: مفهوم «متاورس» به شبکه‌ای از واقعیت‌های مجازی سه‌بعدی، با تأکید بر تعامل اجتماعی که از طریق فضای مجازی و واقعیت افزوده واسطه می‌شود، اشاره دارد. منافع قدرتمندی از توسعه متاورس (ها) حمایت می‌کنند، اما تنزل دادن انسان به یک اثر غیرمادی جمعی با انتقادهای شدید مواجه شده است. این مقاله به بررسی مسئله متاورس در یک بوم وسیع‌تر پرداخته و اشاراتی به راه‌های تبلیغاتی که شرکت‌ها برای تشویق مردم به روی آوردن به متاورس انجام داده‌اند می‌کند. تیلور و سونجی<sup>۱۰</sup> (۲۰۲۲) [۱۳] در مقاله «بیوانفورماتیک و متاورس: آیا ما آماده‌ایم؟» به این موضوع پرداخته‌اند که مؤسسات تجاری و تحقیقاتی که پیش از این عمدتاً برای بازی‌ها دیده می‌شد، در حال بررسی راه‌حلی برای حل مشکلات دنیای واقعی از آموزش، شبیه‌سازی، تجزیه و تحلیل داده‌ها و مطالعه پیشرفت بیماری هستند. مقاله به این موضوع می‌پردازد که چگونه تجسم‌سازی می‌تواند از متاورس در تحقیقات بیوانفورماتیک، مزایا و معایب این فناوری و آنچه که ممکن است در آینده رخ دهد، استفاده کند. میتساکیدیس (۲۰۲۲) [۱۱] در مقاله با عنوان «متاورس» اشاره کرده است که اگر تعامل بین فضای فیزیکی و مجازی به‌طور خلاقانه گسترش یابد، نوید تغییرات بسیاری از جمله آموزش آن‌لاین از راه دور را می‌دهد. مدل‌های جدید آموزش، فراآموزی، آموزش از راه دور مبتنی بر متاورس، پدید خواهند آمد تا تجربیات یادگیری رسمی و غیررسمی غنی، ترکیبی را در پردیس‌های مجازی سه‌بعدی آن‌لاین فراهم کنند. حضور از راه دور، زبان بدن آواتار و حالت صورت، مشارکت مجازی را به همان اندازه مؤثر می‌سازد. علاوه بر این، واقعیت ترکیبی اجتماعی در متاورس می‌تواند آموزش‌های فعال ترکیبی را فعال کند که دانش عمیق‌تر و پایدارتر را پرورش می‌دهد. مهم‌تر از آن، می‌تواند مشارکت جهانی را در شرایط برابر، بدون محدودیت‌های جغرافیایی، امکان‌پذیر سازد. سارسواتی<sup>۱۱</sup> (۲۰۲۲) [۱۲] در مقاله «متاورس: تکنولوژی بزرگ بعدی» به تعریف متاورس، محدودیت‌ها، ویژگی و مزایای متاورس پرداخته است. همان‌طور که متاورس رشد می‌کند، فضاهای آن‌لاینی ایجاد می‌کند که در آن تعاملات کاربر چندبعدی‌تر از فناوری فعلی پشتیبانی می‌شود. اپادهای و خاندلوال<sup>۱۲</sup> (۲۰۲۲) [۱۴] در مقاله «متاورس: آینده آموزش همه‌جانبه» بررسی پذیرش متاورس به‌عنوان یک اکوسیستم آموزشی را انجام داده‌اند. این مقاله در بحث فعلی در مورد ارتباط متاورس برای آموزش متمرکز قرار می‌گیرد. گزارش‌ها،

<sup>9</sup>Valerie Hill & Alyse Dunavant-Jones & A. Marie Vans

<sup>10</sup>Stephen Taylor & Shamit Soneji

<sup>11</sup>Sarswati

<sup>12</sup>Ashwani Kumar Upadhyay & Komal Khandelwal

مطالعات و پیشرفت‌های اخیر نشان می‌دهد که آموزش فراگیر پتانسیل زیادی دارد. به نظر می‌رسد آینده آموزش در متاورس با مزایایی هم برای کارفرمایان و هم برای کارمندان روشن باشد. اکثر مطالعات یاد شده به معرفی متاورس، ویژگی‌ها و تأثیر آن در یادگیری پرداخته است. از آنجایی که پژوهش‌های بسیار کمی در زمینه کتابخانه‌ها در متاورس (برای مثال هیل و ونس، ۲۰۱۷ [۶]) انجام شده است، این مقاله قصد دارد با گردآوری منابع و مطالعه مروری مقالات مرتبط با متاورس و کتابخانه‌ها، فعالیت‌ها و مزایای متاورس برای کتابخانه را شرح دهد.

یکی از امتیازهای ویژه متاورس محدود نبودن به فضا و مکان فیزیکی است. جایی که افراد می‌توانند یکدیگر را بدون توجه به موقعیت جغرافیایی ملاقات کنند، با دوستان و خانواده دور هم جمع شوند، کار کنند و به کسب درآمد بپردازند، یاد بگیرند، بازی کنند و همچنین دسته‌بندی‌های کاملاً جدید را با استفاده از هدست‌های واقعیت مجازی، عینک‌های واقعیت افزوده، گوشی‌های هوشمند، برنامه‌ها یا دستگاه‌های دیگر ایجاد کنند. متاورس به زبان ساده یک واقعیت دیجیتالی است که می‌تواند ترکیبی از رسانه‌های اجتماعی، واقعیت مجازی (VR)، واقعیت افزوده (AR)، بازی آنلاین و ارزش‌های دیجیتال باشد تا به کاربران امکان تعامل مجازی را بدهد.

## ۴ واقعیت مجازی و واقعیت افزوده

### ۱.۴ واقعیت مجازی (VR)

واقعیت مجازی (VR) تصویری از حضور فیزیکی در دنیای غیرفیزیکی است که با احاطه کردن کاربر در سیستم VR ایجاد می‌شود. تصاویر، صدا یا سایر محرک‌ها یک محیط کلی را فراهم می‌کنند. VR یک تجربه شبیه‌سازی شده است که می‌تواند شبیه یا کاملاً متفاوت از دنیای واقعی باشد (سارسواتی، ۲۰۲۲ [۱۲]).

### ۲.۴ واقعیت افزوده (AR)

واقعیت افزوده (AR) نسخه بهبودیافته دنیای فیزیکی واقعی است که از طریق استفاده از عناصر بصری دیجیتال، صدا یا سایر محرک‌های حسی ارائه شده از طریق فناوری به دست می‌آید (سارسواتی، ۲۰۲۲ [۱۲]).

سارسواتی (۲۰۲۲) مزایای متاورس را این‌گونه بیان می‌کند:

۱. باعث ایجاد سرگرمی می‌شود و مردم را دور هم جمع می‌کند تا اوقات خوبی سپری کنند.
۲. با حضور کلاس‌های درسی و آموزشی در متاورس به دلیل حس حضور مشترک، مشارکت افزایش می‌یابد.
۳. مصرف‌کنندگان می‌توانند محصولات را قبل از خرید آزمایش کنند.
۴. ارتقاء سیستم عامل‌های رسانه‌های اجتماعی.
۵. برنامه‌های کاربردی در کسب و کار و آموزش.



## ۵ حضور کتابخانه‌ها در متاورس

حضور در چنین فضایی برای کتابداران ناآشنا نبود زیرا آنها قبلاً تجربه حضور در «زندگی دوم»<sup>۱۳</sup> را داشتند (هیل، جونز، ونس، ۲۰۱۷) [۶]. حضور کتابخانه‌ها نیز مانند دیگر سازمان‌ها و صنایع برای همگامی با سرعت پیشرفت فناوری و پررنگ ماندن نقش خود ضروری به نظر می‌رسد.

مؤسسه پزشکی و دندانپزشکی پیشرفته (IPPT) در دانشگاه ساینس مالزی اولین دانشگاه در مالزی است که دارای کتابخانه فضایی در متاورس است که انواع محیط‌های دیجیتال متصل به دنیای مجازی را بدون کامپیوتر ارائه می‌دهد. مواد منابع به طور خودکار در یک پورتال وب به نام «GoVR» نمایش داده می‌شود تا کاربران بتوانند به اطلاعات در قالب سه بعدی تعاملی تر دسترسی داشته باشند. برای ورود به دنیای متاورس، همه به یک دستگاه تخصصی مانند هدست واقعیت مجازی نیاز دارند. در حال حاضر کتابخانه IPPT با همکاری بخش فناوری اطلاعات، یک سیستم آن لاین داخلی به نام «VR Discovery» ایجاد کرده است و از طریق این سیستم داخلی می‌تواند منابع اطلاعاتی کتابخانه مانند مواد تصویربرداری، مدل‌های تشریحی، کتاب‌های الکترونیکی، اسناد و موارد دیگر را به قالب سه بعدی تبدیل کند. محتوای منبع به طور خودکار در یک پورتال وب به نام «GoVR» نمایش داده می‌شود تا کاربران بتوانند به اطلاعات در قالب سه بعدی تعاملی تر دسترسی داشته باشند (گارسیا، ۲۰۲۲) [۱۰].

## ۶ مزایای متاورس و دنیای مجازی برای کتابداران

طبق برداشت‌ها از گفته‌های دنیل هیل (۲۰۱۷) [۶] مزایای متاورس برای کتابداران را می‌توان این گونه دسته‌بندی کرد:

**حس حضور مشترک:** مزیت مهمی که در دنیای مجازی، فراتر از وبینارها یا پلتفرم‌های یادگیری آنلاین مانند مودل یا تخته سیاه، یافت می‌شود، «حس حضور مشترک» است که فرد هنگام تجسم به عنوان یک آواتار و تعامل در زمان واقعی با دیگر زبان‌آموزان احساس می‌کند.

**سفرهای میدانی:** این ابزارها مزایایی را برای یادگیری و همکاری از راه دور به صورت همزمان و ناهمزمان فراهم می‌کنند.

**توسعه حرفه‌ای:** توسعه حرفه‌ای می‌تواند در دنیای مجازی از طریق کارگاه‌ها، سمینارها و نشست‌ها انجام شود.

**کاهش هزینه‌ها:** شرکت در کنفرانس‌ها، نمایشگاه‌ها، بحث‌های کتاب و رویدادها در دنیای مجازی مقرون به صرفه است. هیچ بلیط هواپیما، هتل، تاکسی یا غذا در جاده مورد نیاز نیست. علاوه بر این، فرد از سرگردانی در سالن‌های یک مرکز همایش برای یافتن جلسات مورد علاقه، پاهایش درد نمی‌گیرد! نمایشگاه‌ها و پوستره‌های

<sup>13</sup>Second Life

تحقیقاتی در دنیای مجازی به همان شیوه‌ای ارائه می‌شوند که در سمپوزیوم‌های دانشگاهی یا کنفرانس‌های آموزشی مشاهده می‌شود.

**کسب تجربه:** دنیای مجازی فرصت‌هایی را برای تجربیاتی فراهم می‌کند که در دنیای فیزیکی نمی‌توان آنها را تجربه کرد، زیرا برخی تجربه‌ها بسیار خطرناک، بسیار گران یا به‌سادگی غیرممکن هستند.

## ۷ فعالیت‌های کتابداران در متاورس

**آموزش سواد اطلاعاتی:** پرداختن به نیازهای سواد اطلاعاتی برای فراگیران در دنیای مجازی شامل کاتالوگ شبیه‌سازی‌های آموزشی و کاتالوگ آموزشی است (هیل، ۲۰۱۷) [۶].

**آموزش کاربران:** کاربران برای آشنایی با محیط کتابخانه، نحوه استفاده از منابع و پرسش سؤالات خود می‌توانند به‌صورت یک تور مجازی از این فضا استفاده کنند (تانگ، ۲۰۲۱) [۷].

**خدمات مرجع:** اکثر کاربران کتابخانه و نیز افرادی که حاضر نیستند به‌صورت حضوری به کتابخانه بیایند، تمایل دارند از اینترنت و اطلاعات شبکه‌ای استفاده کنند. مرجع مجازی زنده در واقع نوعی خدمت مرجع مجازی است که برای ارائه خدمات به کاربران مجازی از گفتگوی اینترنتی یا پیام‌رسانی مبتنی بر متن استفاده می‌کند و از این لحاظ به مرجع رو در رو یا سنتی شبیه است (حسینی و میرحسینی، ۱۳۹۵) [۱]. حال با وجود متاورس محیطی پدید می‌آید که کاربر و کتابدار بدون حضور در کتابخانه به مصاحبه مرجع می‌پردازند و با هم تعامل رو در رو دارند و به‌همین دلیل مشکلات ارتباط الکترونیکی از قبیل خوب درک نکردن نیاز کاربر که در قالب پیام نوشته شده یا درست متوجه نشدن منظور کتابدار، راهنمایی‌های بیشتر در صورت نیاز و ... به‌سادگی صورت می‌پذیرد.

**ترویج کتابخوانی:** متاورس باعث ترویج سریع و آسان کتابخوانی می‌شود (اصنافی، ۱۴۰۱) [۱].

**ارائه مطلب با کیفیت بالا:** به اشتراک گذاشتن منابع در متاورس باعث بالاتر رفتن کیفیت ارائه مطالب می‌شود، زیرا در آنجا مراجعه‌کننده وجود کتابدار را حس می‌کند و تعامل صورت می‌گیرد (میتساکیدیس، ۲۰۲۲) [۱۱].

**قصه‌خوانی و اجرای نمایش برای کودکان:** کتابداران از سراسر دنیا بدون نیاز به حضور فیزیکی در محلی خاص می‌توانند با ساختن آواتارهای مختلف و اختصاص برنامه‌ای برای قصه‌خوانی و اجرای نمایش برای کودکان باعث ایجاد جاذبه‌های بصری شود و کودکان را مشتاق به مطالعه و شنیدن بکنند.

**برگزاری کنفرانس، همایش، نمایشگاه‌ها:** با توجه به حس حضور مشترکی که متاورس به ما می‌دهد لذت حضور در همایش‌ها و نمایشگاه‌ها افزایش پیدا می‌کند. همچنین افراد با احساس حضور در نمایشگاه‌ها قدم زدن در آن مکان‌ها حسی شبیه به واقعیت را تجربه می‌کنند.

## برگزاری کلاس‌های آموزشی و کارگاه‌ها

ماشینیمایا: ماشینیمایا<sup>۱۴</sup> (فیلم گرفته شده در محیط مجازی)

شبیه‌سازی‌های تاریخی: مانند تئاتر گلوب شکسپیر

شبیه‌سازی کتابخانه: تعامل زنده با یک کتابدار مجازی یا منبع (هیل، ۲۰۱۰) [۶].

## ۸ اقدامات لازم برای حضور در متاورس

- تربیت آرشویست و کتابداران متخصص با دانش روز
- تهیه استانداردهای جدید برای ارائه خدمات آرشویی و دیگر خدمات
- توسعه ارتباط بین سامانه‌های اطلاعاتی و ایجاد یکپارچگی
- بهره‌گیری از هوش مصنوعی در ارائه خدمات اطلاعاتی (اصنافی، ۱۴۰۱) [۱].

## ۹ بحث و نتیجه‌گیری

در عصر امروزی ما با نسل دیجیتال رو به رو هستیم. کاربران دیجیتال تمایل کمتری به حضور فیزیکی و روند کند و سنتی کارها دارند. آنها با این فضا رشد کرده‌اند، کلاس‌ها و آموزش‌های مجازی را تجربه کرده‌اند. کتابداران بیش از یک دهه است که در دنیای مجازی پیشگام بوده‌اند و برای هرگونه خدماتی که به شکل مجازی قابل استفاده است مانند تدریس پیش‌تاز بوده‌اند (هیل، جونز، ونس، ۲۰۱۷) [۶]. کتابداران با توجه نسل جدید کاربران باید نیازهای اطلاعاتی و تمایلات آنها را در نظر بگیرد. برای حضور در متاورس ابتدا باید به اقداماتی مثل تربیت و آموزش کتابداران آشنا با دانش روز بپردازیم، همچنین محیطی مناسب برای کتابخانه طراحی کنیم و از خدمات هوش مصنوعی در ارائه اطلاعات بهره بگیریم. آنچه روشن است این که متاورس محیطی برای یادگیری و آموزش است. یادگیری در متاورس به دلیل حضور مجازی کیفیت بهتری پیدا می‌کند، زیرا مشارکت و تعامل بیشتر می‌شود. کاربران می‌توانند به وسیله آواتارهایشان در فضاهای کتابخانه‌ای که با آنها فاصله زیادی دارند، قدم بزنند، از منابع آنها استفاده کنند و با محیط و خدمات آنها آشنا شوند. با توجه به پژوهش انجام شده، کتابخانه‌ها می‌توانند فعالیت‌های بسیاری در متاورس انجام دهند و جایگاه خود را در این تکنولوژی جدید تثبیت کنند و با فعالیت‌های قصه‌گویی و کتابخانه‌ای، نشست‌های نقد و معرفی کتاب و اجرای نمایش حین کتابخوانی باعث علاقه‌مندی بیشتر کاربران به خصوص کودکان به مطالعه و کتاب شوند.

<sup>14</sup>Machinima

## ۱.۹ پیشنهادها

مطالعات انجام شده در حوزه حضور کتابخانه‌ها در متاورس و نقش‌ها آن بسیار کم است؛ از این رو پژوهشگران علاقه‌مند می‌توانند به موضوعات پیشنهادی زیر بپردازند:

- ارزیابی عملکرد خدمات کتابخانه‌ای در متاورس
- نیازهای جدید در کتابخانه‌های متاورس
- معرفی تکنولوژی‌های واقعیت افزوده برای بهبود کیفیت خدمات کتابخانه‌ای

## مراجع

- [۱] حسینی، زهرا سادات و میرحسینی، زهره (۱۳۹۵). آینده فن‌آوری در کتابخانه‌های عمومی (چالش‌ها و فرصت‌ها)، چهارمین کنفرانس ملی توسعه پایدار در علوم تربیتی و روانشناسی، مطالعات اجتماعی و فرهنگی، تهران. <https://civilica.com/doc/546752>
- [۲] فرخی، محمدجواد و شهامت، نادر (۱۴۰۰). نقش و کاربست متاورس در فرآیند یادگیری، چهارمین همایش بین‌المللی روانشناسی، علوم تربیتی و مطالعات اجتماعی، همدان. <https://civilica.com/doc/1450391>
- [۳] اصنافی، امیررضا (۱۴۰۱). کتابخانه از زندگی دوم تا متاورس (کارگاه آموزشی). نمایشگاه کتاب، تهران.
- [4] Kruger, Hilda (2005). I, librarian. INFORMATION TECHNOLOGY AND LIBRARIES, (9), 123-129.
- [5] Hill, V. (2010), Are Librarians Needed in the Metaverse?. Texas Library Journal, 86(1), 8-10.
- [6] Hill, Valerie, Vans, A. Marie, and Dunavant-Jones, Alyse. (2017). Metaverse libraries: Communities as resources. Journal of Virtual studies, 8(2), 27-37.
- [7] Tang, Yingqi. (2021). Help first-year college students to learn their library through an augmented reality game. The Journal of Academic Librarianship. 47. 102294. 10.1016/j.acalib.2020.102294.
- [8] Chohan, Usman W., Metaverse or Metacurse? (February 19, 2022). Available at SSRN: <https://ssrn.com/abstract=4038770>
- [9] Hughes, I. (2022). The Metaverse: Is it the Future?. ITNOW, 64(1), 22-23.
- [10] gurcia, Barbara (2022). Malasia, primero en configurar una biblioteca de medicina en el metaverso. <https://www.saludiarario.com/malasia-biblioteca-metaverso-medicina>
- [11] Mystakidis, S. (2022). Metaverse. Encyclopedia, 2, 486-497.
- [12] Sarswati (2022). Metaverse: the next big technology. 3(6).
- [13] Taylor, S. and Soneji, S. (2022) Bioinformatics and the Metaverse: Are We Ready?. Front. Bioinform.

- [14] Upadhyay, A.K. and Khandelwal, K. (2022), "Metaverse: the future of immersive training," Strategic HR Review, Vol. 21 No. 3, pp. 83-86.





# اثر مشاهده تصاویر خویش انداز زنان تأثیر گذار اینستاگرام بر گرایش خانم‌ها به انجام جراحی‌های زیبایی با میانجی‌گری نارضایتی چهره‌ای

فاطمه تمنائی<sup>۱</sup>، پگاه نجات<sup>۲</sup>

<sup>۱</sup> کارشناسی ارشد، دانشکده علوم تربیتی و روان‌شناسی، دانشگاه شهید بهشتی، تهران، ایران  
tfmpsihologist@gmail.com

<sup>۲</sup> استادیار گروه روان‌شناسی، دانشکده علوم تربیتی و روان‌شناسی، دانشگاه شهید بهشتی، تهران، ایران  
p\_nejat@sbu.ac.ir

## چکیده

هدف: این مطالعه با هدف تعیین اثر مشاهده تصاویر خویش‌انداز زنان تأثیرگذار حوزه زیبایی اینستاگرام بر گرایش خانم‌ها به جراحی زیبایی با میانجی‌گری نارضایتی چهره‌ای انجام شد. روش: پژوهش از نوع آزمایشی با عامل بین آزمودنی نوع تصاویر اینستاگرامی مورد مشاهده (زنان تأثیرگذار اینستاگرام حوزه زیبایی، زنان بازیگر فعال در اینستاگرام، غیرانسان) بود. شرکت‌کنندگان نمونه‌ای در دسترس از ۲۰۱ خانم ۱۶ تا ۴۰ ساله بودند که پس از مشاهده تصاویر، به سؤالات مربوط به نارضایتی چهره‌ای و گرایش به جراحی زیبایی پاسخ دادند. برای آزمودن روابط مفروض از تحلیل کواریانس و تحلیل رگرسیون استفاده شد. یافته‌ها: مشاهده تصاویر تأثیرگذاران زیبایی منجر به گرایش بالاتر به انجام جراحی زیبایی بدن نسبت به مشاهده تصاویر بازیگران شد. نارضایتی چهره‌ای اثر نوع تصاویر مورد مشاهده بر گرایش به انجام جراحی زیبایی را میانجی‌گری نکرد. اثر مستقیم نوع تصاویر مورد مشاهده بر گرایش به انجام جراحی زیبایی بدن و صورت معنادار بود. نتیجه‌گیری: ارائه تصاویر خویش‌انداز اینستاگرامی کمتر از حد انتظار بر نارضایتی چهره‌ای و گرایش به انجام جراحی زیبایی صورت و بدن تأثیرگذار بود. فعال شدن واکنش‌های تدافعی در پاسخ به شهرت می‌تواند یک توضیح ممکن باشد. یافته‌ی حاضر به آگاهی متخصصان حیطه سلامت از عوامل اثرگذار بر قصد افراد برای جراحی‌های زیبایی می‌افزاید.

**کلمات کلیدی:** تأثیر گذاران اینستاگرام، نارضایتی چهره‌ای، گرایش به انجام جراحی زیبایی.

## ۱ مقدمه

در سال ۲۰۲۰ حدود ۱۱ میلیون جراحی زیبایی و ۱۵ میلیون عمل زیبایی بدون جراحی در جهان صورت گرفته است و افراد ۱۹ تا ۴۰ ساله بیشترین متقاضیان این‌گونه عمل‌ها بوده‌اند (انجمن بین‌المللی جراحی زیبایی

پلاستیک، ۲۰۲۰) که ۹۲ درصد آن را زنان تشکیل می‌دهند (انجمن جراحان پلاستیک آمریکا، ۲۰۲۰). طبق آمارهای غیررسمی، در سال ۲۰۲۱ سهم ایران حدود ۱۷۵۰۰۰ عمل زیبایی بوده است (سرویس گردشگری پزشکی جراحی ایران، ۲۰۱۹) و در رتبه‌بندی سال ۲۰۲۰، ایران از نظر تعداد جراحان زیبایی پلاستیک در رتبه ۲۸ قرار گرفت (انجمن بین‌المللی جراحی زیبایی پلاستیک، ۲۰۲۰). با توجه به نوع پوشش زنان ایران که چهره را بیشتر از سایر اندام‌ها می‌نمایاند، جراحی‌های زیبایی صورت به ویژه بینی در ایران پرطرفدار است (راستمنش، گلوک و شادمان، ۲۰۰۹).

در حال حاضر استفاده از رسانه‌های اینترنتی مانند شبکه‌های اجتماعی توئیتر، فیس بوک و اینستاگرام<sup>۱</sup> به سرعت افزایش یافته است (سنسیس، ۲۰۱۸). اینستاگرام با حدود هشتصد میلیون کاربر فعال نسبت به سایر شبکه‌های اجتماعی رشد قابل توجهی داشته و مورد استقبال مردم کشورهای مختلف قرار گرفته است (اسمیت و اندرسون، ۲۰۱۸). کاربران در اینستاگرام به طور روزانه ممکن است تصاویر یا فیلم‌هایی را از خود یا موضوعات مورد علاقه‌شان به اشتراک با سایر کاربران و دنبال‌کنندگان بگذارند. استفاده از شبکه‌های اجتماعی و فعالیت‌های رایجی که در این رسانه‌ها انجام می‌شود، باعث به وجود آمدن نگرانی در مورد ظاهر و تصویر بدن در استفاده‌کنندگان از این رسانه‌ها شده است (فردولی، ویلبرگر و وارتانیان، ۲۰۱۸: هلند و تیگمان، ۲۰۱۶). تأثیرگذاران<sup>۲</sup> فضای مجازی افراد مشهوری هستند که فقط به واسطه فعالیت در شبکه‌های اجتماعی نظیر اینستاگرام به شهرت رسیده‌اند و توانسته‌اند تعداد زیادی از کاربران را پیرو خود کنند. این افراد به واسطه تأثیرات فراوانی که می‌توانند بر پیروان خود بگذارند، میکروسلبیتی<sup>۳</sup> یا تأثیرگذار نامیده شده‌اند (چای، ۲۰۱۸). تأثیرگذاران ممکن است مدل‌های آرایشی و زیبایی<sup>۴</sup> و یا افراد مشهور و شناخته شده فعال در اینستاگرام باشند (چای، ۲۰۱۸). آن‌جی (۲۰۱۹) دریافت که تأثیرگذاران اینستاگرام تا حدی بر پیروان خود نفوذ دارند و به صورت مستقیم یا غیرمستقیم درک آن‌ها را از زیبایی و جراحی‌های زیبایی به چالش می‌کشند.

آنچه از مرور تحقیقات پیشین (فردولی، بینکو و وارتانیان، ۲۰۱۷؛ تیگمان، براون، زاگردو و توماس، ۲۰۱۷؛ تیگمان، هایدن، براون و ولدهوئیس، ۲۰۱۸؛ فردولی و همکاران، ۲۰۱۸؛ کلیمانز، دالمانز، کاربات و آنسچنز، ۲۰۱۸) برداشت می‌شود این است که در زمینه زنان تأثیرگذار حوزه زیبایی اینستاگرام به عنوان نمایندگان نوظهور صنعت زیبایی شبکه‌های اجتماعی و بررسی اثرات مشاهده تصاویر خویش‌انداز این افراد بر گرایش زنان جوان به انجام جراحی‌های زیبایی، خلاء پژوهشی وجود دارد.

دیدگاه نظریه مقایسه اجتماعی<sup>۵</sup> فستینگر (۱۹۵۴)، توضیح می‌دهد که مقایسه‌های اجتماعی زمانی بیشتر صورت می‌گیرد که هدف مقایسه با خود فرد شباهت بیشتری داشته باشد و افراد تمایل دارند خود را با کسانی که احساس شباهت بیشتری نسبت به آن‌ها دارند مقایسه کنند. در اینستاگرام دنبال کردن و مشاهده کردن تصاویر افراد مشهور و مدل‌ها نسبت به سایر اهداف مقایسه‌ای رایج‌تر است (فردولی و همکاران، ۲۰۱۸).

<sup>1</sup>Instagram

<sup>2</sup>Influencers

<sup>3</sup>Micro Celebrity

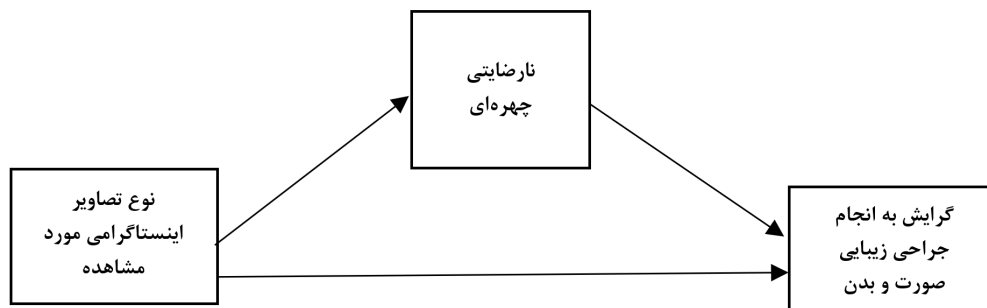
<sup>4</sup>Beauty influencers

<sup>5</sup>Social Comparison

کاربران، تأثیرگذاران اینستاگرام را از لحاظ میزان شباهت در جایگاهی نزدیک‌تر با خود احساس می‌کنند تا با افراد مشهور سنتی در اینستاگرام که امکانات پرهزینه‌شان غیرقابل دستیابی‌تر هست (دین، ۲۰۱۷). از این سو افراد بیشتر تمایل دارند خود را با تأثیرگذاران مقایسه کنند (چای، ۲۰۱۸). در پژوهش حاضر با توجه به استدلال‌های مطرح شده و بهره‌گیری از نظریه مقایسه اجتماعی، زنان بازیگر به عنوان گروهی که از نظر شهرت و زیبایی قابل رقابت با زنان تأثیرگذار حوزه زیبایی اینستاگرام هستند در نظر گرفته شدند و اثرات مشاهده تصاویر اینستاگرامی زنان تأثیرگذار با این گروه مقایسه شد (**فرضیه ۱**: مشاهده تصاویر خویش‌انداز زنان تأثیرگذار ایرانی حوزه زیبایی به علت احساس شباهت و نزدیکی بیشتری که افراد با تأثیرگذارانی که هویت و شهرتشان صرفاً برخاسته از اینستاگرام است دارند، در مشاهده‌کنندگان منجر به گرایش بالاتر برای انجام جراحی زیبایی نسبت به زنان بازیگر ایرانی و گروه غیرانسان می‌شود).

میان مشاهده تصاویر خویش‌انداز که عمدتاً ویرایش، اصلاح یا گزینش شده‌اند با نارضایتی چهره‌ای رابطه وجود دارد (وانگ و همکاران، ۲۰۱۹). نارضایتی چهره‌ای<sup>۶</sup> احساس عدم رضایتی افراد از چهره و رنگ پوست خود است (تامپسون و هاینبرگ، ۱۹۹۵، تیگمان و زینوو، ۲۰۱۹). یکی از فعالیت‌های خاصی که در شبکه‌های اجتماعی و اینستاگرام اخیراً خیلی رواج پیدا کرده است، گرفتن و ارسال عکس‌هایی از خود تحت عنوان خویش‌انداز<sup>۷</sup> است (جاگر، ۲۰۱۹). بیشتر خویش‌اندازهایی که گرفته می‌شوند شامل تصاویری از چهره افراد هستند تا تصاویری از اندام افراد. بنابراین هنگام مشاهده و ویرایش خویش‌اندازها جذابیت‌های چهره‌ای برجسته‌تر می‌شوند (وانگ و همکاران، ۲۰۱۹؛ سان، ۲۰۲۱). پژوهش‌های چندی نشان می‌دهند که نارضایتی از چهره مانند نارضایتی از بدن می‌تواند تمایل زنان را به سمت انتخاب و انجام جراحی‌های زیبایی هدایت کند (سان، ۲۰۲۱). برخی از مطالعات به این نتیجه رسیده‌اند که مشاهده تصاویر خویش‌انداز ایده‌آل زنان در رسانه‌های اجتماعی باعث می‌شود سایر زنان از ظاهر چهره خود نارضایتی بیشتری را تجربه کنند و انگیزه بیشتری برای تغییرات و دست‌کاری‌های جنبه‌های مختلف صورت خود را داشته باشند (فردولی و همکاران، ۲۰۱۸). بنابراین بین نارضایتی‌های ظاهری و اتخاذ رفتارهای جبران‌کننده، اقدامات و جراحی‌های زیبایی نیز رابطه وجود دارد (اوبرین، کیوتی، مینتو، پیپلز، هوپر، کل و همکاران، ۲۰۰۹؛ تیگمان و مک‌گیل، ۲۰۰۴). با این استدلال که بین مقایسه‌های ظاهری را به بالا در اینستاگرام و نارضایتی‌های ظاهری ارتباط وجود دارد (هندریکس، آرپان، کلیتون و ریدگوی، ۲۰۱۷)، نارضایتی چهره‌ای را به عنوان متغیر میانجی ارائه و پیشنهاد می‌دهیم. (**فرضیه ۲**: نارضایتی چهره‌ای اثر نوع تصاویر اینستاگرامی مورد مشاهده بر گرایش زنان به انجام جراحی‌های زیبایی را میانجی‌گری می‌کند، به گونه‌ای که مشاهده تصاویر خویش‌انداز تأثیرگذاران زیبایی اینستاگرام نسبت به تصاویر بازیگران یا تصاویر غیرانسان منجر به نارضایتی چهره‌ای بیشتر و در نتیجه آن، گرایش بیشتر به انجام جراحی‌های زیبایی صورت و بدن می‌شود). شکل ۱ مدل مفهومی روابط مفروض بین متغیرهای پژوهش را ارائه می‌دهد.

<sup>۶</sup>Facial Dissatisfaction<sup>۷</sup>Selfies



شکل ۱: مدل مفهومی روابط مفروض بین متغیرهای پژوهش

این مطالعه بخصوص در بافت‌شناسی فرهنگی-اجتماعی کشور ایران ضرورت پیدا می‌کند. در کشوری که تصاویر زیبایی زنان در مجلات، تبلیغات و برنامه‌های تلویزیونی آن ممنوع است، اینستاگرام اولین بستر آزاد برای ارائه‌ی این تصاویر محسوب می‌شود و لذا نمی‌توان فرض نمود یافته‌های فرهنگ‌های غربی در این خصوص قابل تعمیم به نمونه ایرانی باشد. در نتیجه ضرورت بررسی اثرات مشاهده تصاویر اینستاگرامی بر کاربران ایرانی احساس می‌شود و این مطالعه با هدف مقایسه اثر مشاهده تصاویر خویش‌انداز دوگروه از زنان شناخته شده ایرانی (زنان تأثیرگذار زیبایی و زنان بازیگر ایرانی) در اینستاگرام بر گرایش به انجام جراحی‌های زیبایی صورت و بدن انجام شد.

## ۲ روش، شرکت‌کنندگان و ابزار پژوهش

مطالعه حاضر آزمایشی و از نوع پس‌آزمون با عامل برون آزمودنی سه سطحی نوع تصاویر اینستاگرامی مورد مشاهده (تصاویر زنان تأثیرگذار ایرانی حوزه زیبایی در اینستاگرام، تصاویر زنان بازیگر ایرانی فعال در اینستاگرام، و تصاویر غیرانسان) بود.

### ۱.۲ شرکت‌کنندگان

تعداد کل شرکت‌کنندگان ۲۷۰ نفر با میانگین سنی ۲۴ سال و انحراف استاندارد ۵۶.۴ بود که به طور داوطلبانه برای شرکت در مطالعه آنلاین مراجعه نمودند. خانم بودن و بازه سنی ۱۶ تا ۴۰ سال به عنوان ملاک‌های ورود در ابتدای مطالعه ذکر شده بود. نمونه نهایی متشکل از تعداد ۲۰۱ نفر شد که تحلیل‌های آماری روی آن‌ها انجام گرفت. یک گروه محدودتر نیز از میان نمونه نهایی بر اساس زمان کل آزمون تشکیل شد که تمام مدل‌های میانجی‌گری تعدیل‌شده علاوه بر نمونه نهایی، روی این گروه هم به طور مجزا تکرار شد. از نظر توصیف ویژگی‌های جمعیت‌شناختی و سطح تحصیلات، کارشناسی با درصد فراوانی ۵۸/۲ و دکتری حرفه‌ای با درصد فراوانی ۰/۵، به ترتیب بیشترین و کمترین فراوانی را در میان گروه نمونه داشتند. از لحاظ سابقه اقدام به جراحی زیبایی، ۸۴/۶ درصد از گروه نمونه فاقد سابقه انجام عمل‌های زیبایی بودند. عمل زیبایی بینی با فراوانی ۸ درصد، تتوی ابرو با فراوانی ۳/۵ درصد و تزریق ژل و بوتاکس با فراوانی ۲/۵ درصد به ترتیب

شایع‌ترین عمل‌های زیبایی در میان افراد با سابقه اقدامات زیبایی در گروه نمونه بود. از لحاظ سطح اقتصادی، میانگین ۳/۰۹ و انحراف استاندارد ۰/۷۲ بود.

## ۲.۲ ابزار پژوهش

### ۱.۲.۲ نارضایتی چهره‌ای

به منظور سنجش نارضایتی چهره‌ای از مقیاس نارضایتی چهره‌ای تیگمان و همکاران (۲۰۱۸) استفاده شد. این مقیاس متشکل از دو گویه برای نارضایتی چهره‌ای که شامل عدم رضایت از چهره و عدم رضایت از پوست صورت بود. هر کدام از گویه‌های این مقیاس شامل یک محور افقی ۱۰۰ درجه‌ای بود که با دو نقطه انتهایی (۰=اصلا) و (۱۰۰=بسیار زیاد) برچسب گذاری شده بود. ضریب آلفای کرونباخ مقیاس نارضایتی چهره‌ای در مطالعه تیگمان و زینوو (۲۰۱۹)، ۰/۷۸ گزارش شد و در این مطالعه، ۰/۶۹ بدست آمد.

### ۲.۲.۲ گرایش به انجام جراحی زیبایی صورت و بدن

به منظور سنجش گرایش به انجام جراحی زیبایی صورت و بدن به ترتیب از دو پرسش، «چقدر احتمال می‌دهید که در ده سال آینده نوعی جراحی زیبایی روی صورت تان انجام دهید؟» و «چقدر احتمال می‌دهید که در ده سال آینده نوعی جراحی زیبایی روی بخشی از بدن خود غیر از صورت تان انجام دهید؟» استفاده شد. پاسخ به این سؤالات از اصلا یا بسیار کم=۱ تا بسیار زیاد=۵ متغیر بود.

### ۳.۲.۲ تماس با اینستاگرام و تأثیرگذاران و میزان آشنایی با تأثیرگذاران

به منظور سنجش میزان استفاده از اینستاگرام و سابقه‌ی دنبال کردن تأثیرگذاران دو پرسش محقق ساخته طراحی شدند. سؤالات شامل «معمولا چقدر از اینستاگرام استفاده می‌کنید؟»، «چقدر افراد سرشناس فعال در اینستاگرام با تعداد فالوورهای زیاد را دنبال می‌کنید؟» بودند. پاسخ به این سؤالات از اصلا یا بسیار کم=۱ تا بسیار زیاد=۷ متغیر بود. به منظور سنجش میزان آشنایی با تأثیرگذاران زیبایی و بازیگران، سؤال «چقدر با این فرد آشنا هستید؟» و برای سنجش میزان آشنایی با تصاویر غیرانسان، سؤال «چقدر با پست‌هایی با این مضمون در اینستاگرام مواجه می‌شوید؟» طراحی شدند. پاسخ به این سؤالات از اصلا یا بسیار کم=۱ تا بسیار زیاد=۵ متغیر بود.

### ۴.۲.۲ سؤالات جمعیت‌شناختی

سؤالات جمعیت‌شناختی شامل سن، جنسیت (زن، مرد)، سطح تحصیلات (از زیردیپلم تا دکتری تخصصی)، وضعیت اقتصادی از (بسیار پایین‌تر از متوسط=۱) تا (بسیار بالاتر از متوسط=۵) بودند. همچنین سؤال «سابقه انجام کدام یک از اقدامات زیبایی زیر را دارید؟» جهت بررسی سابقه اقدامات زیبایی در افراد طراحی شد.

## ۳ شیوه اجرا و روش تحلیل داده

شرکت کنندگان به صورت آنلاین در مطالعه مشارکت داشتند و به طور تصادفی به یکی از سه شرایط آزمایشی عبارتند از گروه زنان تأثیرگذار ایرانی حوزه زیبایی اینستاگرام، گروه زنان بازیگر ایرانی فعال در اینستاگرام و گروه غیرانسان گمارده شدند. در ابتدا فرم رضایت آگاهانه به همراه هدف پوششی از مطالعه جهت پنهان ماندن هدف اصلی از شرکت کنندگان و جلوگیری از سوگیری آنها ارائه شد. قبل از نمایش تصاویر شرکت کنندگان به دو سؤال در رابطه با شاخص تماس با اینستاگرام و تأثیرگذاران پاسخ دادند. تصاویر مربوط به شرایط بازیگران شامل ده عکس خویش انداز از چهره ده بازیگر خانم ایرانی بود. تصاویر مربوط به شرایط تأثیرگذاران زیبایی شامل ده عکس خویش انداز از چهره ده تأثیرگذار اینستاگرامی خانم ایرانی فعال در حوزه های زیبایی، آرایشی و مدلینگ بود. تصاویر مربوط به شرایط غیرانسان نیز شامل ده عکس از چیدمان فضای خانه، اماکن و مناظر طبیعی و بدون حضور اشخاص بود که متعلق به صفحه اینستاگرامی ده تأثیرگذار اینستاگرامی خانم ایرانی فعال در حوزه های غیرزیبایی بود. تصاویری که در این مطالعه آزمایشی استفاده شدند از صفحه عمومی و رسمی منتسب به افراد شناخته شده ۱۸ تا ۴۰ سال با تعداد دنبال کنندگان بالای نهمصد هزار نفر انتخاب شدند. تمامی تصاویر با شکل و قالب اصلی پست های اینستاگرامی و با حذف متن نظرات و تعداد پسندها (جهت جلوگیری از هرگونه سوگیری) به شرکت کنندگان نمایش داده شدند. هر تصویر به مدت ۱۰ ثانیه در وسط صفحه نشان داده شد و بلافاصله بعد از اتمام زمان نمایش، دو سؤال در زمینه آشنایی با تأثیرگذاران یا بازیگران و احتمال دنبال کردنشان از شرکت کنندگان پرسیده شد. بعد از اتمام نمایش همه تصاویر، به ترتیب مقیاس های نارضایتی چهره ای و دو پرسش گرایش به انجام جراحی زیبایی ارائه شدند. در ادامه شش سؤال از یک پرسشنامه شخصیتی صرفاً جهت تمرکززدایی از دست کاری آزمایشی ارائه شد.

### ۱.۳ روش تحلیل داده ها

به منظور آزمودن اثر نوع تصاویر اینستاگرامی مورد مشاهده بر گرایش به انجام جراحی زیبایی از تحلیل کواریانس استفاده شد. آشنایی با تأثیرگذاران به عنوان متغیر همگام در مدل نهایی لحاظ و کنترل شد. به منظور آزمودن میانجی گری نارضایتی چهره ای در رابطه بین نوع تصاویر اینستاگرامی مورد مشاهده و گرایش به انجام جراحی زیبایی از مدل شماره ۷ ماکروی پروسس<sup>۸</sup> (هیس، ۲۰۱۸) استفاده شد. متغیر مستقل (نوع تصاویر اینستاگرامی مورد مشاهده) جهت ورود به تحلیل رگرسیون به دو متغیر مستقل متفاوت که هر کدام دارای دو سطح بودند کدگذاری تصنعی<sup>۹</sup> شد.

## ۴ یافته ها

شکل ۱ میانگین و انحراف استاندارد نارضایتی چهره ای، گرایش به انجام جراحی زیبایی صورت و بدن و آشنایی با تأثیرگذاران به تفکیک سه گروه آزمایشی را گزارش می دهد.

<sup>۸</sup>PROCESS

<sup>۹</sup>Dummy coded



جدول ۱: میانگین و انحراف استاندارد متغیرهای اصلی پژوهش

گروه غیرانسان n = ۶۸		گروه بازیگران n = ۶۵		گروه تأثیرگذاران زیبایی n = ۶۸		متغیر
انحراف استاندارد	میانگین	انحراف استاندارد	میانگین	انحراف استاندارد	میانگین	
۲۰/۵۴	۳۰/۵۱	۲۱/۸۰	۳۱/۸۸	۲۳/۸۰	۳۱/۲۱	نارضایتی چهره‌ای
۱۱/۰۵	۲/۰۳	۱/۰۸	۱/۹۵	۱/۲۰	۲/۱۵	گرایش به انجام جراحی زیبایی صورت
۰/۸۵	۱/۴۴	۰/۷۱	۱/۲۶	۰/۹۱	۱/۶۰	گرایش به انجام جراحی زیبایی بدن
۰/۷۵	۲/۹۳	۰/۹۰	۲/۳۸	۰/۵۸	۱/۶۴	آشنایی با تأثیرگذاران

جدول ۲ نتایج تحلیل کواریانس با متغیر مستقل نوع تصاویر اینستاگرامی مورد مشاهده و متغیرهای وابسته گرایش به انجام جراحی زیبایی صورت و بدن با کنترل آشنایی با تأثیرگذاران را ارائه می‌دهد. چنانچه ملاحظه می‌شود اثر نوع تصاویر اینستاگرامی مورد مشاهده بر گرایش به انجام جراحی زیبایی بدن معنادار بود. پیگیری این معناداری با استفاده از آزمون تعقیبی بونفرونی<sup>۱۰</sup> نشان داد که تفاوت میانگین میان تأثیرگذاران زیبایی و بازیگران معنادار بود ( $p = ۰/۰۲۰$ ) و تأثیرگذاران زیبایی با میانگین ۶۸/۱، قصد بیشتری برای انجام جراحی زیبایی بدن نسبت به گروه‌هایی که تصاویر بازیگران با میانگین ۲۶/۱ را مشاهده نمودند، داشتند.

جدول ۲: نتایج تحلیل کواریانس اثر نوع تصاویر اینستاگرامی مورد مشاهده بر گرایش به انجام جراحی زیبایی با کنترل آشنایی با تأثیرگذاران

متغیر وابسته	منبع واریانس	مجموع مجذورات	درجه آزادی	F	معناداری	مجذور اتای
آشنایی با تأثیرگذاران	۶/۱۸	۱	۵/۰۹	۰/۰۳	۰/۲۵	
گرایش به انجام جراحی زیبایی صورت	نوع تصاویر اینستاگرامی مورد مشاهده خطا	۴/۹۱ ۲۳۹/۱۸	۲ ۱۹۷	۲/۰۲	۰/۱۳۵	۰/۰۲
آشنایی با تأثیرگذاران	۱/۴۵	۱	۲/۰۹	۰/۰۱	۰/۱۵۰	
گرایش به انجام جراحی زیبایی بدن	نوع تصاویر اینستاگرامی مورد مشاهده خطا	۵/۱۹ ۱۳۶/۱۵	۲ ۱۹۷	۳/۷۶	۰/۰۲۵	۰/۰۴

جدول ۳ نتایج تحلیل رگرسیون پیش‌بینی نارضایتی چهره‌ای را نشان می‌دهد. طبق این نتایج، اثرات متغیرهای مستقل بازیگران - تأثیرگذاران و غیرانسان - تأثیرگذاران بر نارضایتی چهره‌ای غیرمعنادار بود.

<sup>10</sup>Bonferroni

جدول ۳: نتایج رگرسیون پیش‌بینی نارضایتی چهره‌ای در مدل میانجی‌گری تعدیل شده

متغیر مورد پیش‌بینی	متغیر پیش‌بین	ضریب غیراستاندارد	خطای استاندارد	سطح معناداری	حد پایین بازه اطمینان (بوت استری)	حد بالا بازه اطمینان (بوت استری)
نارضایتی چهره‌ای	متغیر بازیرگان-تأثیرگذاران زیبایی	۰/۲۵	۴/۰۶	۰/۹۵۰	-۷/۷۲	۸/۱۰
	متغیر غیرانسان-تأثیرگذاران زیبایی	۰/۹۱	۴/۶۹	۰/۸۴۶	-۷/۹۴	۱۰/۱۸

در نتایج تحلیل رگرسیون شکل ۴ چنانچه ملاحظه می‌شود، اثر مستقیم متغیر مستقل بازیرگان-تأثیرگذاران بر گرایش به انجام جراحی زیبایی بدن معنادار بود. با ذکر این نکته که این مدل در گروه محدودتر بر اساس زمان کل آزمون هم تکرار شد و یافته‌های مربوط به اثر مستقیم متغیر مستقل بازیرگان-تأثیرگذاران بر گرایش به انجام جراحی زیبایی صورت که در آن ضریب رگرسیون  $-۰/۴۲$ ، خطای استاندارد  $۰/۲۰$ ، سطح معناداری  $۰/۰۳۵$  و بازه اطمینان بوت استری  $[-۰/۸۰, ۰/۰۱]$  کاملاً معنادار شد و ضریب منفی رگرسیون بیانگر آن بود که گرایش به انجام جراحی زیبایی صورت در شرایط تأثیرگذاران بیشتر از شرایط بازیرگان است. بنابراین شرایط تأثیرگذاران زیبایی منجر به گرایش به انجام جراحی زیبایی بالاتر نسبت به شرایط بازیرگان شد. اثر مستقیم متغیر مستقل غیرانسان-تأثیرگذاران بر گرایش به انجام جراحی‌های زیبایی صورت غیر معنادار شد. همچنین اثر نارضایتی چهره‌ای بر گرایش به انجام جراحی زیبایی صورت معنادار شد.

جدول ۴: نتایج تحلیل رگرسیون پیش‌بینی گرایش به انجام جراحی زیبایی توسط نوع تصاویر اینستاگرامی مورد مشاهده با میانجی‌گری نارضایتی چهره‌ای

متغیر وابسته	متغیر پیش‌بین	ضریب غیراستاندارد	خطای استاندارد	معناداری
گرایش به انجام جراحی زیبایی صورت	متغیر مستقل بازیرگان-تأثیرگذاران زیبایی	-۰/۳۵	۰/۱۹	۰/۰۶۵
	متغیر مستقل غیرانسان-تأثیرگذاران زیبایی	۰/۳۸	۰/۲۳	۰/۱۰۱
نارضایتی چهره‌ای	نارضایتی چهره‌ای	۰/۰۱	۰/۰۰	۰/۰۰۲
	آشنایی با تأثیرگذاران	۰/۲۱	۰/۱۰	۰/۰۴۹
متغیر وابسته	متغیر مستقل بازیرگان-تأثیرگذاران زیبایی	-۰/۴۲	۰/۱۵	۰/۰۰۷
	متغیر مستقل غیرانسان-تأثیرگذاران زیبایی	-۰/۳۰	۰/۱۸	۰/۱۰۹
گرایش به انجام جراحی زیبایی بدن	نارضایتی چهره‌ای	۰/۰۰	۰/۰۰	۰/۶۶۴
	آشنایی با تأثیرگذاران	۰/۱۱	۰/۰۹	۰/۲۴۰

جدول ۵ اثرات غیرمستقیم متغیرهای مستقل بر متغیرهای وابسته با میانجی‌گری نارضایتی چهره‌ای در سطوح مختلف مقایسه ظاهری بالاسو را نشان می‌دهند. طبق این نتایج، اثرات غیرمستقیم متغیرهای مستقل بازیرگان-تأثیرگذاران و غیرانسان-تأثیرگذاران در هیچ یک از سطوح گرایش خصلتی به مقایسه ظاهری بالاسو معنادار نشده است. که این موضوع بیانگر عدم میانجی‌گری نارضایتی چهره‌ای در رابطه بین متغیرهای مستقل و گرایش به انجام جراحی زیبایی است.

جدول ۵: اثرات غیرمستقیم متغیرهای مستقل بر گرایش به انجام جراحی زیبایی صورت و بدن با میانجی‌گری نارضایتی چهره‌ای در سطوح مختلف گرایش خصلتی به مقایسه ظاهری بالاسو

متغیر وابسته	متغیر مستقل	گرایش خصلتی به مقایسه ظاهری بالاسو (تعددبگزر)	اندازه اثر غیرمستقیم	خطای استاندارد	حد پایین بازه اطمینان بوت استری	حد بالای بازه اطمینان بوت استری
گرایش به انجام جراحی زیبایی صورت	متغیر مستقل بازگران - تاثیرگذاران زیبایی	(پایین) ۰/۹۲ -	۰/۰۰	۰/۰۶	-۰/۱۱	۰/۱۳
		(متوسط) ۰/۱۲ -	۰/۰۰	۰/۰۴	-۰/۱۰	۰/۰۹
		(بالا) ۰/۹۷	-۰/۰۰	۰/۰۷	-۰/۱۷	۰/۱۳
	متغیر مستقل غیرانسان - تاثیرگذاران زیبایی	(پایین) ۰/۹۲ -	۰/۰۲	۰/۰۶	-۰/۰۸	۰/۱۶
		(متوسط) ۰/۱۲ -	۰/۰۱	۰/۰۵	-۰/۰۹	۰/۱۲
		(بالا) ۰/۹۷	-۰/۰۰	۰/۰۸	-۰/۱۹	۰/۱۶
گرایش به انجام جراحی زیبایی بدن	متغیر مستقل بازگران - تاثیرگذاران زیبایی	(پایین) ۰/۹۲ -	-۰/۰۰	۰/۰۱	-۰/۰۲	۰/۰۳
		(متوسط) ۰/۱۲ -	-۰/۰۰	۰/۰۱	-۰/۰۲	۰/۰۲
		(بالا) ۰/۹۷	-۰/۰۰	۰/۰۱	-۰/۰۳	۰/۰۳
	متغیر مستقل غیرانسان - تاثیرگذاران زیبایی	(پایین) ۰/۹۲ -	-۰/۰۰	۰/۰۱	-۰/۰۲	۰/۰۴
		(متوسط) ۰/۱۲ -	-۰/۰۰	۰/۰۱	-۰/۰۲	۰/۰۳
		(بالا) ۰/۹۷	۰/۰۰	۰/۰۲	-۰/۰۴	۰/۰۴

## ۵ نتیجه‌گیری

مطالعه حاضر با هدف مقایسه اثر مشاهده تصاویر خویش‌انداز دو گروه از زنان شناخته‌شده ایرانی در اینستاگرام (زنان تأثیرگذار زیبایی اینستاگرام و زنان بازیگر ایرانی) بر گرایش به انجام جراحی‌های زیبایی صورت و بدن صورت گرفت و نقش میانجی‌گرانه‌ی نارضایتی چهره‌ای در این رابطه آزمون شد.

در رابطه با فرضیه اول نتایج این پژوهش نشان داد مشاهده تصاویر خویش‌انداز فقط بر گرایش به انجام جراحی زیبایی بدن شرکت‌کنندگان در آینده موثر بود. در نتیجه می‌توان گفت فرضیه شکل‌گیری گرایش به انجام جراحی‌های زیبایی بدن در اثر مشاهده تصاویر خویش‌انداز تایید می‌شود. در تبیین این نتیجه می‌توان

اشاره داشت، عدم اجبار پاسخگویان به باقی ماندن روی تصاویر در حال نمایش به میزان زمان یکسان و مورد نظر در این مطالعه، می‌تواند باعث شود که افراد دست‌کاری را ضعیف‌تر از آنچه انتظار می‌رفت دریافت کرده باشند. نتایج این مطالعه همچنین نشان داد که مشاهده تصاویر خویش‌انداز تأثیرگذاران زیبایی نسبت به تصاویر خویش‌انداز بازیگران گرایش به انجام جراحی زیبایی بدن بالاتری را شکل می‌دهد. این یافته هم جهت با انتظار پژوهشی اولیه بود. به این ترتیب، با توجه به احساس نزدیکی و شباهتی که کاربران اینستاگرام ممکن است نسبت به تأثیرگذاران اینستاگرام داشته باشند (چای، ۲۰۱۸)، می‌توان این احتمال را در نظر گرفت که فرآیند مقایسه اجتماعی و ظاهری با این افراد بیشتر از بازیگران مشهور سینما صورت گرفته است.

در رابطه با فرضیه دوم نتایج این مطالعه نشان دادند که نارضایتی چهره‌ای پیش‌بینی‌کننده‌ی گرایش بالاتر نسبت به انجام جراحی‌های زیبایی (مخصوصاً صورت) در افراد است. از مقایسه گروه‌های تأثیرگذاران زیبایی با بازیگران و تأثیرگذاران زیبایی با غیرانسان می‌توان دریافت، مشاهده تصاویر خویش‌انداز بر میزان نارضایتی چهره‌ای در افراد موثر نمی‌باشد. در نتیجه، مکانیسم اثر نوع تصاویر اینستاگرامی مورد مشاهده بر گرایش به انجام جراحی زیبایی صورت توسط نارضایتی چهره‌ای میانجی‌گری نمی‌شود. در نتیجه فرضیه میانجی‌گری نارضایتی چهره‌ای رد می‌شود. نتایج این مطالعه همچنین نشان دادند که شرایط تأثیرگذاران زیبایی منجر به گرایش به انجام جراحی زیبایی صورت و گرایش به انجام جراحی زیبایی بدن بالاتری نسبت به شرایط بازیگران شد و این اثر توسط افزایش نارضایتی چهره‌ای تبیین نشد و دارای مکانیسم اثر متفاوتی است.

به‌طور کلی نتایج نشان دادند که ارائه تصاویر خویش‌انداز اینستاگرامی کمتر از حد انتظار بر نارضایتی چهره‌ای و گرایش به انجام جراحی زیبایی صورت و بدن تأثیرگذار بود. در تبیین این موضوع می‌توان به این نکته اشاره داشت که امکان فعال شدن نوعی واکنش روان‌شناختی دفاعی در مقابل مشاهده تصاویر تأثیرگذاران اینستاگرامی و بازیگران مشهور در میان شرکت‌کنندگان وجود دارد. در نهایت باید اشاره داشت که محدودیت پوشش زنان بازیگران ایرانی باعث آن شد که شرایط بازیگران از لحاظ پوشش و میزان نمایش زیبایی در مقایسه با تأثیرگذاران زیبایی در وضعیت یکسانی قرار نگرفته باشد و دست‌کاری یکسانی اتفاق نیافته باشد.

با توجه به نتایج حاصل شده به پژوهشگران بعدی توصیه می‌شود مکانیسم‌های میانجی‌گری دیگری را مانند متغیر مقایسه ظاهری موقعیتی در همین مدل نظری امتحان کنند. به‌طورکلی نتایج این مطالعه نشان دادند که ارائه تصاویر خویش‌انداز اینستاگرامی کمتر از حد انتظار بر نارضایتی چهره‌ای و گرایش به انجام جراحی زیبایی تأثیرگذار بوده است. در مورد تفاوت‌های میانجی‌گری نشده بین مشاهده تصاویر تأثیرگذاران زیبایی با دو گروه دیگر در گرایش به جراحی زیبایی، قابل انتظار است که مکانیسم(ها)ی غیر از نارضایتی ظاهری این اثر را میانجی‌گری نماید. یافته حاضر به آگاهی متخصصان حیطه سلامت از عوامل اثرگذار بر قصد افراد برای جراحی‌های زیبایی می‌افزاید.

## سیاس‌گزاری

از تمامی شرکت‌کنندگان این پژوهش اعم از دانشجویان دانشگاه شهید بهشتی و دانشگاه‌های دیگر که در پژوهش ما شرکت کردند نهایت تشکر و قدردانی را داریم.

## مراجع

- [1] Calogero, R. M., Pina, A., Park, L. E., & Rahemtulla, Z. (2010). Objectification theory predicts college women's attitudes toward cosmetic surgery. *Sex Roles*, 63(1-2), 32-41. <https://doi.org/10.1007/s11199-010-9759-5>
- [2] Chae, J. (2018). Explaining females' envy toward social media influencers. *Media Psychology*, 21(2), 246-262.
- [3] Deane, G. (2017). Is it Instagram-Worthy?. An Exploration of the Impact of Instagram on Body Image Perception Among Irish Women aged, 18-24.
- [4] Fardouly, J., Pinkus, R. T., & Vartanian, L. R. (2017). The impact of appearance comparisons made through social media, traditional media, and in-person in women's everyday lives. *Body image*, 20, .31-39
- [5] Fardouly, J., & Vartanian, L. R. (2015). Negative comparisons about one's appearance mediate the relationship between Facebook usage and body image concerns. *Body image*, 12, 82-88. <https://doi.org/10.1016/j.bodyim.2014.10.004>
- [6] Fardouly, J., Willburger, B. K., & Vartanian, L. R. (2018). Instagram use and young women's body image concerns and self-objectification: Testing mediational pathways. *New Media & Society*, 20(4), 1380-1395.
- [7] Festinger, L. (1954). A theory of social comparison processes. *Human Relations*, 7(2), 117-140.
- [8] Gawronski, B., & Bodenhausen, G. V. (2006). Associative and propositional processes in evaluation: an integrative review of implicit and explicit attitude change. *Psychological Bulletin*, 132(5), 692.
- [9] Hayes, A. F. (2018). Introduction to mediation, moderation, and conditional process analysis (2nd Ed.), New York: The Guilford Press.
- [10] Heinberg, L. J., & Thompson, J. K. (1995). Body image and televised images of thinness and attractiveness: A controlled laboratory investigation. *Journal of social and clinical psychology*, 14(4), 325-338. <https://doi.org/10.1521/jscp.1995.14.4.325>
- [11] Hendrickse, J., Arpan, L. M., Clayton, R. B., & Ridgway, J. L. (2017). Instagram and college women's body image: Investigating the roles of appearance-related comparisons and intrasexual competition. *Computers in Human Behavior*, 74, 92-100. <https://doi.org/10.1016/j.chb.2017.04.027>
- [12] Holland, G., & Tiggemann, M. (2016). A systematic review of the impact of the use of social networking sites on body image and disordered eating outcomes. *Body image*, 17, 100-110. <https://doi.org/10.1016/j.bodyim.2016.02.008>

- [13] Iranian surgery. (2019, May 16.) Rhinoplasty in Iran. [Web log message]. Retrieved from <https://iraniansurgery.com/en/rhinoplasty-in-iran>
- [14] ISAPS Global Statistics. International Society of Aesthetic Plastic Surgery. ISAPS International Survey on Aesthetic /Cosmetic Procedures Performed in 2020. <https://www.isaps.org/medical-professionals/isaps-global-statistics>
- [15] Kleemans, M., Daalmans, S., Carbaat, I., & Anschütz, D. (2018). Picture perfect: The direct effect of manipulated Instagram photos on body image in adolescent girls. *Media Psychology*, 21(1), 93-110.
- [16] Ng, C. H. (2019). Impact of Instagram Influencers on Cosmetic Surgery (Doctoral dissertation, Tunku Abdul Rahman University College)
- [17] O'Brien, K. S., Caputi, P., Minto, R., Peoples, G., Hooper, C., Kell, S., & Sawley, E. (2009). Upward and downward physical appearance comparisons: Development of scales and examination of predictive qualities. *Body Image*, 6(3), 201-206.
- [18] Rastmanesh R., Gluck ME., & Shadman Z. (2009). Comparison of body dissatisfaction and cosmetic rhinoplasty with levels of veil practicing in Islamic women *Int J Eat Disord*, 42 (4): 339-45.
- [19] Sensis. The must-know stats from the 2018 yellow social media report [Internet]. Melbourne: Sensis; 2018 [cited 2019 Sep 10]. Available from: <https://www.sensis.com.au/about/our-reports/sensis-social-media-report>
- [20] Sun, Q. (2021). Selfie editing and consideration of cosmetic surgery among young Chinese women: The role of self-objectification and facial dissatisfaction. *Sex Roles*, 84(11), 670-679 <https://doi.org/10.1007/s11199-020-01191-5>
- [21] Smith, A., & Anderson, M. (2018). Social media use in 2018. Pew Research Center.
- [22] Tiggemann, M., & McGill, B. (2004). The role of social comparison in the effect of magazine advertisements on women's mood and body dissatisfaction. *Journal of Social and Clinical Psychology*, 23(1), .23-44
- [23] Tiggemann, M., Brown, Z., Zaccardo, M., & Thomas, N. (2017). "Warning: This image has been digitally altered": The effect of disclaimer labels added to fashion magazine shoots on women's body dissatisfaction. *Body Image*, 21, .107-113
- [24] Tiggemann, M., Hayden, S., Brown, Z., & Veldhuis, J. (2018). The effect of Instagram "likes" on women's social comparison and body dissatisfaction. *Body image*, 26, .90-97 <https://doi.org/10.1016/j.bodyim.2018.07.002>
- [25] Tiggemann, M., & Zaccardo, M. (2015). "Exercise to be fit, not skinny": The effect of fitspiration imagery on women's body image. *Body image*, 15, .61-67 <https://doi.org/10.1016/j.bodyim.2015.06.003>
- [26] Tiggemann, M., & Zinoviev, K. (2019). The effect of # enhancement-free Instagram images and hashtags on women's body image. *Body image*, 31, .131-138 <https://doi.org/10.1016/j.bodyim.2019.09.004>



- [27] Wang, Y., Fardouly, J., Vartanian, L. R., & Lei, L. (2019). Selfie-viewing and facial dissatisfaction among Chinese adolescents: A moderated mediation model of general attractiveness internalization and body appreciation. *Body Image*, 30, .35-43 <https://doi.org/10.1016/j.bodyim.2019.05.001>



## مدل مفهومی فضای سایبر از دیدگاه کاربرد علوم داده در امنیت سایبری

سید نصیب اله دوستی مطلق<sup>۱</sup>، علی اصغر نوروزی<sup>۲</sup>

<sup>۱</sup>عضو هیات علمی دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی  
doustimotlagh@chmail.ir

<sup>۲</sup>محقق دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی  
alianorouzi@chmail.ir

### چکیده

دوام، رشد و توسعه هر کشوری در گروی امنیت ملی آن است. از مهم‌ترین جنبه‌های امنیت ملی در دنیای امروزی، امنیت سایبری است. در سال‌های اخیر حجم، تنوع، نرخ تولید و پیچیدگی تهدیدها و حملات سایبری افزایش چشم‌گیری داشته است. علوم داده و یادگیری ماشین حوزه‌های پژوهشی در حال رشدی هستند که راهکارهای مناسبی را برای مواجهه با این چالش‌ها ارائه می‌دهند. در حقیقت، روش‌های یادگیری ماشین و علوم داده عنصر کلیدی برای خودکار و هوشمند کردن سامانه‌های امنیتی شده‌اند. برای استفاده دقیق و همه‌جانبه از علوم داده در ارتقای امنیت سایبری نیاز به مدل مفهومی فضای سایبر است. در پژوهش حاضر جهت ارائه مدل مفهومی از رویکرد کیفی استفاده شده است. برای این منظور در مصاحبه با نخبگان امنیت فضای سایبر و علوم داده سه مفهوم (۱) کاربر، محتوا و خدمات، (۲) حکمرانی و (۳) زیرساخت به مثابه ابعاد اساسی مدل فضای سایبر از دیدگاه کاربرد علوم داده در امنیت سایبری مورد شناسایی قرار گرفتند و سپس مؤلفه‌های هر یک از این ابعاد استخراج شدند.

**کلمات کلیدی:** فضای سایبر، امنیت فضای سایبر، علوم داده، یادگیری ماشین، ارزیابی امنیت سایبری.

## ۱ مقدمه

فضای سایبر در عصر کنونی، بخش مهمی از زندگی افراد، اقتصاد کشورها، سیاست و حتی مسائل امنیتی و نظامی شده است و قابل چشم‌پوشی نیست. از مهم‌ترین مسائل مطرح در فضای سایبر امنیت آن است. با افزایش و تکامل حملات در فضای سایبر، نیاز به وجود سامانه‌های خودکار برای تکمیل تجزیه و تحلیل انسانی بیش از پیش احساس می‌شود. علاوه بر این، یافتن آسیب‌پذیری‌ها و رخنه‌ها به مساله‌ای بسیار دشوار تبدیل شده است. اندازه فضای سایبر و حجم داده‌ها و اطلاعات موجود در آن چنان در حال رشد است که به نظر

غیر ممکن است که بدان از کجا باید شروع کرد. حفاظت از داده‌ها و سامانه‌های رایانه‌ای در مقابل حملات سایبری یکی از حیاتی‌ترین وظایف امنیت سایبری است. لازمه این امر استفاده از روش‌های حفاظت دقیق و خودکار (یا نیمه‌خودکار) است. حفاظت دقیق و خودکار با علوم داده امکان‌پذیر می‌شود. علوم داده ترکیبی از ابزار، روش‌ها و الگوریتم‌ها برای پردازش و تحلیل داده‌ها و استخراج دانش از آن‌ها است. علوم داده از اشتراک علوم و فنونی همچون آمار، هوش مصنوعی و به خصوص روش‌های یادگیری ماشین، داده‌کاوی، روش‌های بصری‌سازی، پایگاه داده‌ها و روش‌های پردازش داده ایجاد شده است [۵]. به دلیل اهمیت علوم داده و کاربردهای زیاد آن، در سال‌های اخیر راه‌کارهای متعددی برای استفاده از علوم داده به منظور تشخیص رخدادها و حملات سایبری (چه از قبل شناخته‌شده و چه ناشناخته) و محافظت از سامانه‌های حساس پیشنهاد و عملیاتی شده است [۶][۷]. با استفاده از علوم داده در امنیت سایبری، الگوها و رفتارهای پیچیده حمله‌کنندگان شناسایی می‌شود، قابلیت‌های شناسایی و جلوگیری از حملات سایبری بهبود پیدا می‌کند، اطلاعات در مورد تهدیدات سایبری افزایش می‌یابد و اشتراک گذاری فوری اطلاعات در مورد تهدیدات تسهیل می‌گردد. برای استفاده دقیق و همه‌جانبه از علوم داده در ارتقای امنیت سایبری نیاز به مدل مفهومی فضای سایبر است.

هدف این پژوهش ارائه مدل مفهومی برای فضای سایبر از دیدگاه کاربرد علوم داده در ارتقای امنیت سایبری است. این مدل شامل سه بعد اساسی (۱) کاربر، محتوا و خدمات، (۲) حکمرانی و (۳) زیرساخت است. بعد اول شامل مؤلفه‌های تحلیل داده‌ها، تحلیل، پیش‌بینی و واکنش به تهدیدها و حملات و شبکه‌های اجتماعی است. بعد حکمرانی شامل مؤلفه‌های قوانین، ارزیابی، حکمرانی داده، تصمیم‌گیری مبتنی بر داده، بودجه، بومی‌سازی و استفاده از شرکت‌های خصوصی، ظرفیت‌سازی، آموزش، تحقیق و توسعه و مرکز فرماندهی واحد است. بعد زیرساخت نیز حاوی مؤلفه‌های مرکز عملیات امنیت سایبری، شبکه‌های ارتباطی مناسب برای تحلیل و تشخیص تهدیدها و حملات، سخت‌افزار مناسب برای تحلیل و تشخیص تهدیدها و حملات، فناوری ابر برای ذخیره و تحلیل داده‌ها و زیرساخت مناسب کلان داده‌ها (موازی، توزیع‌شده) است. از این مدل و ابعاد و مؤلفه‌های آن می‌توان برای تبیین نقش علوم داده در ارتقای امنیت سایبری و همچنین ارزیابی وضعیت کشور یا یک سازمان در حوزه امنیت سایبری و علوم داده بهره برد.

## ۲ مروری بر کارهای دیگران

فضای سایبر شامل اینترنت، شبکه‌ها، سامانه‌ها، لوازم جانبی، داده‌ها و کاربران در محیط اطلاعات است. این محیط بهم پیوسته برای حاکمیت جهانی، تجاری، نظامی و امنیت ملی حائز اهمیت است (Caton, 2019). به دلیل پیچیدگی بالای فضای سایبر از مدل‌های گوناگونی برای توصیف و تحلیل آن استفاده می‌شود. در ادامه برخی از این مدل‌ها مرور می‌شوند.

## ۱.۲ مدل سه لایه وزارت دفاع آمریکا

از منظر وزارت دفاع آمریکا، فضای سایبر در سه بعد مجزا ولی کاملاً درهم تنیده و پیوسته تشریح می‌گردد که همواره با افراد، سازمان‌ها و سامانه‌ها در تعامل است. این ابعاد عبارتند از: فیزیکی (مانند گوشی‌های همراه)، اطلاعاتی (مانند توزیع اطلاعات) و شناختی یا فکری (مانند ادراک و برداشت) [۷]. شکل ۱ ابعاد به هم پیوسته فضای سایبر و نحوه ارتباط آن‌ها را نشان می‌دهد. بعد فیزیکی از سامانه‌های فرماندهی و کنترل، تصمیم‌گیرنده‌های کلیدی و زیرساخت‌های حمایتی تشکیل شده است. این بعد شامل شبکه‌های ارتباطی، انسان، امکانات C2، روزنامه‌ها، کتاب‌ها، برج‌های میکروویو، لپ‌تاپ‌ها، تلفن‌های هوشمند یا هر چیز دیگر قابل اندازه‌گیری شهودی است. بعد فیزیکی مرتبط با محدوده‌های نظامی، ملی، اقتصادی و جغرافیایی است. بعد اطلاعاتی کجایی و چگونگی جمع‌آوری، پردازش، ذخیره، انتشار و حافظت از اطلاعات را شامل می‌شود. بعد شناختی شامل ذهن کسانی است که عمل‌های انتقال، دریافت، پاسخ یا کنش را روی اطلاعات انجام می‌دهند. این بعد به پردازش اطلاعات، ادراک، قضاوت و تصمیم‌گیری افراد یا گروه‌ها اشاره دارد. عناصر این بعد تحت تاثیر عواملی مانند اعتقادات فردی و فرهنگی، هنجارها، آسیب‌پذیری‌ها، انگیزه‌ها، احساسات، تجربیات، اخلاق، آموزش، سلامت روان، هویت‌ها و ایدئولوژی‌هاست.



شکل ۱: ابعاد به هم پیوسته فضای سایبر [۷]

## ۲.۲ مدل زیمت و اسکودیس

مدل زیمت و اسکودیس [۸] دارای چهار دامنه زیرساخت/سیستم‌ها، محتوا/کاربرد، مردم/اجتماع و حکمرانی است. در شکل ۲ این چهار دامنه نشان داده شده است. دامنه زیرساخت/سامانه‌ها شامل اجزای فیزیکی و زیرساخت فنی است. دامنه محتوا/کاربرد شامل پایگاه‌های اطلاعاتی و سازوکارهای دسترسی و پردازش

دامنه حکمرانی		
دامنه مردم/اجتماع	دامنه محتوا/کاربرد	دامنه زیرساخت/سامانه‌ها

شکل ۲: مدل زیمت و اسکودیس [۸]

اطلاعات است. دامنه مردم/اجتماع شامل ارتباطات و تعاملات بین انسان‌ها و اطلاعات است. در نهایت، دامنه حکمرانی شامل سازوکارهای مدیریتی و نظارتی برای حکمرانی بر سه دامنه دیگر است.

### ۳.۲ مدل شورای عالی فضای مجازی

فضای مجازی کشور، پوششی بسیار وسیع در حوزه‌های مختلف فضای مجازی (بستر، خدمات، محتوا، کاربر، مقررات و امنیت) دارد که محدوده آن، با شرط قرار گرفتن خدمت‌دهنده یا کاربر در قلمرو حاکمیتی نظام جمهوری اسلامی ایران، قابل تعریف است. بر این اساس در اسناد شورای عالی فضای مجازی کشور مدل شش لایه‌ای برای فضای سایبر تبیین شده است که در شکل ۳ قابل مشاهده است [۱].



شکل ۳: مدل شش لایه شورای عالی فضای مجازی [۱]

### ۴.۲ مدل‌های دیگر

تقی‌پور و اسماعیلی [۲] یک مدل مفهومی به عنوان الگو و زیرساخت شناختی برای دفاع سایبری جمهوری اسلامی ایران پیشنهاد داده‌اند. این مدل شامل سه بعد بازدارندگی، پدافند (دفع) و برگشت‌پذیری (تاب‌آوری) است. بازدارندگی مانع ذهنی محکمی را برای دشمنان ایجاد می‌کند تا با افزایش هزینه‌های حملات سایبری، در مرحله طرح‌ریزی و قبل از آن، عملیات حمله را با تزلزل مواجه سازد. پدافند به معنای دفاع در مقابل حملات است و به دو نوع عامل و غیر عامل دسته‌بندی می‌شود. برگشت‌پذیری نیز عبارت است از توانایی یک سازمان برای مقاومت، واکنش و بازیابی در حملات سایبری.

رمضان‌زاده و همکاران [۳] یک مدل مفهومی برای ارزیابی قدرت سایبری نیروهای مسلح با تأکید بر بعد بازدارندگی سایبری ارائه کرده‌اند. این مدل دارای مؤلفه‌های پنج‌گانه استحکام‌سازی، پاسخ به تهاجم سایبری، پیشیمان‌کنندگی دشمن (اقدام متقابل)، بازیابی و استمرار عملیات (افزودگی) است. همه این مؤلفه‌ها مربوط به بعد بازدارندگی سایبری هستند و می‌توانند در شناسایی و اولویت‌بندی سرمایه‌های سایبری نیروهای مسلح به منظور ایجاد زمینه بازدارندگی سایبری در مقابل تهدیدات، مفید باشند.



رحیم‌اف و موحدی [۴] یک الگوی راهبردی برای ارزیابی عملیات سایبری پیشنهاد داده‌اند. آن‌ها استدلال می‌کنند که توان انجام موفق عملیات سایبری، باعث افزایش قدرت سایبری، ایجاد بازدارندگی سایبری و کاهش تهدیدات سایبری می‌شود. بنابراین ارزیابی فعالیت‌های سایبری جهت شناسایی ضعف‌ها و قوت‌ها و بررسی میزان اثربخشی فعالیت‌ها اجتناب‌ناپذیر است. به این منظور، رحیم‌اف و موحدی یک الگوی راهبردی شامل سه بعد ارزیابی طراحی و طرح‌ریزی، ارزیابی آمادگی رزمی و ارزیابی اجرا پیشنهاد می‌دهند. این بعدها به ده مؤلفه و هفتادوسه شاخص تقسیم‌بندی شده‌اند.

### ۳ مدل پیشنهادی

پس از مصاحبه با نخبگان، ابعاد مدل مفهومی ارزیابی موارد زیر انتخاب شدند:

- کاربر، محتوا و خدمات
- حکمرانی
- زیرساخت

مدل مرجع برای انتخاب این ابعاد مدل شش لایه مرکز ملی فضای مجازی بود. به دلیل این که در اینجا دیدگاه امنیت سایبری داریم، لایه امنیت حذف شد. در حقیقت امنیت در تمام ابعاد به صورت ضمنی وجود دارد. قابل ذکر است که تمام موارد امنیتی در این مدل مفهومی، مربوط به امنیت غیر عامل هستند. لایه‌های کاربر، محتوا و خدمات در یک بعد ادغام شدند، زیرا که دیدگاه پژوهش علوم داده است و جدا کردن این سه لایه منجر به پیچیدگی غیر ضروری مؤلفه‌ها می‌شود. هر بعد دارای سه تا هشت مؤلفه است. برخی از مؤلفه‌ها نیز به زیرمؤلفه‌ها شکسته شده‌اند تا پیچیدگی کاهش یابد. شکل ۴ و جدول ۱ ابعاد، مؤلفه‌ها و زیرمؤلفه‌های مدل مفهومی ارزیابی استخراجی از مصاحبه نخبگی را نشان می‌دهد.

بعد کاربر، محتوا و خدمات شامل شبکه‌های اجتماعی و کلیه افراد مرتبط با فضای مجازی، داده‌ها، اطلاعات داخلی و راداری، متن ایمیل‌ها، تعاملات و اطلاعات ردوبدل شده در شبکه‌های ارتباطی و اجتماعی، ذخیره و پردازش اطلاعات، تحلیل، پیش‌بینی و واکنش به تهدیدها و حملات، به‌روزرسانی سامانه‌ها، خدمات اتوماسیون، برنامه‌های کاربردی، خدمات مبتنی بر وب، پست الکترونیکی، سامانه فایل‌ها و غیره است. بعد حکمرانی شامل اقدامات قانونی، سازمان‌دهی، ظرفیت‌سازی، تنظیم قوانین و مقررات، ارزیابی، بودجه و بومی‌سازی است.

بعد زیرساخت شامل هر سازوکار مرتبط با زیرساخت و معماری، سخت‌افزار و پروتکل‌ها، رایانه‌های راداری، حسگرها، سامانه‌های کنترلی، ابر و غیره است.

در ادامه برخی از اصطلاحات موجود در مؤلفه‌ها و زیرمؤلفه‌ها توضیح داده می‌شود.

- آسیب‌پذیری در مقوله امنیت سایبری نقطه ضعفی است که می‌تواند توسط مجرمان سایبری برای دسترسی غیر مجاز به یک سامانه رایانه‌ای مورد سو استفاده قرار گیرد.



شکل ۴: مدل مفهومی فضای سایبر از دیدگاه کاربرد علوم داده در امنیت سایبری

جدول ۱: ابعاد، مؤلفه‌ها و زیرمؤلفه‌های مدل مفهومی

ابعاد	مؤلفه‌ها	زیرمؤلفه‌ها
کاربر، محتوا و خدمات	تحلیل داده‌ها	جمع‌آوری داده‌ها
		پردازش، گزینش و تحلیل داده‌ها
		ذخیره داده‌ها
	تحلیل، پیش‌بینی و واکنش به تهدیدها و حملات	پایش و تشخیص ریسک‌ها و تهدیدها
		کشف، مدیریت و کنترل آسیب‌پذیری‌ها و بدافزار
		واکنش به تهدیدها و حملات و طرح تداوم
		اطلاعات راهبردی تهدید رایانه‌ای
		مدیریت اطلاعات و رخدادهای امنیتی
شبکه‌های اجتماعی		
حکمرانی	قوانین	تنظیم قوانین مرتبط با داده‌های حساس
		نظارت بر حسن اجرای قوانین و سیاست‌ها
		نحوه اشتراک اطلاعات بین سازمان‌ها
		راهبرد ملی برای امنیت فضای سایبر
		اجرای مانورهای حملات سایبری
	ارزیابی	ارزیابی سامانه‌های موجود
		حکمرانی داده
		تصمیم‌گیری مبتنی بر داده
		بودجه
		بومی‌سازی و استفاده از شرکت‌های خصوصی
ظرفیت‌سازی، آموزش، تحقیق و توسعه	مرکز فرماندهی واحد	
	زیرساخت	مرکز عملیات امنیت سایبری
		شبکه‌های ارتباطی مناسب برای تحلیل و تشخیص تهدیدها و حملات
		سخت‌افزار مناسب برای تحلیل و تشخیص تهدیدها و حملات
		فناوری ابر برای ذخیره و تحلیل داده‌ها
زیرساخت مناسب کلان داده‌ها (موازی، توزیع‌شده)		

- تهدید در فضای سایبر یک اقدام یا رویداد منفی بالقوه است که توسط یک آسیب‌پذیری تسهیل شده است. به طور کلی تهدید سایبری یک اقدام مخرب است که به دنبال آسیب رساندن به داده‌ها و یا سرقت داده‌ها و یا تاثیر ناخواسته بر یک سامانه یا برنامه رایانه‌ای است.
- حمله سایبری هر گونه تهاجمی است که سامانه‌های اطلاعاتی رایانه‌ای، شبکه‌های رایانه‌ای یا زیرساخت‌ها را هدف قرار می‌دهد. در این اقدام، مهاجم شخص یا فرایندی است که تلاش می‌کند بدون مجوز به داده‌ها، عملکردها یا سایر مناطق محدود شده سامانه دسترسی پیدا کند. این دسترسی به احتمال زیاد با قصد تخریب است.
- طرح تداوم توانایی یک سازمان و کسب‌وکار برای ادامه ارائه خدمات در سطوح قابل قبول از پیش تعریف شده، پس از یک حادثه غیر مترقبه، مانند حمله سایبری است.
- مرکز عملیات امنیت سایبری یک تیم امنیت اطلاعات را در خود جای داده است که مسئول نظارت و تجزیه و تحلیل وضعیت امنیتی سازمان به صورت مداوم است. هدف تیم مرکز عملیات امنیت سایبری شناسایی، تجزیه و تحلیل و پاسخ به حوادث امنیت سایبری با استفاده از ترکیبی از راه‌حل‌های فناوری و مجموعه‌ای قوی از فرایندها است. مراکز عملیات امنیتی معمولاً متشکل از تحلیلگران و مهندسان امنیتی و همچنین مدیرانی است که بر عملیات امنیتی نظارت می‌کنند.
- اطلاعات راهبردی تهدید سایبری دانش، مهارت و اطلاعات مبتنی بر تجربه در مورد وقوع و ارزیابی تهدیدات سایبری یا فیزیکی و عوامل تهدید هستند که می‌توانند در کمک به کاهش حملات احتمالی و رویدادهای مضر فضای سایبر مفید باشند [۹].
- حکمرانی داده مجموعه‌ای از فرایندها، نقش‌ها، استانداردها و معیارهایی است که استفاده موثر و کارآمد از اطلاعات را در توانمند ساختن سازمان یا دولت برای دستیابی به اهداف خود تضمین می‌کند. حکمرانی داده تضمین می‌کند که نقش‌های مرتبط با داده‌ها در سازمان یا دولت به وضوح تعریف شده‌اند [۱۰].
- تصمیم‌گیری مبتنی بر داده اصطلاحی است که برای فرایند و تکنیک تصمیم‌گیری براساس تجزیه و تحلیل داده‌ها و ارزیابی اطلاعات به کار می‌رود. در این نوع تصمیم‌گیری از شهود استفاده‌ای نمی‌شود و تنها داده‌ها و اطلاعات استخراج شده از آن‌ها ملاک تصمیمات هستند [۱۱].
- کلان داده‌ها به مجموعه داده‌هایی گفته می‌شود که در حجم و تنوع زیاد و با شتاب بالایی تولید می‌شوند [۱۲].

## ۴ نتیجه‌گیری و پیشنهاد

در این پژوهش یک مدل مفهومی برای فضای سایبر از دیدگاه کاربرد علوم داده در ارتقای امنیت سایبری پیشنهاد شد. این مدل دارای سه بعد (۱) کاربر، محتوا و خدمات، (۲) حکمرانی و (۳) زیرساخت است. هر بعد نیز به سه تا هشت مؤلفه تقسیم می‌شود. برخی از مؤلفه‌ها نیز به زیرمؤلفه‌ها شکسته می‌شوند. در ادامه این پژوهش می‌توان براساس این مدل پرسشنامه‌ای طراحی کرد و در اختیار کارشناسان امنیت سایبری و علوم داده قرار داد. با تحلیل آماری نتایج این پرسشنامه، مثلاً روش آماری حداقل مربعات جزئی، می‌توان روابط بین مدل، ابعاد و مؤلفه‌ها را مورد بررسی قرار داد تا مدل از لحاظ کمی نیز مورد تایید قرار گیرد. به علاوه، از این مدل می‌توان برای ارزیابی وضعیت امنیت سایبری و علوم داده در فضای سایبری کشور بهره برد.

## مراجع

- [۱] فیروزآبادی، سیدابوالحسن. درآمدی بر حکمرانی فضای مجازی. انتشارات دانشگاه امام صادق (علیه السلام)، ۱۳۹۹.
- [۲] تقی‌پور، رضا و اسماعیلی، علی. طراحی مدل مفهومی الگوی دفاع سایبری جمهوری اسلامی ایران. فصلنامه امنیت ملی، ۱۳۹۷.
- [۳] رمضان‌زاده، مجتبی، غیوری‌ثالث، مجید، احمدوند، علی‌محمد، آقایی، محسن، و فرخی، ابراهیم نظری. ارائه مدل مفهومی ارزیابی قدرت سایبری نیروهای مسلح با تاکید بر بعد بازدارندگی سایبری. فصل‌نامه مدیریت نظامی، ۱۳۹۹.
- [۴] رحیم‌اف، هانی و موحدی‌صفت، محمدرضا. الگوی راهبردی ارزیابی عملیات سایبری. فصل‌نامه مدیریت نظامی، ۱۳۹۹.
- [5] Martinez, I., Viles, E., and Olaizola, IG. Data science methodologies: current challenges and future approaches. *Big Data Research*, 2021.
- [6] Dasgupta, D., Akhtar, Z., and Sen, S. Machine learning in cybersecurity: a comprehensive survey. *The Journal of Defense Modeling and Simulation*, 2022.
- [7] Selvarathi, C. A survey on machine learning approach to detect malware. *Turkish Journal of Computer and Mathematics Education*, 2021.
- [8] Zimet, E. and Skoudis, E. A graphical introduction to the structural elements of cyberspace. *Cyberpower and national security*, 2009.
- [9] Wagner, T. D., Mahbub, K., Palomar, E, and Abdallah, A. E. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*, 2019.
- [10] Abraham, R., Schneider, J., and Vom Brocke, J. Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 2019.
- [11] Garouani, M., Ahmad, A., Bouneffa, M., Hamlich, M., Bourguin, G., and Lewandowski, A. Towards big industrial data mining through explainable automated machine learning. *The International Journal of Advanced Manufacturing Technology*, 2022.

- [12] Provost, F. and Fawcett, T. Data science and its relationship to big data and data-driven decision making. *Big data*, 2013.



## الگوی تدوین نقشه‌ی راهبرد حکمرانی بر فضای سایبر جمهوری اسلامی ایران

ساسان چمنی<sup>۱</sup>، محسن آقایی<sup>۲</sup>

<sup>۱</sup> دانشجوی دکتری مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی  
chamani.sasan@ut.ac.ir

<sup>۲</sup> عضو هیئت علمی دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

### چکیده

عالم سایبر در حال دمیدن روح سایبر به هر پدیده‌ی طبیعی است. با توجه به سازماندهی دولت‌های متخصص در به آشوب کشاندن جامعه اسلامی ایران با بهره‌گیری از این فضا، نیازمند نقشه راهبرد جامعی برای حکمرانی بر فضای سایبری جمهوری اسلامی ایران می‌باشیم. تدوین نقشه راهبرد حکمرانی بر فضای سایبر، راهبردهای حاکم بر فضای سایبری را اثربخش و عملیاتی می‌نماید. از طرفی روند تدوین نقشه راهبرد در سازمان‌ها به عنوان یک چالش اساسی مطرح بوده و یک روند جامع برای این موضوع که پوشش‌دهنده‌ی تمام ابعاد باشد وجود ندارد. برای این منظور در این مقاله ضمن تبیین واژه حکمرانی و تعامل آن با فضای سایبر، با مطالعه و بررسی میدانی مبتنی بر روش تحقیق توصیفی تحلیلی، انواع روش‌های تدوین نقشه‌ی راهبرد در منابع مختلف و با تحلیل و در نظر گرفتن مسائل و چالش‌های حکمرانی بر فضای سایبر کشور از قبیل زیر ساخت، جامعه و جنگ شناختی، تهاجمات و نقش ذی‌نفعان در این عرصه؛ الگوی تدوین نقشه‌ی راهبرد حکمرانی بر فضای سایبری جمهوری اسلامی ایران تدوین و ارائه می‌گردد.

**کلمات کلیدی:** اهداف راهبردی، فضای سایبر، نقشه‌ی راهبرد، حکمرانی بر فضای سایبر.

### ۱ مقدمه

لزوم برخورداری از یک نقشه جامع، تصویرسازی آینده مطلوب، تعیین مطلوبیت‌های راهبردی از جمله رسالت، مأموریت، چشم‌انداز، تبیین و پیگیری اهداف بلندمدت، قانع نشدن به وضع موجود؛ نمونه‌هایی از توصیه‌های راهبردی است که رهبر معظم انقلاب اسلامی امام خامنه‌ای (مدظله) در دیدار با مسئولین، نخبگان و حتی در دیدارهای عمومی و خطبه‌های نماز جمعه بر آن‌ها تأکید مکرر داشته‌اند.

فضای مجازی در زمان حاضر در تمامی ابعاد زندگی فردی و اجتماعی مردم جهان نفوذ کرده و در حال ایجاد یک تمدن جدید بشری است که از تمدن‌های قبل به مراتب فراگیرتر است. بدون شک حکمرانی چنین

فضایی که از یک طرف با تسهیل ارتباط و ارائه فناوریها و خدمات جدید و شگفتآور ضریب نفوذ بسیار بالایی داشته و بسیار سریعتر از فرهنگ غرب در حال هضم کردن کاربران یعنی مردم خود است و از طرف دیگر با قابلیت‌های خود در حال تبدیل کردن حاکمیت ملی حکومتی به یک حاکمیت شبکه‌های شرکتی فرامرزی است. این مسئله بیش از سایر کشورها برای جمهوری اسلامی ایران یک تهدید محسوب میشود؛ چرا که این کشور همواره در معرض تهدیدات دشمنان خود به خصوص جریان صهیونیسم قرار دارد و اکثر شرکتهای بزرگ و صاحب نفوذ در فضای مجازی تحت سلطه این جریان هستند (غلامی، ۱۳۹۸).

جهت‌گیری ذهن‌ها در پشت فضای غبارآلود جذاب سایبری، داستان شهر آژ<sup>۱</sup> را تداعی می‌کند که همه‌چیز در آن زمردین و فریبنده به نظر می‌رسد، اما در حقیقت شهری معمولی بود که همه آن را از پشت عینک‌های سبزرنگ مشاهده می‌کردند و در توهم برتر بودن، خاص بودن و بی‌عیب بودن زیست می‌کردند. فضای سایبر با این‌چنین جلوه‌ایی خودنمایی می‌کند. آفت جدی فضای سایبر که نفوذش عالم‌گیر است، توهم بی‌عیبی و برتر بودن را انتشار داده است. فضای سایبر با همه خصیصه‌های خویش و تحول در ارتقاء سطح زندگی انسانی از آنجایی که در ورای خود انگیزه‌هایی خاص را دنبال می‌کند، به‌مثابه ظرف آلوده‌ای شده است که موجب فساد و تباهی و بیماری می‌شود. لزوم تنظیم شیوه حکمرانی متناسب با اقتضات سرزمینی بدیهی و عقلانی است (همان‌گونه که اروپا نیز ایده اینترنتِ اعتماد را با حکمرانی نوین، پیگیری می‌کند) (کیانخواه، ۱۳۹۷).

امروزه توسعه‌ی امنیت فضای سایبر همسو با ملاحظات حفاظتی و ایمنی مرزها و زیرساخت‌های حساس نظیر نیروگاه‌ها، سدها، پادگان‌ها، مراکز و تأسیسات هسته‌ای به عنوان یکی از دغدغه‌های اصلی کشور است. نحوه تعامل با فضای سایبر کلیدی‌ترین موردی است که باید سازمان‌ها در راهبردهای خود لحاظ نمایند. امروزه این رویکرد، در دکترین سازمان‌ها قرار گرفته است. از سویی مشخص بودن دکترین و وجود اسناد راهبردی امنیت سایبری، پیش‌نیاز ورود به طرح جامع در فضای سایبر است (Alexander, (Wells, 2008) Klimburg, 2012).

جمهوری اسلامی ایران در حوزه مجازی نیز همانند حوزه‌های سیاسی و امنیتی، یکی از جدی‌ترین اهداف ایالات متحده آمریکا است. حملات سایبری در کنار تحریم تجهیزات، از اساسی‌ترین روش‌هایی هست که تاکنون علیه ایران به کار گرفته شده است (تهاجم مدرن، ۱۳۹۲، ص ۴۳). این حملات در سالیان اخیر همواره متوجه زیرساخت‌ها و تأسیسات تکنولوژیک ایران بوده است، از آغاز اولین دوره ریاست جمهوری اوباما در ایالات متحده، تولید نسل جدید ویروس‌ها برای حملات سایبری علیه جمهوری اسلامی ایران با سازماندهی دولتی آغاز شد (همان، ۱۳۹۲، ص ۵۴).

ویروس‌های رایانه‌ای بی‌شماری از جمله استاکس‌نت<sup>۲</sup> (برای حمله به بخش‌های صنعتی)، گاوس<sup>۳</sup> (برای حمله به سیستم بانکی)، فلیم<sup>۴</sup> (برای حمله به زیرساخت‌های نفتی)، مدی<sup>۵</sup> (برای حمله به نرم‌افزارهای

<sup>1</sup>The Wizard of Oz

<sup>2</sup>Stuxnet

<sup>3</sup>Gauss

<sup>4</sup>Flame

<sup>5</sup>Madi

ارتباطی روی رایانه‌های عمومی کاربران) و ناریلام<sup>۶</sup> (برای تخریب پایگاه‌های داده اقتصادی، مالی و نیروی انسانی) یکی پس از دیگری تولیداتی بودند که مشترکا توسط NSA و موساد برای تهاجم سایبری علیه ایران طراحی شدند (همان، ۱۳۹۲، ص ۶۶). با توجه به مخاطرات تأثیر گذار این حملات در مؤلفه‌های امنیت ملی از جمله زیر ساخت‌های حیاتی، حساس، مهم، تدوین راهبردهای اثر بخش و عملیاتی برای مدیریت هدفمند بر فضای سایبر اجتناب ناپذیر است. تدوین نقشه راهبرد حکمرانی بر فضای سایبر راه حل جامعی است برای پیاده‌سازی اثربخش و عملیاتی راهبردهای حکمرانی بر فضای سایبر.

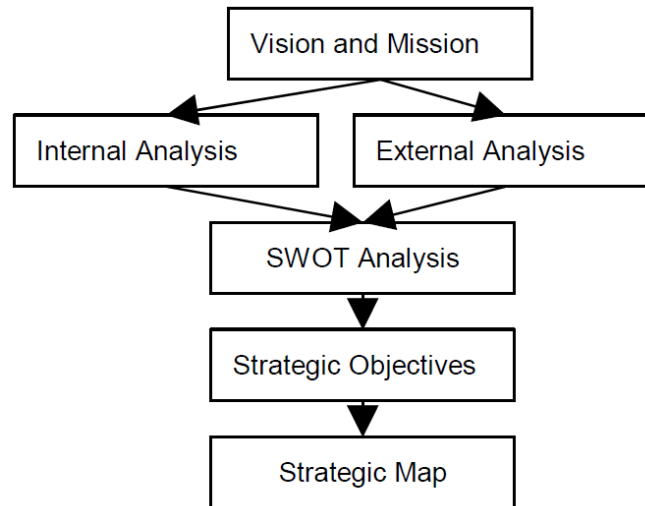
یکی از اصلی‌ترین چالش‌های تدوین نقشه راهبرد حکمرانی بر فضای سایبر، نداشتن الگوی مشخص و کاملی است که پوشش‌دهنده تمامی نیازمندی‌های مربوط به فرآیند تدوین نقشه راهبرد باشد (Neeley, 1999). در خصوص چالش‌های مدیریت هدفمند بر فضای سایبر (حکمرانی بر فضای سایبر) و راهبردهای لازم برای تحقق این مهم مطالب و محتواهای متعددی تدوین و نشر یافته است، اما در این خصوص یک الگو و نقشه جامع‌نگری که از زوایا و منظرهای متفاوت به راهبردهای این حوزه نگریسته شود و شاخص‌های تحقق راهبردها را احصا نموده باشد، موجود نیست و در این تحقیق به دنبال یافتن و طراحی الگویی جامع برای پاسخ به این مسئله هستیم. در تدوین نقشه راهبرد حکمرانی بر فضای سایبر، رویکرد ارزش‌محوری برای نظام جمهوری اسلامی، امنیت پایدار فضای سایبر ملی مبتنی بر مدیریت اثربخش می‌باشد (مجازی، ۱۳۹۷). لذا رویکردهای عمومی برای نقشه‌های راهبرد تجاری نمی‌توانند مبنای جهت دهنده برای تدوین نقشه راهبرد حکمرانی بر فضای سایبر باشند. در این مقاله، با رویکرد مؤلفه‌های حکمرانی بر فضای سایبر، الگوی تدوین نقشه راهبرد حکمرانی بر فضای سایبر ارائه گردیده است.

در ادامه ابتدا در بخش دوم انواع مدل‌های تدوین نقشه راهبرد بررسی می‌گردد و سپس در بخش سوم مسائلی اصلی حکمرانی بر فضای سایبر کشور بیان می‌گردد و سپس با ارائه یک الگوی پیشنهادی برای نقشه راهبرد حکمرانی بر فضای سایبر کشور، گام‌های سلسله‌مراتبی رسیدن به آن توضیح داده خواهد شد.

## ۲ روش تحقیق

نوع پژوهش حاضر توسعه‌های و آینده‌نگرانه است. روش تحقیق آن ترکیبی از توصیفی تحلیلی و اخذ نظرهای خبرگان به صورت کیفی می‌باشد. در ابتدا اطلاعات مورد نیاز از طریق بررسی منابع، کتب و مقالات پژوهشی جمع‌آوری گردیده و سپس مورد بررسی و تحلیل قرار گرفته است. بر اساس یافته‌های پژوهشی یک الگوی جامع تدوین نقشه راهبرد حکمرانی بر فضای سایبر ارائه گردیده و مبتنی بر یافته‌های دو تحقیق مرجع که یکی از آنها چالش‌های حکمرانی بر فضای سایبر (کیانخواه، ۱۳۹۷) و دیگری راهبردهای تحقق حکمرانی در قالب الگوی شش ضلعی (رضا غلامی، ۱۳۹۸) می‌باشند؛ اقدام به ارائه نمونه نقشه راهبرد حکمرانی بر این فضا گردیده است. در نهایت الگوی معرفی شده با اخذ نظرات (در قالب مصاحبه تخصصی) خبرگان راهبردی حوزه سایبر مورد ارزیابی قرار گرفته است.

<sup>6</sup>Narilam



شکل ۱: الگوی اول در طراحی نقشه راهبرد (Luis, 2007)

### ۳ بررسی الگوهای موجود تدوین نقشه راهبرد

اولویت‌دار بودن مطلوبیت‌های اساسی، اهداف کلان و یا موضوعات راهبردی در سازمان‌های مختلف باعث شده بر اساس این موضوعات الگوهای مختلفی برای تدوین نقشه راهبرد ارایه گردد. میزان توجه به فرآیند تجزیه و تحلیل عوامل محیطی و داخلی سازمان‌ها در شکل‌گیری این الگوها نقش اصلی را دارا می‌باشد. الگوهای تدوین نقشه راهبرد مورد استفاده در تعداد زیادی از انواع سازمان‌ها، نشان می‌دهد که الگوهای مورد استفاده شامل سه الگو بوده است (Sterner, 2003) (Luis, 2007).

در الگوی شماره ۱ (شکل ۱) مطلوبیت‌های اساسی و عوامل محیطی و درونی در الگوی تدوین نقشه راهبرد تأثیرگذار است. در این الگو پس از تعیین مطلوبیت‌های اساسی، بررسی عوامل محیطی انجام می‌گیرد و با استفاده از ماتریس SWOT ضمن احصاء اهداف راهبردی<sup>۷</sup>، به طراحی نقشه راهبرد پرداخته می‌شود. در الگوی شماره ۲ (شکل ۲) مطلوبیت‌های اساسی و اهداف کلان در الگوی تدوین نقشه راهبرد تأثیرگذار است. روش دوم شبیه به روش اول است، اما تفاوت در این است که دو نوع از اهداف تعریف شده است: اهداف عمومی<sup>۸</sup> به‌طور مستقیم از چشم‌انداز و مأموریت تعریف شده است، در حالی که اهداف خاص<sup>۹</sup> از تجزیه و تحلیل SWOT تعریف شده است.

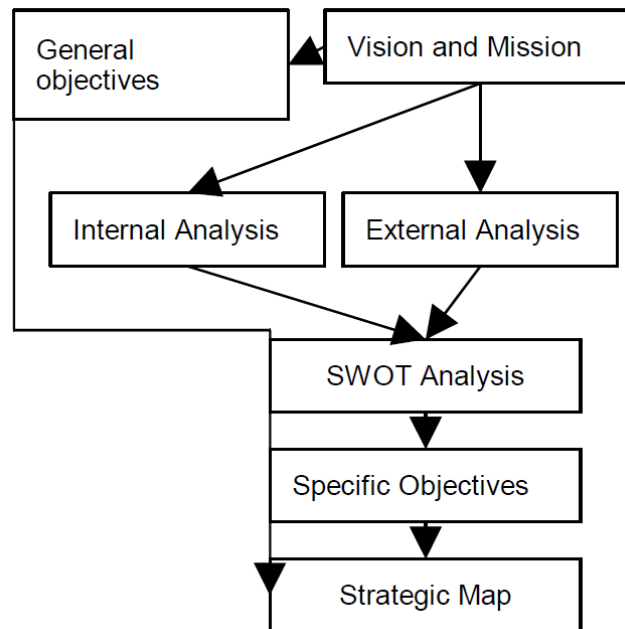
در الگوی شماره ۳ (شکل ۳) مطلوبیت‌های اساسی و اهداف کلان در الگوی تدوین نقشه راهبرد تأثیرگذار است. در این الگو شناسایی موضوعات راهبردی<sup>۱۰</sup> از چشم‌انداز و مأموریت سازمان تعریف می‌شود که مبنایی

<sup>7</sup>Strategic Objectives

<sup>8</sup>General Objectives

<sup>9</sup>Specific Objectives

<sup>10</sup>Strategic Themes

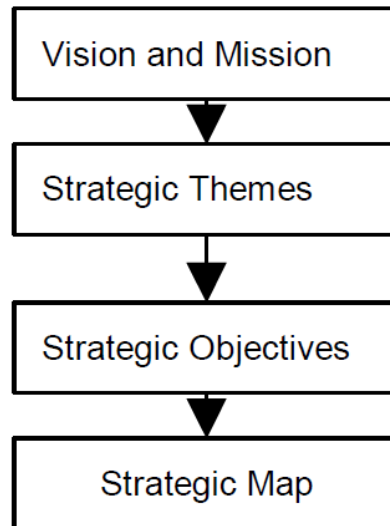


شکل ۲: الگوی دوم در طراحی نقشه راهبرد (Luis, 2007)

است برای تعریف اهداف راهبردی.

بر اساس بررسی لویس (Luis, 2007) ۵۰ درصد سازمان‌ها از روش اول و ۱۶/۵ درصد سازمان‌ها از روش دوم و ۳۳/۵ درصد سازمان‌ها از روش سوم استفاده کرده‌اند. سازمان‌ها برای تهیه نقشه راهبرد خود، متناسب با مأموریت و سایر شرایط از قالب‌هایی که حاصل تجربه‌های موفق سازمان‌ها و شرکت‌های مختلف می‌باشد به عنوان الگوی تدوین نقشه استفاده می‌نمایند. می‌توان گفت که ساختار واحد و سلسله‌مراتبی مشخصی برای تدوین نقشه راهبرد وجود ندارد. در واقع می‌توان معایب زیر را در روند تدوین نقشه راهبرد اشاره نمود (Neeley, 1999):

۱. الگوی مشخص و کاملی که پوشش‌دهنده تمامی نیازمندی‌های مربوط به فرآیند تدوین نقشه راهبرد باشد معرفی نشده است.
۲. در الگوها و قالب‌های معرفی شده طریقه احصای گام‌به‌گام بخش‌های مختلف الگو از قبیل اهداف و فرآیندهای وجه داخلی به صورت کامل توضیح داده نشده است.
۳. روش مشخصی برای احصای روابط علت و معلولی بین اهداف قید نشده است.
۴. به دلیل عدم تعیین چارچوب مشخص برای نقشه راهبرد، دیده شده است که هر سازمانی متناسب سلیقه خود تصویر علت و معلولی از راهبردهای سازمانی خویش را به عنوان نقشه راهبرد خود ارائه نموده است.



شکل ۳: الگوی سوم در طراحی نقشه راهبرد (Luis, 2007)

## ۴ تبیین واژه حکمرانی

حکمرانی واژه‌ای است که از اوایل دهه ۱۹۹۰ رایج شد و معمولاً مشابه با دولت و به جای آن مورد استفاده قرار گرفته است. فرهنگ فشرده آکسفورد دولت را به عنوان مجموعه‌ای از نهادهای تشکیل شده از افراد که یک اداره و یا وزارتخانه را هدایت و اداره می‌کنند، تعریف می‌کند. این فرهنگ همچنین دولت را «روش حکومت کردن» تعریف می‌کند. این فرهنگ تعریف بسیار مشابهی برای حکمرانی ارائه می‌دهد که عبارت است از: عمل، روش، حقیقت و یا وظیفه‌ی حکومت کردن، نفوذ و کنترل. همان‌گونه که مشاهده می‌شود، این دو واژه بسیار گمراه‌کننده و مبهم هستند (قیونلو، ۱۳۹۷).

اما این ابهام در کاربرد این دو واژه، پیامدهای نامناسبی را به همراه خواهد داشت. نتیجه آن خواهد بود که مسائل مربوط به خط مشی، بی‌چون و چرا تبدیل به یک مسئله دولتی می‌شود. پیامد منطقی این موضوع، چنین خواهد بود که مسئولیت رسیدگی به این مسئله ضرورتاً بر دوش دولت قرار می‌گیرد و راه‌های دیگر برای پرداختن به مسئله و یا بخش‌های دیگر جامعه که باید در پرداختن به مسئله از خود ابتکاراتی بروز دهند، مد نظر قرار نخواهند گرفت. پس، یکی دانستن دولت با حکمرانی، روش‌های شناسایی مسئله را محدود خواهد کرد و باعث گمراه شدن فرد در شناسایی استراتژی‌های مختلفی می‌شوند که برای برطرف کردن مشکل، در دسترس و مناسب خواهند بود. به‌طور خلاصه، وجود ابهام در واژه‌شناسی مرتبط با حکمرانی می‌تواند پیامدهای اجرایی مهمی در پی داشته باشد. این امر ممکن است بر تعریف مسئله و نحوه تجزیه و تحلیل خط مشی رفع آن تأثیر بگذارد.

پروفسور دونالدکتل در کتاب خود با عنوان تغییر حکمرانی<sup>۱۱</sup> مباحثی را در خصوص تمایز بین دولت و

<sup>11</sup> Transformations of governance



حکمرانی ارائه می‌دهد. دولت یک فراساختار نهادی<sup>۱۲</sup> است که جامعه برای تبدیل سیاست‌ها به خط‌مشی‌ها و قانون مورد استفاده قرار می‌دهد. حکمرانی، پیامد (نتیجه) تعامل دولت، خدمات عمومی و شهروندان از طریق فرایند سیاسی، توسعه خط‌مشی، طراحی برنامه و ارائه خدمت است. در اصل، مفهوم حکمرانی را می‌توان برای اشکال مختلف اقدامات اشتراکی مورد استفاده قرار داد. حکمرانی متوجه ابعاد استراتژیک‌تر هدایت است، یعنی اتخاذ تصمیمات کلان‌تر در خصوص نحوه هدایت و نقش‌ها. به عبارت دیگر، حکمرانی فقط متوجه این سؤال نیست که «به کجا برویم» بلکه در پی پاسخگویی به این سؤالات نیز هست: چه کسی باید در تصمیم‌گیری دخیل باشد و با چه ظرفیتی. مفهوم حکمرانی در چهار سطح زیر مطرح است:

- حکمرانی در فضای جهانی، که با مسائل فراتر از حوزه دولت‌های ملی سروکار دارد.
- حکمرانی در فضای ملی، یعنی درون یک کشور. این سطح خود دارای سطوح زیر است: سطح ملی، استانی، شهری و محلی.
- حکمرانی در فضای سازمان یا حکمرانی سازمانی. این سطح شامل فعالیت‌های مختلف سازمان‌ها می‌شود که معمولاً باید در برابر هیأت مدیره پاسخگو باشد. برخی از این سازمان‌ها خصوصی‌اند (نظیر شرکت‌های تجاری خصوصی) و برخی دیگر دولتی نظیر (بیمارستان‌ها، مدرسه‌ها، شرکت‌های دولتی و ...)
- حکمرانی در فضای جوامع محلی، که این سطح شامل فعالیت‌هایی در سطح محلی می‌شود (قیونلو، ۱۳۹۷).

حکمرانی بیان شیوه و حالت حکومت کردن است و حاکمیت ابزار و نتیجه حکومت کردن را ترسیم می‌کند. در حکمرانی به مجموعه‌ای از فرایندها اشاره دارد که با قدرت، اقتدار و نفوذ، سیاست‌ها و رویه‌هایی را برای حکومت کردن در دست می‌گیرد. وادی حکمرانی، وادی هدایت و کنترل است و با خلق و بازتولید قوانین، هنجارهای اجتماعی و اقدامات ساختاریافته در ارتباط است. از طرفی، حکمرانی نیازمند جهت و تنظیم‌غایت است. یعنی حکمرانی برای هدف و غرضی شکل می‌گیرد. همان‌طور که در حاکمیت شرکتی<sup>۱۳</sup> هدف تنظیم روابط بین سهام‌دار و هیئت مدیره است تا بتوان حداکثر منفعت و ارزش پایدار را برای سهام‌دار تحقق بخشید. به‌طور کلی ویژگی حکمرانی می‌تواند فرایندمحور، یعنی توجه به اثربخشی فرایند، کل‌نگر، یعنی توجه به تمام فعل و انفعالات سیستم و پدیده، پیش‌بینی‌پذیر یعنی درک بیرونی درست از عکس‌العمل حکمرانی در شرایط متفاوت، پاسخگویی یعنی بیان هم علت و هم دلیل تصمیم و مسئولیت‌پذیری در اقدامات، مسئله‌محور یعنی انضمامی و ناظر به مکان و زمان مشخص و درنهایت جهت‌دار یعنی هدایت و کنترل برای دستیابی به تعالی و ارتقاء مشخص باشد (کیانخواه، ۱۳۹۷).

<sup>12</sup>Institutional superstructure

<sup>13</sup>Corporate Governance

در حکمرانی سایبری، حکمرانی متعلق مفهومی به نام سایبر است (البته حکمرانی سایبر با حکمرانی سایبری متفاوت است، اما به نظر می‌آید حکمرانی در حال سایبری شدن است). مفهوم سایبر در عین سادگی و درک عمومی دارای ابعاد و گستره‌ای ناشناخته است. در کشور ما فضای سایبر<sup>۱۴</sup> معادل مفهومی به نام فضای مجازی قرارداد شده است. انگاره نگارنده از سایبر مفهومی دقیق‌تر و عمیق‌تر از دو مفهوم فضای سایبر و فضای مجازی است. در چند سال گذشته بحث‌های متنوعی پیرامون مجاز و مجازی بودن و حقیقی بودن فضای سایبر شده است. البته شاید با کوچک‌ترین آشنایی با گستره سایبر این بحث‌های حاشیه‌ای و غیر مرتبط با حل مسائل سایبر شکل نمی‌گرفت. پدیده‌ایی که نگارنده از آن به سایبر یاد می‌کند، عالم نوپدید است که طلیعه‌هایی از آن آشکار شده است. عالم نوپدید نه به‌مثابه عوالمی که حکما از آن یاد می‌کنند، بلکه منظور شکل جدیدی از زندگی است که تاکنون بشر آن را تجربه نکرده است. این عالم نوپدید در مقابل عالم عادت‌شده‌ای است که بشر سال‌ها از زمان هبوط حضرت آدم (ع) آن را تجربه کرده است. انقلاب کشاورزی و انقلاب صنعتی و تحولات فناورانه از این دست، همیشه بخشی از عالم محسوسات ما را تغییر داده یعنی به‌طور مثال با قوانین فیزیکی خودرو طراحی شده، نیروگاه برق تولید کرده، نفت استخراج و پالایش شده، 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 نیز مصنوعات و محسوساتی را ساخت. این تحول ژرف عالم نوپدید است که فراتر از تعاریف ساده از فضای سایبر یا فضای مجازی است.

عالم نوپدید سایبر در حال بلعیدن عالم کنونی است و زیست‌جهان نوینی را بر پایه فناوری، شتاب و همگرایی در حال شکل دادن است که همه رفتارهای فردی و اجتماعی را در خود جای داده و بزرگ‌تر از عالم عادت شده کنونی 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 به‌سمت این عالم هستیم، به هر پدیده طبیعی در حال دمیدن روح سایبر است. 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 روح سایبری کنش سایبری نیز دارند. مفاهیمی همچون واقعیت مجازی<sup>۱۵</sup> با کمک سیستم‌های سایبر فیزیکال<sup>۱۶</sup> و اینترنت همه‌چیز<sup>۱۷</sup> در حال ساختن اثر فیزیکی برای اجسامی کاملاً سایبری هستند. کمک‌یار استاد در زمان تدریس برای بیان اثربخشی آموزش، دستیار سایبری مذاکره‌کننده برای بیان سطوح پیچیده و کشف ابعاد مذاکره، استراتژیست‌یار برای معمار سازمان و فرمانده نظامی یا هر آنچه شما در خیال و تصور خود بسازید، قابلیت تحقق سایبری با اثر فیزیکال دارد. انگار ما به ساخت عالمی شبیه عالم کن‌فیکونی خیال که گسترده و متکثر بین همه انسان‌هاست نزدیک شده‌ایم - به‌مثابه عالم خیال متصلی که تعلق و قطع ذهن در وجود و عدم آن تأثیر ندارد - خیال محسوس یکپارچه متکثر جهانی در حال پدید آمدن است.

حال همین فضای سایبر خالی از جهت نیست. به‌وضوح تغییر هویت و فرهنگ‌ها با فضای سایبر قابل

<sup>14</sup>Cyberspace

<sup>15</sup>Virtual Reality

<sup>16</sup>Cyber-Physical Systems

<sup>17</sup>Internet of Everything

مشاهده است. فضای سایبر و عالم سایبر صرفاً حوزه فناوری نیست که در فضای انسانی-اجتماعی امتداد یافته است، بلکه ذاتاً حوزه شناختی و اجتماعی است. جنگ شناختی و تغییر هویت دینی و ملی با فضای سایبر قابل انکار نیست. این تغییر در لابلای جذابیت فناوری، به روز بودن، کسب و کارهای دیجیتالی، اعتماد به شبکه‌های اجتماعی و ... نهفته است. در کلان فضای سایبر دو جهت‌گیری (۱) اشراف راهبردی برای ایالات متحده و ابر شرکت‌ها و (۲) جهانی‌سازی سبک زندگی غربی قابل مشاهده است. یکی از شئون قدرت در فضای سایبر اشراف همه‌جانبه است. به کمک جریان گسترده اطلاعات شخصی، اجتماعی و ملی و ملی سازی فضای سایبر که از بین مسیریاب‌های متنوع شبکه و خدمات اینترنتی انتقال می‌یابد و تکنیک‌های تحلیل داده عظیم<sup>۱۸</sup> همه صاحبان صنایع سایبری و دولت‌ها به سمت جمع‌آوری، تحلیل و اشراف بر سایبر جوامع و کشورها و استعمار نوین سوق داده است. در حقیقت مهندسی و مدیریت فکر که منجر به مهندسی فرهنگی، اقتصادی و سیاسی می‌شود برای ابرشرکت‌ها و آمریکا که به نوعی مالک زیرساخت و دربردارنده سرویس‌های جهانی است، تحقق می‌یابد. از طرفی سبک زندگی غرب مدرن که از تمدن غربی با رویکردهای اقتصادی و فرهنگی خاص خود است، در حال جهانی‌سازی به زعم جذابیت فناوری است. این تحقق نه فقط در محتوای پراکنده شده از طریق سایبر که در فرم روابط نیز نهفته است. در حقیقت ماده و صورت هستند که در راستای قابلیت‌ها و انگیزه‌های پدیدآورنده محقق شده و خدمت و خدمتی را می‌سازد. در عالم سایبر قدرت نرم و سخت سایبری با ساخت سبک زندگی گره خورده است (کیانخواه، ۱۳۹۷).

تحقیقات در استفاده از مفاهیم حکمرانی و حکمرانی سایبری در راهبردهای ملی امنیت سایبری نشان می‌دهد که تعداد کمی از دولت‌ها از واژه «حکمرانی» استفاده می‌کنند و واژه «حکمرانی سایبری» تنها توسط دولت کانادا استفاده می‌شود. این مفهوم در ابتدا توسط دولت‌های غربی به کار رفت که به تعریفی از حکمرانی اشاره دارد که کاملاً با قانون بین‌المللی همخوانی دارد. راهبردهای امنیت سایبری در بیشتر کشورها نشان می‌دهد که حملات سایبری ممکن است تهدیدی برای حاکمیت دولت باشد و تأکید آنها بر حفاظت از حاکمیت دولت است. برای رسیدن به این هدف، دولت‌ها برای بهبود امنیت سایبری در فناوری‌های اطلاعاتی و شبکه‌های دولتی، دفاع و زیرساخت‌های حیاتی برنامه‌ریزی‌هایی انجام داده‌اند. بحث غالب محققان این حوزه، حقوق و تعهدات مرتبط با حاکمیت دولت و نحوه استفاده از آن در فضای مجازی و همچنین بعد فیزیکی حاکمیت در فضای مجازی است؛ زیرساخت‌های فیزیکی برای عملکرد مناسب فضای مجازی ضروری است و اکثر این زیرساخت‌ها در قلمرویی قرار دارند. بنابراین حاکمیت دولتی در فضای مجازی می‌تواند به عنوان توسعه‌ای از حاکمیت ارضی دولت در نظر گرفته شود (مرکز ملی فضای مجازی، ۱۳۹۷).

## ۵ مهم‌ترین مسائل و چالش‌های حکمرانی بر فضای سایبری

بزرگ‌ترین خطر هنگام به وجود آمدن تغییرات، خود تغییرات نیستند بلکه عمل کردن با منطق دیروز است. مقارن با توسعه فضای سایبر در کشور، در صورت عدم توجه به توسعه امنیت آن، شاهد افزایش و گسترده‌تری تهدیدات و جرائم و آسیب‌ها در این فضا خواهیم بود. شناخت وضع موجود فضای سایبر کشور به دلیل

<sup>18</sup>Big Data Analytics

وسعت و پیچیدگی آن و همچنین تأثیر پذیری از تعداد زیادی از ذی‌نفعان، دشوار است. فضای سایبر یک ابزار است و هر شخص یا نهادی می‌تواند این ابزار را برای تحقق اهداف خود به کار گیرد. این فضا در معرض چالش‌ها، آسیب‌ها و تهدیدهای گوناگونی نظیر ارتکاب جرائم سازمان‌یافته، تخریب بانک‌های اطلاعاتی، حملات مختل‌کننده خدمات، جاسوسی، خرابکاری، نقض حریم خصوصی و نقض حقوق مالکیت معنوی قرار دارد، به طوری که نپرداختن یا رویکرد نادرست به امنیت این فضا، مانعی بزرگ پیشروی گسترش کاربرد این فضا و ورود به جامعه اطلاعاتی خواهد بود. یک جامعه اطلاعاتی ایمن جامعه‌ای است که در آن همه کاربران به این جامعه اطمینان دارند و قادرند اطلاعات را به گونه‌ای مطمئن به اشتراک گذارده و مدیریت نمایند (ایران، ۱۳۹۰).

توسعه فضای سایبر در ابعاد و حوزه‌های مختلف، فرصت‌های مناسبی را برای کشور فراهم ساخته است اما از فرصت‌های موجود در فضای سایبر به خوبی استفاده نمی‌شود. به عبارت دیگر، مشکلات و ضعف‌های داخلی اجازه بهره‌برداری بیشتر از فرصت‌ها را نمی‌دهد. لذا لازم است به نحوی برنامه ریزی شود که ضمن پوشش دادن ضعف‌های داخلی، از فرصت‌ها نیز حداکثر بهره‌برداری صورت پذیرد (مجمع گروه مطالعات و تحقیقات راهبردی، ۱۳۸۸).

فضای سایبر عرصه مراقبت، کنترل، مقابله، مخاصمه و فصل‌نخست‌درگیری در مدل جدید تهدیدات بین‌المللی می‌باشد لذا این فضا علاوه بر سایر ویژگی‌های یک عرصه امنیتی و دفاعی است. امنیت در فضای سایبر یک مفهوم یکپارچه پیوسته و غیرقابل تفکیک (بین اجزاء و بخش‌های تشکیل‌دهنده) می‌باشد. حوزه تأثیر امنیت فضای سایبر، کلیه فعالیت‌های آحاد جامعه (حقیقی و حقوقی، دولتی و خصوصی) در این فضا را شامل می‌شود.

از اصلی‌ترین مسائل حکمرانی بر فضای سایبری نظام جمهوری اسلامی ایران، سیاست‌های خصمانه استکبار جهانی بر علیه کشور ما می‌باشد. برای داشتن یک دفاع اثربخش در فضای سایبر لازم است سیاست‌گذاری و برنامه ریزی در این فضا به نحوی باشد که با بهره‌گیری مناسب از ظرفیت‌های علمی و پژوهشی کشور ضمن حمایت از تولیدات داخلی، در جهت ایجاد انسجام و هماهنگی بین ساختارهای حکمرانی بر فضای سایبر گام برداریم. برای داشتن یک نگاه همه‌جانبه برای امن‌سازی فضای سایبر ملی به ویژه زیرساخت‌های حیاتی کشور و حمایت و تقویت همه‌جانبه و نظام‌مند از ظرفیت‌های داخلی در حوزه سایبر از جمله تولید دانش، تحقیق، توسعه و صنعت، نیازمند داشتن یک نقشه راهبرد جامع می‌باشیم (مجمع گروه مطالعات و تحقیقات راهبردی، ۱۳۸۸).

فضای سایبر با سرعت بالایی در حال پیش رفتن است. سرویس‌های مکان‌محور در حال رصد توانمندی‌های اقتدارافزای جامعه در پوشش جذابیت فناوری است. شبکه‌های اجتماعی به ابرگراف تعاملات و روابط جامعه دست پیدا کرده‌اند و کسی دیگر از رصد پنهان نیست. محتواهای نادقیق و مغرضانه به مراجع کاذب معتبر شده در فضای سایبر تبدیل شده است. موتورهای جستجو در حال جهت‌دهی به فکر و اندیشه کاربر و مهندسی و مدیریت جامعه هستند. مرورگرها همه تعاملات و ارتباطات کاربران و جوامع را رصد می‌کنند و سرویس‌های ابری در حال متمرکز ساختن داده‌ها هستند و اینترنت اشیا به رصد همه رفتارها می‌پردازد. جنگ نرم و ناتوی فرهنگی غرب با بستر فضای سایبر ملموس شده است. با این حال برخی این

جنگ همه‌جانبه را در پوشش فناوری‌های جذاب و فریبنده سایبری نمی‌بینند (کیانخواه، ۱۳۹۷).  
به خدمت گرفتن هر پدیده نیازمند فهم دقیق آن است و نیاز به توجه به مصالح و مفاسد آن دارد. فضای سایبر در کنار تحولات مطلوب و پر شتاب آن دارای مفاسد است که موجب چالش‌های کلیدی برای حکمرانی کشور شده است. عمده چالش‌های حکمرانی با گسترش فضای سایبر عبارتند از:

۱. هژمونی آمریکا در مدیریت و کنترل فضای سایبر

۲. شناسایی و نظارت فراحاکمیتی بر توانمندی‌های اقتدارافزای جامعه

۳. تهدیدات و تهاجمات سایبری

۴. پذیرش الگوی رفتاری و سبک زندگی فراملی و فرافرهنگی

۵. مهندسی و مدیریت فرهنگی فراملی

۶. فرهنگ منحط و اباحه‌گر

غلبه بر این چالش‌ها نیازمند ترسیم چارچوبی برای حکمرانی نوین است (کیانخواه، ۱۳۹۷).

## ۶ راهبردهای اساسی پیشنهادی برای تحقق حکمرانی

در سال‌های اخیر و با وجود تأسیس شورای عالی فضای مجازی و زحمات زیادی که دلسوزان این میدان در زمینه تغییر موقعیت جمهوری اسلامی در مواجهه با فضای مجازی کشیده‌اند، اما هیچوقت «ایده جامعی» برای حکمرانی در این فضا نداشته‌ایم. البته ایده جامع از طرفی از بطن یک ادراک عمیق و همه‌جانبه از فضای مجازی و تحولات جهانی در این عرصه زاییده می‌شود و از طرف دیگر، زمانی متولد می‌شود که رویکرد انفعالی به فضای مجازی به رویکرد فعال و مبتکرانه تبدیل شده باشد. بنابراین، شاید این انتظار که کشور ما در سال‌های قبل به یک ایده جامع درباره حکمرانی رسیده باشد، انتظار به‌جایی به‌شمار نیاید. علاوه بر این، روشن است که تحقق ایده جامع نه فقط نیازمند عزم و اراده پولادین، بلکه محتاج یک هدایت، یک هماهنگی، یک مانع‌برداری و یک هم‌افزایی جدی در این عرصه است (غلامی، ۱۳۹۸).

### راهبرد اساسی ۱: تکمیل و راه‌اندازی شبکه ملی اطلاعات

بر اساس طراحی کلان شورای عالی فضای مجازی، شبکه ملی اطلاعات از سه لایه زیرساخت، محتوا و خدمات تشکیل شده است. تاکنون به لطف الهی و با زحمات وزارت ارتباطات و فناوری اطلاعات، بخش مهمی از لایه اول، یعنی لایه زیرساخت شکل گرفته است. با وجود این، باید کاری کرد تا بر اساس یک نقشه مهندسی دقیقتر، این لایه با همه لوازم آن قابل بهره‌برداری بوده و تست‌های لازم روی آن مثبت باشد. لایه زیرساخت به تنهایی می‌تواند علاوه بر تأمین سطح خوبی از امنیت، اعم از امنیت ملی و امنیت تک تک کاربران چه در

حوزه فنی، چه در حوزه اقتصادی و چه در حوزه فرهنگی سیاسی، فرصت برخورداری از سرعت بالا و قیمت مناسب را فراهم کند ضمن آنکه شبکه ملی اطلاعات از طریق دروازه‌های هوشمند خود با فضای مجازی جهانی ارتباط دارد و اتفاقاً فرصت‌های بیشتر و مقرون به صرفه‌تری را برای ارتباطات جهانی فراهم میکند. با وجود این، سرمایه‌گذاری همه جانبه و شروع عملیات شکل‌گیری لایه دوم و سوم باید در دستور کار شورای عالی فضای مجازی قرار بگیرد تا همزمان با تکمیل لایه اول بخش مهمی از این دو لایه نیز تمام شود.

## راهبرد اساسی ۲: شکل‌دهی به اینترنت دوم یا ایجاد شبکه فراملی اطلاعات

ما باید برای مهار قدرت جریان امریکایی صهیونیستی، جهان را به سمت شکل‌گیری اینترنت دوم سوق دهیم. امروز چینی‌ها، روس‌ها و خلیجی‌های دیگر از انگیزه لازم برای ورود به این میدان برخوردارند و جمهوری اسلامی می‌تواند بر کسب منافع مشترک خود با دیگران و البته با حفظ شبکه ملی اطلاعات در بطن اینترنت دوم یا شبکه فراملی اطلاعات، به سهم خود در ایجاد شکاف بین امریکاییها و دیگران نقش آفرین باشد.

## راهبرد اساسی ۳: شکل‌دهی یک ائتلاف جهانی برای کاهش اختیارات آمریکا در فضای مجازی و ایجاد نظام حقوق بین‌الملل برای فضای مجازی

روشن است که فضای مجازی در شرایط فعلی به شیوه کدخدگری اداره می‌شود و کدخدا خود را به هیچ‌کس پاسخگو نمی‌داند. شاید بدانید که تا الآن تلاش‌های زیادی برای کشاندن مسائل فضای مجازی به سازمان ملل و مجامع وابسته به آن از سوی کشورهای مختلف صورت گرفته اما با مخالفت و کارشکنی امریکایی‌ها روبرو شده است. بنابراین، ما باید با تأسیس معاونت فضای مجازی در وزارت خارجه و تربیت دیپلمات‌های زبده و شجاع، به سمت ایجاد یا تقویت ائتلاف‌هایی که خواهان کاهش اختیارات بی‌حد و مرز امریکایی‌ها در فضای مجازی هستند، حرکت کنیم و در این زمینه از تأثیر دیپلماسی عمومی هم غافل نباشیم.

## راهبرد اساسی ۴: ایجاد غلبه گفتمانی برای مواجهه معقول و انقلابی با فضای مجازی

هرگونه موفقیت در تحقق الگوی حکمرانی، مستلزم ایجاد فضای ذهنی مناسب به مفهوم باز شدن یک چتر گفتمانی بسیار قوی بر روی این الگو است. این چتر گفتمانی است که بازیگران داخلی و حتی بین‌المللی همسو با جمهوری اسلامی و فراتر از آن، کل مردم را به صورت خودجوش با سیاست‌های جمهوری اسلامی همراه خواهد کرد و موانع را به راحتی از سر راه برخواهد داشت. ما امروز فاقد این چتر گفتمانی هستیم و حتی اجازه داده‌ایم گفتمان‌هایی که با سیاست‌های جمهوری اسلامی همسو نیستند در جامعه ما رشد کنند. البته ایجاد چتر گفتمانی نه تنها متدولوژی خاص خود را دارد بلکه از لوازمی برخوردار است که یکی از مهم‌ترین آن، وفاق نظری میان مسئولان ارشد کشور است.



## راهبرد اساسی ۵: راه اندازی شرکت های عظیم غیردولتی با رویکرد فراملی و باز کردن میدان نوآوری

لازمه بازیگری در میدان و قرار گرفتن در مقام قانون گذاری، ایجاد بسترهای مساعد برای شکل گیری شرکتهای بزرگ دانش بنیان است. یعنی جمهوری اسلامی باید با ایجاد صندوق مالی قوی و ارائه تسهیلات درشت، زمینه شکل گیری شرکتهای دانش بنیان حول طرح های خلاقانه را فراهم کند. هرچند در ابتدا این شرکتهای در محیط های کوچک و محلی شکوفا می شوند اما باید از قابلیت کار فراملی برخوردار باشند. البته از آنجا که کشور ما در معرض یک نفوذ سازمان دهی شده از بیرون است، جا دارد بسترسازی برای شکل گیری این شرکتهای کاملاً محتاطانه باشد. در حال حاضر الگوی گنگو<sup>۱۹</sup> یعنی مجموعه های مردم نهادی که ارتباط معناداری با دولت دارند، در بعضی کشورها تجربه شده و این تجربه قابل سرایت به ایران است. حتی می توان به الگویی دست یافت که امکان جذب سرمایه گذار خارجی به شیوه امن را نیز فراهم کند. وقتی شرکتهای کوچک تدریجاً به فعلیت رسید، ادغام این شرکتهای با هم با هدف ایجاد شرکتهای بزرگ تر و تواناتر، گام بعدی است که باید برداشته شود.

## راهبرد اساسی ۶: ایجاد بسیج سایبری با رویکرد محتوایی

بسیج سایبری با ارتش سایبری تفاوت دارد. بسیج سایبری، یعنی آموزش و به میدان آوری میلیونی مردم در جهت دفاع محتوایی از مرزهای ملی و دینی. در واقع، ما نباید نسبت به حمایت از ارزش های اسلامی و انقلابی در فضای مجازی و خنثی سازی هجومی که به این ارزش ها می شود، سستی به خرج دهیم؛ این در حالی است که در سال های اخیر، یکی از نقاط تمرکز دشمنان ما عملیات روانی علیه افکار عمومی بوده است. در عین حال، وقتی صحبت از بسیج سایبری می کنیم، این بسیج اختصاصی به مردم ایران ندارد و می تواند همفکران ما در اقصی نقاط جهان که مهم ترین دغدغه آنها ارزش های الهی است را هم در درون خود جا دهد (غلامی، ۱۳۹۸).

## ۷ الگوی پیشنهادی تدوین نقشه راهبرد حکمرانی بر فضای سایبری

باقی ماندن راهبردهای اساسی مربوط به حکمرانی بر فضای سایبر در سطح کلیات و یا جهت گیری های کلی و عدم توجه به جاری سازی این راهبردها از چالش های اساسی است که مانع اجرایی شدن راهبردهای حکمرانی بر فضای سایبری می شود. نقشه راهبرد حکمرانی بر فضای سایبر تلاش می کند راهبردهای اساسی حکمرانی بر فضای سایبری را در چارچوب روابط علی و معلولی نمایش داده و نشان دهد که چگونه راهبردهای حکمرانی بر فضای سایبری می توانند به اهداف قابل اندازه گیری و عملیات مشخصی تبدیل شوند تا واحدهای سازمان و کارکنان درک مشترک داشته و نسبت به پیاده سازی آنها اقدام نمایند (رابرت اس. کاپلان و دیوید پی.

<sup>19</sup>Gongo

نورتون، ۲۰۱۲). نقشه راهبرد حکمرانی بر فضای سایبر با تعیین روابط بین اهداف راهبردی در منظرهای مختلف، به پیاده‌سازی کامل و مطمئن راهبردهای حکمرانی بر فضای سایبری کمک کرده و نتایج مورد انتظار وجه‌های اثر بخشی و ذی‌نفعان را به عملکرد مطلوب فرآیندهای مهم داخلی مرتبط می‌سازد (کاپلان و نورتون، ۱۳۹۰) (Info-Tech Research, 2001) (قهرمانی، ۱۳۹۱). در تدوین نقشه راهبرد حکمرانی بر فضای سایبر تشخیص فرآیندهایی که برتری یافتن در آن‌ها به ارزش‌آفرینی برای ذی‌نفعان می‌انجامد، بسیار مهم است زیرا ایجاد ارزش برای ذی‌نفعان مستلزم انجام فرآیندهای عملیاتی سازمان به صورتی کارآمد و اثربخش است. رویکردهای موجود ارزش‌محوری برای ذی‌نفعان در فرآیند تدوین نقشه راهبرد عبارتند از رهبری محصول، هزینه نهایی پایین، مشتری‌مداری و راه حل جامع به ذی‌نفعان (کاپلان و نورتون، ۱۳۹۰) که محوریت این رویکردها مبتنی بر سودآوری برای سازمان و ذی‌نفعان می‌باشد.

برای برخورداری از یک سازوکار همه‌جانبه برای دفاع از فضای سایبر ملی نیازمند پرداختن به تمامی ابعاد حکمرانی بر فضای سایبر هستیم. با در نظر گرفتن مسائل مربوط به حکمرانی بر فضای سایبری ایران، الگوی پیشنهادی برای تدوین نقشه راهبرد حکمرانی بر فضای سایبری در شکل ۴ ارائه شده است. بر اساس این الگو مضامین راهبردی حکمرانی بر فضای سایبری که حاصل برنامه‌ریزی راهبردی می‌باشند در وجوه نقشه راهبرد اهداف مشخصی را دربر خواهند داشت و در بالاترین بخش نقشه منجر به نیل به اهداف کلان حکمرانی بر فضای سایبری می‌گردند. الگوی ارائه شده توسط مصاحبه با خبرگان و پرسش‌نامه مورد راستی‌آزمایی قرار گرفته است.

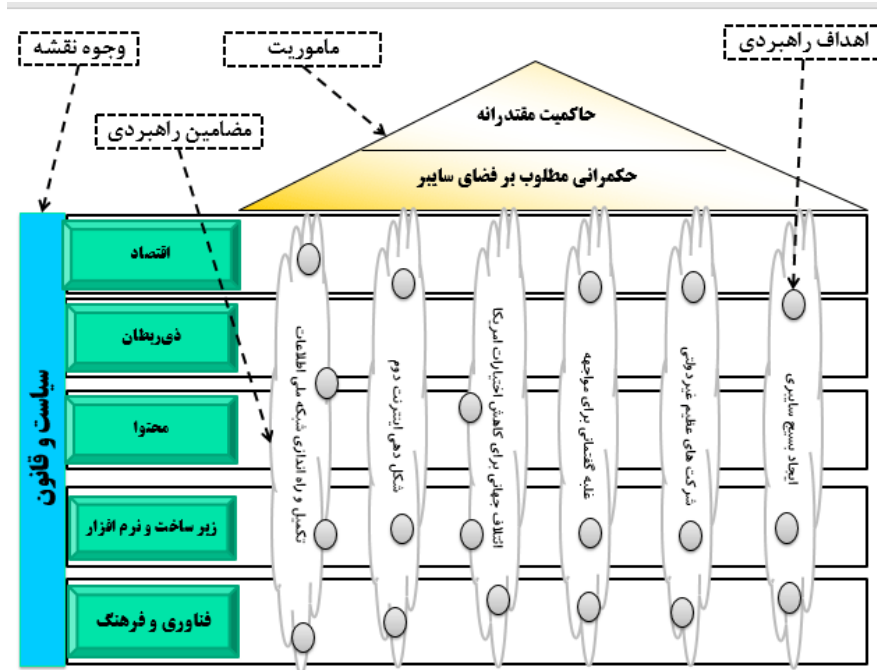
شش وجه تعیین‌شده پاسخگوی تمامی موضوعات حوزه حکمرانی بر فضای سایبری بوده و این امکان را فراهم می‌آورد که راهبردهای حوزه حکمرانی بر فضای سایبر در قالب اهداف کمی و کیفی از منظرهای مختلف مورد بررسی قرار گیرند.

تهیه الگوی پیشنهادی نقشه راهبرد حکمرانی بر فضای سایبر دارای فرآیندهای گام به گام تعیین‌شده‌ای است که خروجی هر گام به‌عنوان ورودی برای مراحل بعدی مورد استفاده قرار می‌گیرد، در ادامه گام‌های پیشنهادی تدوین نقشه راهبرد حکمرانی بر فضای سایبر ارائه شده است (قهرمانی، ۱۳۹۱).

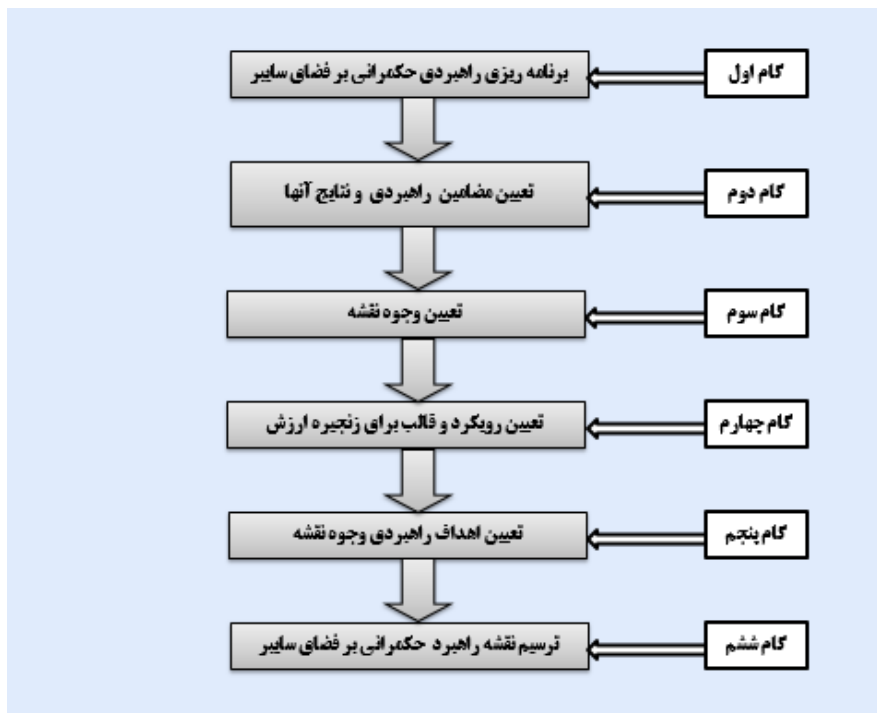
مراحل کلی تدوین نقشه راهبرد حکمرانی بر فضای سایبر به شرح شکل ۵ می‌باشد که هرکدام به‌صورت جداگانه در ادامه توضیح داده شده است:

## ۱.۷ (گام اول) برنامه‌ریزی راهبردی حکمرانی بر فضای سایبری

برنامه‌ریزی راهبردی حکمرانی بر فضای سایبر، عبارت است از فرآیندی که از طریق آن محیط داخلی و خارجی فضای سایبر ملی را تحلیل کرده و از این تحلیل شناخت کافی نسبت به فضای سایبر به‌دست آورده، بر اساس شناخت حاصله مسیر راهبردی پایه‌گذاری می‌شود. راهبردهای سایبری حاصل، ما را برای رسیدن به اهداف تعیین شده کمک می‌نماید. تمامی این اقدامات برای ارضای اعضای کلیدی فضای سایبر که تحت عنوان ذی‌نفعان فضای سایبر نامیده می‌شوند، به انجام می‌رسد. در گام برنامه‌ریزی راهبردی حکمرانی بر فضای سایبری مراحل زیر انجام می‌گیرد:



شکل ۴: قالب پیشنهادی نقشه راهبرد حکمرانی بر فضای سایبری



شکل ۵: گام‌های پیشنهادی تدوین نقشه راهبرد

۱. تعیین مطلوبیت‌های اساسی راهبردی حکمرانی بر فضای سایبری
۲. بررسی و تجزیه و تحلیل محیط داخلی و خارجی فضای سایبر ملی
۳. راه‌یابی راهبردی حکمرانی بر فضای سایبری

## ۲.۷ گام دوم) تعیین مضامین راهبردی حکمرانی بر فضای سایبر

مضامین راهبردی منعکس کننده‌ی نظرات مدیران ارشد است در مورد آنچه که باید در داخل سازمان انجام شود تا نتایج راهبردی محقق گردند. بنابراین مضامین راهبردی عموماً به فرایندهای عملیاتی سازمان مربوط می‌شوند. (رابرت اس. کاپلان و دیوید پی. نورتون، ۲۰۱۲) خواستگاه مضامین راهبردی، فرایندها می‌باشند. در واقع مضامین راهبردی، بیانگر این مطلب هستند که: برای رسیدن به اهداف کلان سازمان، چه کارهایی بایستی صورت پذیرد. مضامین راهبردی رکن اساسی در پیشرفت و ترقی سازمان هستند (Info-Tech Re-search, 2001). برای احصای مضامین راهبردی به این روش عمل می‌شود که بعد از احصای موضوعات اساسی حکمرانی بر فضای سایبری، اولویت‌های اساسی به عنوان مضامین راهبردی انتخاب می‌گردند. نتایج پیش بینی شده حاصل از اجرای مضامین راهبردی را می‌توان به عنوان اهداف کلان یا اهداف راهبردی بالاترین وجه نقشه در نظر گرفت.

## ۳.۷ گام سوم) تعیین وجوه نقشه

در عصر اقتصاد مبتنی بر دانش فعالیت‌های ارزش‌آفرین سازمان‌ها فقط متکی به دارایی‌های مشهود آنان نیست. امروزه دانش و قابلیت کارکنان، روابط با مشتریان سازمان، دارایی‌هایی به مراتب ارزشمندتر از دارایی‌های فیزیکی‌اند و توانمندی سازمان‌ها در به‌کارگیری این دارایی‌های نامشهود قدرت اصلی ارزش‌آفرینی آن‌ها را رقم می‌زند. بنابراین سازمان‌هایی موفق خواهند بود که عملکرد خود را فقط مبتنی بر منظر مالی نکنند بلکه به منظرهای مشتری، فرایندهای داخلی و یادگیری و رشد نیز توجه داشته است. بنابراین چهار منظر زیر در تدوین نقشه راهبرد مورد ارزیابی قرار می‌گیرد (Robert Kaplan, David Norton, 2004)، (Robert S. Kaplan, David P. Norton, 1996): مالی، مشتری، فرایندهای داخلی و یادگیری و رشد. از آنجایی که کسب موفقیت مالی هدف اولیه اکثر سازمان‌های دولتی و غیرانتفاعی نیست، این‌گونه سازمان‌ها با منظر مالی که در رأس روش ارزیابی قرار دارد، مشکل دارند و دو وجه مالی و مشتری را با هم ادغام می‌نمایند (Robert S. Kaplan, David P. Norton, 1992).

در ارایه الگوی نقشه راهبرد حکمرانی بر فضای سایبر، با توجه به اینکه هدف نظام جمهوری اسلامی در این فضا، بهره‌مندی سالم و امن جامعه از این فضا می‌باشد. بهره‌مندی اقتصادی آحاد ذیربطان مبتنی بر سایبر مد نظر می‌باشد بنابراین بالاترین وجه نقشه را وجه اقتصاد نامگذاری نموده‌ایم. ذیربطان به‌عنوان یکی از مهم‌ترین گروه‌های تأثیرگذار و تأثیرپذیر فضای سایبر کشور، نیازمند توجه ویژه‌ای هستند و باید در تحلیل عوامل محیطی، شناسایی فرصت‌ها و تهدیدها و به‌تبع آن در شناسایی مسائل مهم به‌منظور تعیین راهبردهای فضای سایبری کشور مدنظر قرار گیرند. با توجه به نقش بسیار مهمی که زیرساخت و نرم‌افزار در فضای سایبر

عده‌دار هستند، در تدوین نقشه حکمرانی بر فضای سایبر نیز از همین عنوان برای وجه فرآیندهای داخلی استفاده می‌شود. معادل وجه رشد و یادگیری، وجه فناوری و فرهنگ نام‌گذاری گردیده است تا پوشش‌دهنده تمامی موضوعات فناوری، انسانی و آموزش باشد.

#### ۴.۷ (گام چهارم) تعیین رویکرد و قالب برای زنجیره ارزش

مرکز و محور هر راهبرد عملیاتی، مرتبط ساختن فرایندهای داخلی سازمان به نتایج بهبود یافته‌ی مشتری است. در واقع ارزش پیشنهادی به مشتری داده می‌شود. ارزش پیشنهادی به مشتری و اینکه چگونه این ارزش به رشد و سودآوری برای سهامداران منجر شود، زیربنای راهبردی است. جوهره راهبرد در فعالیت‌ها نهفته است (کاپلان و نورتون، ۱۳۹۰). هنر تدوین و توسعه یک راهبرد موفقیت آمیز، حصول اطمینان نسبت به هم‌سویی بین فعالیت‌های داخلی یک سازمان و ارزش‌های پیشنهادی به مشتریان آن است. فعالیت‌های یک سازمان در فرایندهای داخلی سازمان نهفته است و زنجیره ارزش آن را تشکیل می‌دهد (رابرت اس. کاپلان و دیوید پی. نورتون، ۲۰۱۲).

با توجه به این که تمامی ذی‌نفعان فضای سایبر به دنبال بهره‌مندی از خدمات این فضا در یک فضای قابل اعتماد و امن می‌باشند، ارزش در نظر گرفته برای ذی‌نفعان در الگوی پیشنهادی نقشه حکمرانی بر فضای سایبر عبارت است از: خدمات فضای سایبر مبتنی بر امنیت پایدار.

#### ۵.۷ (گام پنجم) تعیین اهداف راهبردی وجوه و روابط علی و معلولی آن‌ها

اهداف به‌طور کلی به اهداف کلان (بلندمدت)، اهداف راهبردی (میان مدت) و اهداف عملیاتی (کوتاه مدت) تقسیم می‌شوند. اهداف کلان سازمان در قالب‌های گوناگون و با دوره‌های زمانی متفاوتی بیان می‌شوند. آن‌ها می‌توانند اهداف مالی یا اهداف غیرمالی باشند.

مضامین و نتایج راهبردی پایه و اساس تعیین اهداف راهبردی است. اهداف راهبردی چگونه ایجاد ارزش پیشنهادی به مشتری را توصیف می‌نماید. اهداف راهبردی را شاخص اصلی ۱ راهبرد می‌نامند. این اهداف نشان‌دهنده‌ی بهبود مستمر و پیوسته در سازمان بوده و اقداماتی می‌باشند که سازمان را در جهت مستندسازی، ارزیابی و اجرایی نمودن اقدامات و پروژه‌های سازمان یاری می‌رساند. درواقع اهداف راهبردی اهداف وجوه هستند (قهرمانی، ۱۳۹۱)، (Stevenson, 1995).

اهداف در چهار وجه در زنجیره‌ای از روابط علی به یکدیگر پیوسته‌اند و برای اینکه بتوانیم در جهت مدیریت بهتر بر اهدافی که در وجوه مختلف قرار می‌گیرند، بهتر است که برای هر مضمون یک مالک قرار دهیم تا این مالکان بتوانند در رابطه با پایش و تحقق اهداف و ابتکارات آن پاسخگو باشند. مدیران و ذی‌نفعان بایستی در مورد اهدافشان در چهار وجه توافق داشته باشند، انتخاب معیارها با موافقت مدیران در مورد چیزی که می‌خواهند پیاده کنند و شیوه‌ای که می‌خواهند موفقیت را توصیف نمایند، ساده‌تر می‌شود. حتی اگر معیارهای اولیه‌ی اهداف کامل نباشند، مدیران می‌توانند معیارها را در دوره‌های بعدی اصلاح کنند؛ بدون این که مجبور باشند دوباره در مورد راهبرد بحث کنند. اهداف تغییری نمی‌کنند، حتی اگر معیار اهداف با توجه به تجارب و منابع اطلاعاتی جدید دگرگون شوند (قهرمانی، ۱۳۹۱)، (کریمی قهرودی، ۱۳۸۴).

## ۸ نتیجه گیری

داشتن نگاه همه جانبه به موضوع حکمرانی بر فضای سایبر در تمامی ابعاد اعم از فناوری، زیرساخت، فرایندها، ذیربطان، سیاست و اقتصاد، لزوم داشتن یک نقشه راهبرد جامع که به تمامی مسائل این حوزه پرداخته باشد را بیشتر نمایان می کند. در این مقاله با مطالعه الگوهای رایج تدوین نقشه راهبرد، به مقایسه این الگوها با هم پرداخته شد. در جهت پاسخگویی به مسائل اصلی حکمرانی بر فضای سایبر و با بهره برداری از مقایسه الگوهای تعیین شده یک الگوی کلی برای نقشه راهبرد حکمرانی بر فضای سایبر ارائه گردید.

الگوی پیشنهادی نقشه راهبرد حکمرانی بر فضای سایبر دارای فرآیندهای گام به گام تعیین شده‌ای است که خروجی هر گام به عنوان ورودی برای مراحل بعدی مورد استفاده قرار می گیرد. تدوین نقشه راهبرد حکمرانی بر فضای سایبر، پاسخی است به چالش عدم پیاده سازی و اجرایی شدن راهبردهای حکمرانی بر فضای سایبر، که ضمن نمایش اهداف راهبردی در چارچوب روابط علی و معلولی، نشان می دهد که چگونه راهبردهای سایبری را می توان به اهداف قابل اندازه گیری و عملیاتی مشخص تبدیل کرد.

پیوستار تدوین نقشه راهبرد حکمرانی بر فضای سایبر با تدوین مطلوبیت های اساسی حکمرانی بر فضای سایبر (چشم انداز، بیانیه مأموریت) شروع شده و با تجزیه و تحلیل عوامل محیطی به مجموعه ای از راهبردها دست پیدا می کنیم. راهبردهای با اولویت بالا به عنوان مضامین راهبردی شناخته می شوند. نتایج حاصل از مضامین راهبردی به عنوان اهداف راهبردی بالاترین وجه در نظر گرفته شده و بر اساس ارزش در نظر گرفته شده برای ذیربطان، ضمن تعیین اهداف سایر وجوه، درخت اهداف مربوط به نقشه در تمام وجوه احصاء می گردد. در نهایت بر اساس قالب زنجیره ارزش و فرآیندهای داخلی تعیین شده به ترسیم نقشه راهبرد حکمرانی بر فضای سایبر پرداخته شده و سنجه های مربوط به اهداف نیز تعیین می گردند. موضوعات تحقیقی زیر می توانند تکمیل کننده مباحث ارائه شده باشند:

- روش های ارزیابی راهبردی متناسب با حکمرانی بر فضای سایبری
- الگوی مناسب برنامه ریزی راهبردی حکمرانی بر فضای سایبر
- ارائه الگوی کامل برای احصاء فرآیندهای داخلی نقشه راهبرد حکمرانی بر فضای سایبر
- طراحی سامانه های نرم افزاری مبتنی بر نقشه راهبرد حکمرانی بر فضای سایبر
- تعیین معیارهای اندازه گیری دست یابی به اهداف راهبردی حکمرانی بر فضای سایبری
- تعیین مقادیر مطلوب برای معیارها در وجوه نقشه راهبرد حکمرانی بر فضای سایبر

## مراجع

[۱] رابرت اس. کاپلان و دیوید پی. نورتون (۱۳۹۰). نقشه استراتژی تبدیل دارایی های نامشهود به پیامدهای مشهود (ویراست ۲). (ترجمه: ابوطالب گره ئی، المحرر، حسین اکبری، مسعود سلطانی، و امیر ملکی)، تهران، ایران، آریانا قلم.



- [۲] رابرت اس. کاپلان و دیوید پی. نورتون (۱۳۸۵). سازمان استراتژی محور (ترجمه: نسترن قربانی، تدوین: پرویز بختیاری)، تهران، ایران، سازمان مدیریت صنعتی.
- [۳] سازمان بسیج (۱۳۹۲). تهاجم مدرن.
- [۴] سازمان فناوری اطلاعات ایران (۱۳۹۰). کتاب مرجع سال ۹۰ افتا. تهران، مؤسسه توسعه و گسترش افتا.
- [۵] گروه مطالعات و تحقیقات راهبردی مجمع (۱۳۸۸). فناوری و قدرت ملی. تهران، داغا.
- [۶] محمد رضا قهرمانی (۱۳۹۱). دوازده گام تا تدوین و پیاده‌سازی کارت امتیازی متوازن و تعیین شاخص‌های عملکردی (ویرایش سوم)، تهران.
- [7] Alexander Klimburg (Ed.) (2012). National Cyber Security Framework Manual.
- [8] H. Stevenson (1995). Defining Corporate Strengths and Weaknesses in Readings in Strategic Management. (David Asch and Cliff Bowman, Ed.), Mac Millan.
- [9] Info-Tech Research Group (2001). Strategic IT Planning: Info-Tech's Step-by-step Consulting Methodology. London: Info-Tech Research Group.
- [10] J. Christopher Wells (2008). Defense in Depth: Strategies for Information Security.
- [11] Jan Aidemark And Håkan Sterner (2003). A Framework for Strategic Balancing of Knowledge Management Initiatives. Proceedings of the 36th Hawaii International Conference on System Sciences, 10.
- [12] Neeley (1999). The performance measurement revolution: why now and what next. International Journal of Operations & Production Management.
- [13] Luis Quezada (2007). The 19th International Conference on Production Research. University of Santiago of Chile (USACH): Pontifical Catholic University of Valparaiso (PUCV).
- [14] Robert S. Kaplan, David P. Norton (2004). Strategy Maps: Converting Intangible Assets to Tangible Outcomes. Harvard Business School Press.
- [15] Robert S. Kaplan, David P. Norton (January, 1992). The Balanced Scorecard: Measures That Drive Performance. Harvard Business Review.
- [16] Robert S. Kaplan, David P. Norton (1996). The Balanced Scorecard :Translating Strategy into Action. Harvard Business School press.



## نقد گفتمان رایج تبلیغ دینی در فضای سایبر از منظر شاخصه انتظار

زهره جمالی زواره<sup>۱</sup>، محسن خوشفر<sup>۲</sup>

<sup>۱</sup> طلبه سطح ۴ (مدرس حوزه و دانشگاه)، رشته تفسیر تطبیقی، مرکز حوزوی عالی تخصصی فاطمه الزهرا علیها

سلام، اصفهان، ایران

jamali@whc.ir

<sup>۲</sup> استادیار گروه حدیث الجامعه المصطفی

mohsenkhoshfar@yahoo.com

### چکیده

فعالیت‌هایی که در فضای سایبر در جهت نشر معارف دینی انجام می‌شود از جهات مختلف قابل بررسی است. نگاه فرامکانی بدون توجه به جزئیات، نگاهی کلان به آنچه انجام شده و می‌شود، دارد. با توجه به فراگیری استفاده از فضای سایبر و تبعات فعالیت‌های نادرست احتمالی، ضرورت و اهمیت این کار بدیهی است. بررسی کل کلام حضرت مهدی نشان می‌دهد از همان ابتدای تولد، روح حاکم بر کلام ایشان نوعی ایجاد آمادگی در پیروان، در جهت درک و باور حضور امام، بدون ارتباط مستقیم با ایشان بوده است؛ بنابراین شاخص انتظار به معنای خاص آن، همان «زمان غیبت بودن» است. نتیجه حاصل از بررسی سخنان حضرت آن است که، در حادثه واقعه فضای سایبر، پیروی همگان به ویژه علما و مبلغان دین، از رهنمودهای رهبری در نحوه مواجهه و عملکرد، جزء وظایف بلکه از الزامات و ضروریات زمان غیبت است. در این تحقیق که به روش توصیفی تحلیلی با رویکرد انتقادی و در جمع‌آوری داده‌ها از روش کتابخانه‌ای و رصد مستقیم استفاده شد؛ بر طبق تحلیل و تبیین بیانات مقام معظم رهبری به عنوان جایگاه ولایت فقیه امروز، مشخص شد؛ عدم شناخت جامع و عمل بر طبق بخشی از یک منظومه، ابزارانگاری فضای سایبر از پنج جهت، نگاه ناقص به فضای سایبر، روحیه تسلیم و عدم قاطعیت در میدان مبارزه و عدم وحدت عملکرد و نگاه کلان و بین‌المللی و القای سرگردانی به مردم مهم‌ترین نقدهای فعالیت‌های کنونی است. بر طبق بررسی‌های انجام‌شده متأسفانه فعالیت‌های تبلیغی در فضای سایبر کنونی با جهاد تبلیغ تا حد قابل توجهی فاصله دارد.

**کلمات کلیدی:** فضای سایبر، تبلیغ دین، گفتمان رایج، نقد، شاخصه انتظار.

### ۱ مقدمه

در حال حاضر اینترنت، بستر عظیمی برای تشکیل بزرگترین شبکه‌های ارتباطی جهان بین افراد گوناگون فراهم نموده است که بیش از سه میلیارد نفر از جمعیت کره زمین در بستر آن از طریق فضای سایبر، حضور

دارند. کمتر کسی است که اثر این فضای حقیقی را بر سبک زندگی اعضای آن باور نداشته باشد. همین مهم باعث شده است که فعالیت‌های قابل توجهی در قالب‌های گوناگون در این فضا به منظور ترویج معارف اسلامی، توسط ارگان‌ها و مبلغان پاک نیت و دغدغه‌مند صورت گیرد. رصد این فعالیت‌ها نشان دهنده باورهایی عمومی بین مبلغان یا به تعبیری گفتمانی رایج است که متأسفانه نتیجه چندان مطلوبی نداشته است. از این جهت و با توجه به زمان غیبت، نوشتار حاضر در تبیین نتیجه حاصل با رصد فعالیت‌های موجود در صدد است با بررسی کلام حضرت مهدی عجل الله تعالی فرجه الشریف شاخص یا شاخصه‌های انتظار و مبنای تبلیغی را تعیین نموده و سپس بر اساس تحلیل فعالیت‌ها بر این شاخص، برخی نقدهای احتمالی را تبیین نماید. براساس تحقیق انجام شده، شاخص انتظار (زمان غیبت بودن) و مبنای تبلیغ «نصح» مبلغین زاهد از طریق حرکت بر طبق راهبردهای ولایت فقیه است. بر این اساس، مهمترین نقدهای فعالیت‌های کنونی در پنج عنوان تحلیل شده است. نتایج بررسی از طریق پایگاه‌های تخصصی منابع پژوهشی، نشان دهنده آن است که بیش از ۲۴۰ مقاله که به صورت مستقیم در عنوان خود از کلید واژه «فضای مجازی» استفاده نموده اند، ثبت شده است. طبق بررسی اجمالی تمامی عناوین، اکثر این مقالات مربوط به چند سال اخیر بوده و در بین مقالات، تعداد قابل توجهی از طریق بررسی موردی و به روش میدانی انجام شده است. موضوعات متغیر و از فقهی تا تجاری متفاوت است. در بین مقالات موجود، تعدادی انگشت شمار به موضوع حاضر نزدیک است از جمله «آسیب شناسی روش های تبلیغ دین در فضای مجازی» نوشته خانم انسیه اسدی و حجت اله ایوبی و محمد سلطانی فر که در چهل و دومین شماره مجله مدیریت فرهنگی در سال ۱۳۹۷ چاپ شده است. ویژگی خاص مقاله نامبرده علاوه بر پیمایشی بودن و تمرکز بر جامعه آماری محدود ۱۷۵ نفر؛ آن است که در تدوین چارچوب نظری از نظریه عمل بوردیو و مدل دین مداری شجاعی زند استفاده شده و محاسبه طبق فرمول کوکران انجام شده است و علاوه بر عدم انطباق عنوان، از این جهت نیز با نوشتار فوق تفاوت اساسی و بنیانی دارد. بر طبق بررسی های انجام شده متأسفانه فعالیت های تبلیغی در فضای سایبر کنونی با جهاد تبلیغ تا حد قابل توجهی فاصله دارد.

## ۲ مبادی بحث

ظهور منجی آخر الزمان، اندیشه ای است جهانی که بشر را بر محور انتظار جمع می‌نماید. امت اسلامی بر اساس آموزه‌های نبی اکرم صلی الله علیه و آله مصداق منحصر منجی آخر الزمان را وجود مبارک حضرت مهدی عجل الله تعالی فرجه الشریف می‌دانند و بر خلاف سایر اندیشه‌ها که تنها به موعود بودن منجی باور دارند نه موجود بودن او، اعتقاد راسخ در موجود بودن مهدی موعود دارند (جوادی آملی، ۱۳۹۷: ۱۶۴ و ۱۶۵).

در تبیین معنای حقیقی انتظار روایات متعددی وجود دارد که در اینجا به نقل ابوبصیر از امام صادق علیه السلام بسنده می‌شود: «لِيُعِدَّنَّ أَحَدَكُمْ لِيُخْرُجَ الْقَائِمِ وَ لَوْ سَهْمًا...» (نعمانی، ج ۱، ۳۲۰: ۱۳۹۷). دقت در روایت مذکور مشخص می‌نماید منتظر واقعی لازم است خود را آماده نموده و انسان تا مرد مبارزه و جهاد نباشد، نمی‌تواند خود را در زمره منتظران حقیقی بداند. بنابراین لازمه انتظار حقیقی آن است که شخص

منتظر در عرصه عملی به اسلحه رزم و آموختن شیوه‌های نوین مجهز و در عرصه جهاد علمی به سلاح قلم و سخن مسلح باشد و بداند بخش مهمی از پیروزی آن حضرت بسته به رشد فرهنگی جامعه بشری است. این عبادات والا، عرصه‌های گوناگونی دارد که در هر یک، عنصر انتظار تجلی خاصی دارد و به شیوه متفاوت مطرح می‌شود (جوادی آملی، ۱۳۹۷: ۱۶۵-۱۶۷).

علما به ویژه عالمان علوم الهی و پاسداران حریم دین، پیشگامان صلاح و فساد امت اسلام هستند از این جهت نقش موثری در زمینه سازی ظهور بر عهده دارند. از آنجایی که بزرگ‌ترین معلم انتظار حقیقی، حضرت مهدی عجل الله تعالی فرجه الشریف است با توجه به دعای «اللهم الرزقنا توفیق الطاعة...» (کفعمی، بی تا: ص ۳۴۹) که از دعا‌های ارزشمند حضرت و بیانگر مجموعه وظایف فرد و جامعه منتظر است، ناظر به هدف این نوشتار، حضرت وظیفه گروه علما را «زهد» و «نصیحت» معرفی می‌فرمایند. بیان دو وظیفه عمده این گروه، در قسمت‌های آغازین وظایف گروه‌ها بعد از بیان وظایف شخصی منتظران و امور اجتماعی و سیاسی، نشان از اهمیت وظیفه و نقش موثر این گروه در اصلاح فرهنگ انتظار و هدایت منتظران است. بنابراین زهد به معنای عدم تعلق باطنی به دنیا و متعلقات آن و نصیحت به معنای خلوص در اندیشه و قول و فعل به گونه ای که با یکرنگی و خلوص خیر خواه امت بوده و جز به خیر و صلاح آن نیندیشند و سخن نگویند دو وظیفه عمده علما از منظر حضرت مهدی عجل الله تعالی فرجه الشریف است (جوادی آملی، ۱۳۹۷: ۲۰۰-۲۰۷). به بیانی می‌توان «زهد» را با مسامحه نسبتی فردی و نصیحت را نسبت اجتماعی برای علمای دین دانست. ماده «ن ص ح» و مشقات آن در قرآن سیزده بار استفاده شده است (عبدالباقی، ۱۳۹۱: ۸۵۲). شش مورد در سوره اعراف (ر.ک آیات ۷۹، ۹۳، ۶۲، ۶۸، ۲۱، ۷۹)، دو مورد در سوره هود (ر.ک آیه ۳۴)، دو مورد در سوره قصص (ر.ک آیات ۱۲، ۲۰) و در سوره یوسف (ر.ک آیه ۱۱)، تحریم (ر.ک آیه ۸) و توبه (ر.ک آیه ۹۱) هر کدام یک مورد. بررسی آیات مذکور نشان می‌دهد تمام آیات نامبرده مرتبط با یکی از پیامبران الهی است و در چهار مورد مستقیماً اشاره شده رسالات پروردگرم را ابلاغ کردم و سپس با عطف از یکی از مشتقات این واژه استفاده شده است. «نصح» در لغت قرآن به معنای «قصد کردن کار یا فعلی است که صلاح طرف مقابل در آن باشد» (راغب اصفهانی، ۱۳۹۲ق: ۵۱۵) از جهتی با توجه به اینکه آنچه در ادبیات رایج، تبلیغ نامیده می‌شود، از بعد مبنای ارتباطی و ارکان آن، برگرفته از نظریه «فراگرد ارتباطات» است که اولین بار در بنیاد خاندان صهیونیستی راکفلر توسط لاسول مطرح شده است (ر.ک غمامی، ۱۳۹۱: ۱۹۵-۲۵۷)؛ بنابراین با تکیه بر کلام حضرت مهدی عجل الله تعالی فرجه الشریف و ضمیمه آیات نامبرده در کاربرد این واژه و لغت، مبنای خود در تبلیغ را به جای انتقال پیام، «نصیحة» قرار داده هر چند نصیحت، منطبق بر تبلیغ نیست؛ اگر چه از آن بیگانه هم نیست.

فعالیت‌هایی که در فضای سایبر به عنوان فعالیت تبلیغی در جهت نشر معارف دینی انجام می‌شود از نگاه‌های مختلف قابل بررسی و نقد است. به عنوان مثال از جهت کلی می‌شود به این مقوله به تعبیری نگاه درون مکانی داشت و فرا مکانی. با این توضیح که در نگاه درون مکانی، به محتوای تبلیغی موجود مراجعه و ضمن دسته بندی از جهات مختلف، محتوا را از جهت انطباق با اصول تبلیغ دینی و اقتضای این محیط بررسی نمود؛ آن هم از ابعاد گوناگون و مختلف که گستردگی و پیچیدگی قابل توجهی خواهد داشت. کما اینکه گاهی با عنوان‌های مختلف از جمله تقوا در فضای مجازی به برخی ابعاد آن پرداخته شده است. در

واقع در این نگاه غرق در فضا شده و بعد از رصد و دقت در جزئیات و شناخت عدم انطباقها، برای سامان دهی محتوا تلاش می‌شود و راهکارهای پیشنهادی ارائه می‌گردد. البته این نگاه بدین معنا نیست که فعالان بدون هیچ دقتی کار را شروع نموده و سپس به دنبال بررسی هستند؛ بلکه ناظر به نگاهی محدودتر است. می‌توان ادعا کرد آنچه تا کنون به عنوان پایش فعالیت‌ها نسبت به این فضا، انجام شده اصولاً در این دسته قابل ثبت است. در نگاه فرا مکانی، کاری به جزئیات موجود، محتوا و اشکالات جزئی نداشته و سعی می‌شود نگاه از بیرون باشد. به عنوان نگاهی کلان تر بر آنچه انجام شده و می‌شود و دقتی در جهت سیاست‌گذاری کلان طولانی مدت در آینده. در واقع در این نگاه گویی از محیط فاصله گرفته و با شناختی کلی، کلیات فعالیت‌هایی که انجام شده است را بررسی نموده و با افقی بلندتر به قضیه نگاه می‌شود. رویکرد ما در این نوشتار فرا مکانی است. در نگاه فرا مکانی، ابعاد و نگرش‌های متفاوتی قابل بررسی است که با توجه به دغدغه این نوشتار، نگرش تبلیغی است. رصد فعالیت‌های تبلیغی موجود نشان می‌دهد، گفتمان رایج در بین فعالان عرصه تبلیغ در این فضا، از جهت ارکان تبلیغ در بیان رایج امروزی، نگرشی ابزاری است. یعنی فضای سایبر محیط تبلیغی فرض می‌شود؛ یا به بیانی دقیق‌تر آنچه ارتباط بین فرستنده و پذیرنده پیام را ممکن می‌سازد و زمینه انتقال پیام را فراهم می‌نماید؛ یا همان ابزار تبلیغی، با این فرض و با تکیه بر کلام نورانی حضرت مهدی عجل الله تعالی فرجه الشریف نقد و بررسی انجام خواهد شد. پیش از ورود به بحث لازم است کلیاتی از نوع فعالیت‌های در حال انجام نیز بیان شود. به طور کلی بر اساس رصد انجام شده از نظر مشارکت، فعالیت‌ها یا فردی است یا گروهی و منظور از فردی بودن، اعم از یک شخص، یک مؤسسه یا یک گروه و صنف خاص و گروهی منظور تشکیلاتی و هماهنگ بین گروه‌هایی با اهداف مشترک. از این جهت غالب فعالیت‌ها فردی است جز برخی موارد اندک مثل عملیات‌های سایبری که در جای خود بحث خواهد شد. بنابراین از جهت مشارکت، هماهنگی برنامه‌ای خاصی بین اکثر فعالیت‌ها دیده نمی‌شود و فعالیت‌ها غیر مشارکتی و به صورت شناور و توده‌ای است. از بعد جغرافیایی اکثر فعالیت‌ها در پیام‌رسان‌ها و اپلیکیشن‌های ارتباطی غیر بومی انجام می‌شود هر چند از این بعد، کمی مسامحه در نظر گرفته شده است چرا که در کل به بیانی پتانسیل ورود به فضای سایبر غیر بومی است. از نظر محتوا گستردگی قابل توجهی مانند آموزشی، اخبار، مهارتی و غیره در قالب‌های مختلف عکس، فیلم، متن، صوت و چند رسانه‌ای مشاهده می‌شود. ناگفته نماند مقصود از مبلغان اعم از عالمان دینی و مراکز و تشکلاتی است که دغدغه ترویج و نشر معارف دینی دارند. همچنین نقد فعالیت‌های حاضر به هیچ عنوان ناظر به عدم حسن نیت و عیب‌جویی بر دغدغه‌ها و فعالیت‌های خالصانه این گروه‌ها نیست. نیت نگارنده تقویت وحدت با رفع اشکالات احتمالی است.

### ۳ شاخص انتظار در کلام حضرت امام مهدی (عجل الله تعالی فرجه الشریف)

مؤسسه الامام الهادی علیه السلام قم، مجموعه کلام حضرت مهدی عجل الله تعالی فرجه الشریف را ۲۳۸ روایت نقل نموده است. شیوه تنظیم را بر اساس سیر زمان در نظر گرفته و کلام گهربار ایشان را در هشت دسته اصلی؛ دسته اول کلام ایشان در زمان حیات پدر بزرگوار ایشان، دسته دوم تا ششم به تفکیک در دوران



نائبان خاص و دسته هفتم کلام ایشان در زمان غیبت کبری و بخش هشتم ادعیه و زیارات روایت شده از ایشان تجمیع نموده است (مؤسسه الامام الهادی علیه السلام، ۱۴۳۳ق: ۱-۴۲۰). اگرچه با اندکی مسامحه آنچه مرتبط با این نوشتار است، کلام دسته هفتم است ولی بررسی کل کلام ایشان نشان می دهد از همان ابتدای تولد، روح حاکم بر کلام ایشان نوعی ایجاد آمادگی در پیروان، در جهت درک و باور حضور امام، بدون ارتباط مستقیم با ایشان بوده است. این هدف نیز به اشکال مختلف بیان شده است؛ گاهی با تقویت باور «... إِنَّ الْأَرْضَ لَا تَخْلُو مِنْ حُجَّةٍ...» (ابن بابویه، ۱۳۹۵، ج ۲: ۴۴۵)، زمانی با ارجاع به اشخاص مورد وثوق «... وَقَفْنَا عَلَى كِتَابِهِ وَ ثَقَّنَّا بِمَا هُوَ عَلَيْهِ...» (شیخ طوسی، ۱۴۲۵، ج ۱: ۳۷۲)؛ زمانی با بشارت و هشدارهای لطیف واقع بینانه «... إِنَّا غَيْرُ مُهْمَلِينَ لِمُرَاعَاتِكُمْ وَ لَا نَاسِينَ لِدِكْرِكُمْ...» (طبرسی، ۱۴۰۳ق، ج ۲: ۴۹۷)؛ گاهی با تشریح اهداف «... وَ إِنِّي أَدْعُوكُمْ إِلَى اللَّهِ وَ إِلَى رَسُولِهِ صَلَّى اللَّهُ عَلَيْهِ وَ سَلَّمَ، وَ الْعَمَلِ بِكِتَابِهِ، وَ إِمَاتَةِ الْبَاطِلِ، وَ إِخِيَاءِ سُنَّتِهِ...» (ابن طاووس، ۱۴۱۶ق، ج ۱: ۱۳۷)؛ زمانی با رد امید و ناامیدی ناشی از سخنان بی اساس و به بیان دقیق تر دعوت به صبر و استقامت «... وَ أَمَا طُهُورُ الْفَرْجِ فَإِنَّهُ إِلَى اللَّهِ عَزَّ وَ جَلَّ كَذَبَ الْوَقَاتُونَ...» (شیخ طوسی، ۱۴۲۵، ج ۱: ۲۹۰)؛ گاهی با تشریح ممکن بودن حضور نافع بدون مشاهده شدن «... وَ أَمَا وَجْهُ الْإِتِّفَاعِ بِي فِي غَيْبَتِي فَكَالْإِتِّفَاعِ بِالشَّمْسِ إِذَا غَيْبَهَا عَنِ الْأَبْصَارِ السَّحَابُ...» (طبرسی، ۱۴۰۳ق، ج ۲: ۴۶۹)؛ گاهی از طریق توجه دادن به باور حضور ایشان «... فَإِنَّا يَحِيطُ عَلِمْنَا بِأَبْنَائِكُمْ، وَ لَا يَعْزُبُ عَنَّا شَيْءٌ مِنْ أَخْبَارِكُمْ...» (فیض کاشانی و شاه مرتضی، ۱۳۷۲، ج ۱: ۲۴۱)؛ و گاهی هم با راهنمایی مسیر «... وَ أَمَا الْحَوَادِثُ الْوَأَقَعَةُ فَارْجِعُوا فِيهَا إِلَى رِوَاةٍ حَدِيثِنَا فَإِنَّهُمْ حُجَّتِي عَلَيْكُمْ وَ أَنَا حُجَّةُ اللَّهِ عَلَيْهِمْ...» (ابن بابویه، ۱۳۹۵، ج ۲: ۴۸۳). بنابراین مهم ترین شاخص انتظاری که می توان از کلام ایشان استخراج نمود همان اصطلاح «غیبت» در متون دینی است. پس شاخص انتظار البته به معنای خاص آن، همان «زمان غیبت» بودن آن است که آیت الله جوادی آملی آن را اینگونه توصیف می نمایند که؛ مردم از محضر مبارک امام زمان (عجل الله تعالی فرجه الشریف) غایب اند و ایشان ولی حق و شاهد بر خلق است و مومن منتظر لازم است وظیفه خود را در زمان غیبت بشناسد و بررسی کند آیا به وظیفه خود عمل نموده است یا خیر (جوادی آملی، ۱۳۹۷: ۱۲۷ و ۱۲۸) در همین راستا و اطمینان از انجام وظیفه، با رجوع به کلام حضرت مهدی (عجل الله تعالی فرجه الشریف)، کلیدی ترین کلامی که توجه هر منصفی را به سمت خود جلب می نماید آنجایی است که حضرت در پاسخ مشکلات اسحاق بن یعقوب با واسطه محمد بن عثمان العمری در نکته ششم فرمودند: «... وَ أَمَا الْحَوَادِثُ الْوَأَقَعَةُ فَارْجِعُوا فِيهَا إِلَى رِوَاةٍ حَدِيثِنَا فَإِنَّهُمْ حُجَّتِي عَلَيْكُمْ وَ أَنَا حُجَّةُ اللَّهِ عَلَيْهِمْ...» (ابن بابویه، ۱۳۹۵، ج ۲: ۴۸۳). کمره ای این قسمت از کلام حضرت را این گونه ترجمه نموده است: «اما در حکم پیشآمدهای تازه برآیایان حدیث ما رجوع کنید زیرا آن ها حجت بر شمایند و من حجت بر آنهایم». اگر چه برخی قائل به دلالت این سخن بر مسائل فقهی جدید هستند ولی علمای زیادی از جمله امام خمینی (ره) با بحثی استدلالی صراحت دارند که در دلالت این روایت بر ولی فقیه تردیدی نیست (امام خمینی (ره)، ۱۳۶۹، ج ۱: ۴۵-۴۸)، همچنین یعقوبی در جلسه چهاردهم درس خارج فقه خود در مشهد در سال ۱۳۹۵، به صورت مفصل دلالت روایت به همراه پاسخ اشکالات و جبران ضعف سندی روایت را بحث نموده اند که از طریق سایت وسائل، پایگاه تخصصی فقه حکومتی در دسترس عموم است. آیت الله معرفت در مقاله «ولایت

فقیه از دیدگاه شیخ انصاری و آیت‌الله خویی» در بین نقل دلائل از هر دو عالم، بر روایت مذکور اشاره نموده و آن را از جمله دلایل دلالت بر ولایت فقیه و شؤونات او مطرح نموده اند و در نهایت اذعان داشته اند، مقصود از ولایت فقیه در عصر غیبت، همین عهدهداری و مسؤولیت در راستای مصلحت های مردمی است و این خود، انجام وظیفه و خدمتی است که شارع مقدس مسؤولیت آن را بر عهده فقیه جامع شرایط قرار داده است (معرفت، ۱۳۷۸: ۲۴۶-۲۶۴). بنابراین دلالت روایت بر رجوع به ولایت فقیه در عصر غیبت در حوادث واقعه مسأله‌ای اثبات شده است و بر علما و دغدغه‌مندان لازم است این اصل را در انجام وظیفه خود رعایت نمایند. ممکن است برای برخی، سؤالات و شبهاتی در این زمینه مطرح باشد که آیت‌الله مصباح به‌طور مفصل و با بیانی روان و قابل فهم عموم، این مسائل را در کتاب «پرسش و پاسخ‌های دانشجویی» جلد دوم مباحث ولایت فقیه (مصباح یزدی، ۱۳۹۱، ج ۲: ۸۷-۱۱۶) و همچنین کتاب «نگاهی گذرا به نظریه ولایت فقیه» (مصباح یزدی، ۱۳۹۶: ۱-۱۵۹) پاسخ داده‌اند. در اینکه «فضای سایبر» از وقایع دهه‌های اخیر است هم شکی وجود ندارد، بنابراین از آنچه گفته شد، می‌توان نتیجه گرفت که در حادثه واقعه فضای سایبر، در زمان غیبت، طبق کلام حضرت مهدی (عج) پیروی همگان به‌ویژه علما و مبلغان دین، از رهنمودهای رهبری در نحوه مواجهه و عملکرد، جزء وظایف بلکه از الزامات و ضروریات زمان حاضر است، به‌ویژه با توجه به موقعیت خاص سیاسی دینی کشور ایران.

## ۴ نقد فعالیت‌های تبلیغی فضای سایبر بر طبق منظومه فکری ولایت فقیه

بررسی بیانات مقام معظم رهبری به عنوان جایگاه ولایت فقیه امروز، نشان می‌دهد، فضای سایبر و مسائل آن نزد ایشان اهمیت خاصی داشته و در بسیاری از مواضع و زمان‌های ویژه به این مسئله پرداخته و راهنمایی‌های راهبردی دقیقی در این زمینه داشته‌اند که متأسفانه بسیاری از این فرمان‌ها بر زمین مانده و یا توجهی به اصل آن نشده است. تعداد فیش‌های این موضوع در کلام ایشان فراوان است و ترتیب زمانی آن نشان از آن دارد که از بدو ورود اینترنت به ایران، یکی از دغدغه‌های ایشان بوده و هست. نقدها نسبت به تطبیق فعالیت‌های تبلیغی جاری با منظومه فکری ایشان بسیار است ولی در اینجا به برخی از آنها اشاره می‌شود.

### ۱.۴ عدم شناخت جامع و عمل بر طبق بخشی از یک منظومه

منظومه فکری مقام معظم رهبری در این موضوع هم از ویژگی‌های منظومه فکری ایشان در سایر موضوعات مستثنا نبوده و همه آنها در مجموع راهگشاست. اگرچه یک فرد یا یک مجموعه نمی‌تواند بر تمام این اوامر جامه عمل بپوشاند اما این مسئله تنافی با ضرورت آگاهی از اصول و کلیات این منظومه ندارد. بارها مشاهده شده برخی افراد و سازمان‌ها بر اساس یک جمله از کلام ایشان راهی را شروع می‌نمایند در صورتی که اگر این جمله در مجموع سخنان ایشان دیده شود و مورد بررسی قرار گیرد این نوع عملکرد کاملاً متضاد با آن شیوه است. متأسفانه به دلیل رعایت اخلاق، امکان نام بردن از برخی مجموعه‌ها و نوع فعالیت و ملاک آنها نیست ولی مصداق‌های این مورد فراوان است. به تعبیری، بسیاری از فعالیت‌ها از بخش‌هایی از کلام رهبری

در جهت تأیید فعالیت خود استفاده نموده اند نه اینکه کلام بررسی و بر طبق کل این نظام فکری بخشی از کار را دست گرفته و تلاش کنند برای عملی شدن آن. به عنوان مثالی کلی، تکیه و استدلال خیلی از مبلغان نسبت به حضور در فضای غیر بومی، استفاده از فرصت های این فضا که در کلام رهبری به آن اشاره شده است مطرح می شود (بیانات، ۱۳۹۱: علما و روحانیون خراسان شمالی)؛ در صورتی که نسبت به این کلام که «در میدان تنظیم شده ای از سوی دشمن بازی نکنید... چون چه ببرید، چه ببازید، به نفع اوست» (بیانات، ۱۳۸۷: دیدار با دانش آموزان و دانشجویان) سنجیده نشده است. منظور از این مثال تأیید و عدم تأیید حضور در این فضا نیست، منظور قابل تامل بودن حرکت های معکوس است. اینکه فعالیتی قصد شود و برای تأیید آن کلامی از ایشان علم شود بدون توجه به کلیات، همچنان که روشی نادرست است می تواند تبعات زیادی داشته باشد که شکست یا مغایرت هایی که با اصول اسلامی پیدا خواهد کرد، به اعتبار آن جایگاه ضربه خواهد زد. چیزی شبیه آنچه در مسئله بورس اتفاق افتاد. بنابراین برای کسی که به عنوان مبلغ دینی در این مسیر قدم می گذارد لازم است حداقل مجموع سخنان ایشان در مورد موضوع فضای سایبر را مطالعه و در مواردی که مربوط به سایر موضوعات می شود، مراجعاتی به این موضوعات هم داشته باشد. این می طلبد مجموعه هایی این تبیین را انجام و حاصل کار را در قالب مجموعه هایی مکتوب و کارگاهی در اختیار این قشر دغدغه مند قرار داده و حرکت آنها را هدایت کنند که متأسفانه کارهای جدی در این زمینه انجام نشده است. البته کتاب منظومه فکری ایشان در مورد فضای سایبر توسط مجموعه ای در حال تدوین است.

## ۲.۴ ابزار بودن فضای سایبر

در مبادی بحث بیان شد که گفتمان رایج بین مبلغان در فضای سایبر و البته عموم جامعه ابزار بودن این فضا است. نقد این گفتمان حداقل در چند جهت قابل دقت است. با فرض اینکه این فضا ابزار باشد چند سؤال در برابر مدعیان آن مطرح است.

منظور از ابزار بودن چیست؟ آیا این ابزارانگاری ساده معادل فرهنگ قرآنی و وظیفه زمان غیبت است؟ مقام معظم رهبری در بخشی از بیانات خود در تبیین عبارت «وَمِنْ رِبَاطِ الْحَيْلِ» (انفال، ۶۳) این عبارت را معادل ابزار می داند و در ویژگی های ابزار مناسب قدرت و اقتدار نظام بیان می نمایند؛ «ابزار باید پیشرفته باشد؛ باید ناوابسته باشد؛ ابزار باید مال خود شما باشد؛ خود شما باید ابزار را به وجود آورده باشید، تولید کرده باشید، ابداع کرده باشید؛ به معنای حقیقی کلمه مالک ابزار باید باشید. ابزار باید به روز باشد. باید دید امروز به چه ابزاری نیاز است، ابزار باید متنوع باشد»؛ سپس به وضوح اشاره می فرمایند، مسئله ای فضای مجازی، امروز جزو ابزارها است (بیانات، ۱۳۹۸: دیدار با دانشجویان دانشگاه امام حسین (علیه السلام)). هدف ما از بیان این مطلب آن نیست که باید و نباید استفاده را مشخص نماییم بلکه به این منظور است که به عنوان مبلغ دینی از خود سؤال کنیم فعالیت های ما در فضای مجازی تا چه اندازه به این سمت و سو و روشننگری و تبیین نسبت به ایجاد چنین مطالباتی در مخاطب است؟

فرض دوم مبنی بر ابزار رسانه ای دانستن فضای سایبر است. کمتر کسی است که به رسانه بودن فضای سایبر اذعان نداشته باشد حداقل در عرف جامعه علمی امروز، چنین نگاهی از بدیهیات شمرده می شود. اما از این بُعد هم متأسفانه فعالیت مبلغان با واقعیت موجود هماهنگی لازم را ندارد. مقام معظم رهبری در

سخنان خود اشاره دارند که فهم درست از واقعیت‌های کشور و جهان، دشمن را به تلاطم می‌اندازد و با آن مبارزه می‌نماید و ابزار آن را ابزار رسانه معرفی می‌نمایند. ایشان به صراحت بیان می‌کنند «ابزار بسیار خطرناک رسانه، بخصوص رسانه‌هایی که امروز نوپدید است» (بیانات، ۱۳۹۷: دیدار ده هزار نفری بسیجیان). ایشان در بخش دیگری از سخنان خود بیان می‌دارند دشمن از ابزار رسانه استفاده می‌کند برای اثرگذاری بر افکار عمومی. ابزار رسانه، ابزار مهمی است و اگر دست دشمن باشد، ابزار خطرناکی است. ابزار رسانه را تشبیه می‌کنند به سلاح‌های شیمیایی در جنگ نظامی؛ ویژگی سلاح شیمیایی را این‌گونه مطرح می‌نمایند که سلاح شیمیایی تانک و تجهیزات را از بین نمی‌برد؛ تجهیزات می‌ماند و انسان‌ها از بین می‌روند و از قدرت استفاده‌ی از ابزار می‌افتند و تصریح می‌فرمایند؛ ابزار رسانه هم این‌جور است. امروز از تلویزیون، از رادیو، از اینترنت، از شبکه‌های اجتماعی، از انواع و اقسام وسایل فضای مجازی، علیه افکار عمومی ما استفاده می‌شود (بیانات، ۱۳۹۷: دیدار ده هزار نفری بسیجیان). بنابراین جا دارد از خود سؤال کنیم که نگاه ابزاری ما به رسانه وابسته‌ای مثل فضای سایبر این‌گونه است؟

فرض سوم مبنی بر نظریات مطرح در فناوری یا همان تکنولوژی است. شاید بتوان ابزارانگاری فعلی را ناشی از تفکر پیشرفت علم و تکنولوژی و نادرست بودن همراه نشدن و مبارزه با آن دانست همان‌طور که کم نیستند افرادی که تلقی آنها در مورد رسانه‌های نوپدید از جمله فضای سایبر این‌گونه است. در مورد فلسفه فناوری (ر.ک خسروی، پوشنه و کیانی بختیاری، ۱۳۹۰: ۷۰-۷۵) که به نوعی روش استفاده و بهره‌مندی از آن را تحت تاثیر قرار می‌دهد، نظریه‌هایی وجود دارد که مهم‌ترین آنها عبارت است از؛ ابزارانگاری، جبرانگاری، ذات‌انگاری و ارزش یا اراده‌انگاری. طبق نظریه ابزارانگاری تکنولوژی صرفاً ابزاری در دست انسان است که نه ارزش بار است و نه توان تغییر اجتماعی دارد و این انسان است که تکنولوژی را برای رسیدن به هدف خود به کار می‌گیرد و ابزار از خود هویتی ندارد. در نظریه جبرباوری ساخت و تحول تکنولوژی بر اساس منطقی درونی شکل می‌گیرد که تحولی است خارج از کنترل انسان با این بیان که تکنولوژی‌های گذشته تکنولوژی‌های آینده را تعیین می‌کنند و انسان نمی‌تواند مانع تحول تکنولوژی، ساخت تکنولوژی یا حتی تغییر آن شود. در اراده‌انگاری انسان به شکل مختار تکنولوژی را می‌سازد، هر چند اراده انسان محدودیت‌هایی دارد ولی در چارچوب محدودیت‌های تکنیکی و فیزیکی این انسان است که تعیین می‌کند که یک ابزار چه طرح و کارکردی داشته باشد. ذات‌باوری مقابل نظریه ابزارگرایی است. تکنولوژی ماهیت و ذات خاص دارد که توان تغییر معادلات اجتماعی، فرهنگی و سیاسی را دارد. جدای از اهمیت هر نظریه و پیروان کثیر آنها مهم ترکیب این نظریات است (شریف زاده و مقدم حیدری، ۱۳۹۴: ۲۹-۵۱). پایه‌گذار تمام این نظریات غربی‌ها هستند و در حال حاضر بین نخبگان فرهنگی اسلامی که با این نظریات آشنایی دارند اختلاف نظر وجود داشته و نظرات ترکیبی هم طرفداران قابل توجهی دارد. ما در اینجا دنبال مشخص نمودن موضع صحیح نبوده و ضمن اینکه ادعا می‌شود اکثر مبلغان این فضا با این نظریات آشنایی نداشته و بدون آگاهی و شناخت و تحقیق پیرو برخی از آنها هستند، با یک جمله، عمل بر طبق هر کدام از این نظریات را پاسخ می‌دهیم و آن اینکه، آیا فضای سایبری فعلی ما تکنولوژی است و یا ثمره‌ای از تکنولوژی که در دانش و نشر و ... وابستگی صد در صدی به دشمن دارد؟ بنابراین در موضع استفاده از ثمره دانش دیگران به شکل وابسته و طبق قوانین آنها لازم است در این جایگاه تعیین موضع نمود.

فرض چهارم آنکه ابزار بودن فضای سایبر را ناشی از نگاه، مساوی بودن رسانه با ابزار دانست. که این فرض هم اشکال آن از سه مورد قبل کمتر نیست. اینکه رسانه را معادل ابزار بدانیم خیالی خام و ناشی از عدم آگاهی است. کارشناسان رسانه برای هر رسانه چه مدرن و چه قدیمی هفت رکن قائل هستند که عبارت است از؛ حاکمیت، زیرساخت سخت افزاری، زیرساخت نرم افزاری، خدمات، محتوا، ابزار و کاربر که همه ارکان تحت اشراف حاکمیت است. به عنوان مثال در یک نشریه ساده، عده ای تصمیم بر این کار گرفته، سیاست های کلان خود را تبیین نموده، برای اجرایی شدن آن مدیرانی تعیین و این سیاست ها تبدیل به قانون هایی می شود که همان لایه حاکمیت است، برای اجرایی شدن قطعاً سخت افزارهایی نیاز است و نرم افزارهایی که روح این سخت افزارهاست مثل خود چاپگر و آن برنامه ای که آن را به کار می اندازد، خدمات همان ستون ها و عناوین و محتوا آنچه ذیل آن درج می شود و ابزار همان کاغذ و کاربر انسانی که نشریه به دست او می رسد، آیا می توان فضای سایبر را از چنین سیر منطقی، در حد یک ابزار کاهش داد؟ (ر.ک کهوند، ۱۳۹۷: ۲۷-۱۱۳). نه تنها این ارکان برای فضای سایبر قطعی است، بلکه بر طبق تحقیقات، عمده سرمایه گذاری مالی و محتوایی توسط ۷ شرکت چندملیتی یهودی انجام می شود اگرچه تعداد تا ۵۵ شرکت است. در کلام مقام معظم رهبری این گروه با «زرسالاران اقتدارطلب» تعبیر شده است «... این اشغالگر کیست؟ پاسخ این نیست که این اشغالگر دولت امریکا یا فلان دولت دیگر است؛ نه، این اشغالگر یک طبقه ای اجتماعی است؛ طبقه ای که دولت امریکا و دولت های دیگر را به قدر توانایی و قدرت خود و آمادگی آنها دارد هدایت می کند. البته در بافت و ساخت این دولت ها هم بدون شک افراد این طبقه حضور دارند؛ اما هدایت، هدایت یک دولت نیست؛ هدایت یک مجموعه ای طبقاتی است، که اگر بخواهیم در یک عبارت برای اینها اسم معین کنیم، باید بگوییم «زرسالاران اقتدارطلب». هدفشان هم سیطره بر منابع حیاتی و مالی همه ی دنیاست. البته این سیطره، یک الزامات سیاسی دارد که همان نظم نوین جهانی است؛ یک الزامات علمی و اداری دارد که بتدریج خود را به آن نزدیک می کنند. مسأله ی جهانی سازی که امروز در تجارت، پول، فرهنگ و شبکه های فرهنگی - مثل اینترنت و مانند آن - مطرح است، همه دانسته و نادانسته در خدمت این مجموعه ای طبقاتی است» (بیانات، ۱۳۸۳: دیدار مسئولین صدا و سیما)

فرض پنجم نگاه از نوع مدیریت ابزار است. از اشخاصی که به عنوان مثال شبکه اجتماعی یا پیام رسان را ابزار می پندارند باید سؤال نمود، این ابزار به نسبت مدیریت ابزار و کاربر از چه نوع ابزارهایی است؟ آیا همانند چاقو است که مدیر و کاربر یک نفرند؟ آیا بسان خلبان هواپیما مدیریت با برج خلبان است ولی خلبان همچنان استقلال خود را دارد و یا همچون ماشین آموزش رانندگی، کاربر تنها توهم مدیریت دارد؟ اگر این گونه است چرا در کوچک ترین مسئله فضای مجازی اجازه نشر یک عکس از سردار مقاومت داده نمی شود؟ چرا کاربری فعالان ضد صهیونی حذف می شود؟ چطور فیلم های منا یک شبه از تاریخ برخی نرم افزارها حذف شد؟ نامه های رهبر به جوانان اروپا کجا رفت؟ در مقابل؛ چه طور آموزش نحوه حمل اسلحه سرد به یک نوجوان افغانستانی به نحو احسن انجام می شود؟ قمار و قاچاق انسان و صفحات پورنو آزاد است؟ بنابراین مدیریت کاربر بر این ابزار توهمی بیش نیست و کاری که این به ظاهر ابزارها انجام می دهند تنظیم رفتار مخاطب طبق قمرزهای مالکان است نه پهنه ای برای نشر مصلحت.

گذشته از اینکه فضای سایبر محیط اجرایی شدن حاکمیت از طریق سایبرنتیک یعنی کنترل پدیده از



طریق جریان اطلاعات است نه ابزاری خنثی و فی سبیل الله با نیت خیرخواهانه و کمک به مبلغان، فرض‌های دیگری هم برای نقد این نوع نگاه وجود دارد که به همین میزان بسنده می‌شود. از آنچه بیان شد می‌توان نتیجه گرفت متأسفانه نگاه ابزاری برخی از ما مبلغان در حد نگاه به اسباب‌بازی کودکان، غیرجدی و عامیانه است؛ و در فاصله گرفتن خط تبلیغی از ولایت فقیه همین کافی است که: «این ابزارهای جدیدی که وارد میدان شده است، اینها همه ابزارهایی هستند برای تسلط بر فرهنگ یک کشور. بنده با این حرف نمی‌خواهم بگویم این ابزارها را از زندگی خودمان خارج کنیم؛ نه، اینها ابزارهایی هستند که می‌توانند مفید واقع بشوند اما سلطه‌ی دشمن را از این ابزارها بایستی سلب کرد. نمی‌توانید شما برای اینکه مثلاً فرض بفرمایید رادیو و تلویزیون داشته باشید، رادیو تلویزیونتان را بدهید در اختیار دشمن؛ اینترنت هم همین‌جور است، فضای مجازی هم همین‌جور است» (بیانات، ۱۳۹۵: دیدار مردمی مراسم رحلت امام خمینی (ره)).

### ۳.۴ نگاه ناقص به فضای مجازی

همان‌طور که قبلاً بیان شد و شواهد هم بر این مهم دلالت دارد، اکثر فعالیت‌های تبلیغی به روش ایجاد کانال، گروه، صفحه و غالباً در نرم‌افزارهای غیربومی انجام می‌شود. در مواردی هم به شکل سایت و وبلاگ صورت می‌گیرد که غالب آن به صورت انتشار محتوا است. یعنی گفتمان رایج از لحاظ شیوه عمل آن است که مخاطب فضای مجازی در این مکان‌ها حضور حداکثری داشته و باید از این فرصت استفاده نمود؛ یا نهایت در حد تولید اپلیکیشن‌هایی با محتوای مد نظر و قابل اجرا بر زیرساخت‌های غیر بومی؛ یا به ندرت عملیات‌هایی که بازنشر حداکثری کاربران شرکت‌کننده، بدون در نظر گرفتن فیلترینگ حسابی و اینکه هش‌تگ ترند شده به چه محتوایی توسط مدیران لینک خواهد شد و آدرس تک تک سربازان گمنام و غیررسمی را روشن می‌کند، در صدد ترند کردن، هش‌تگ‌های خاصی در پیام‌رسان‌های هدف است. نقد ما در این شیوه، بر درستی و نادرستی نوع فعالیت نیست بلکه تجدید نظری در مورد تعریف فضای سایبر است. آنچه فعالیت‌های تبلیغی کنونی بر آن متمرکز شده است، بخش ناچیزی از فضای سایبر است. خدمات فضای سایبر و به‌طور کلی بستر دیجیتال در دو دسته خدمات پایه و خدمات کاربردی قابل تفکیک است. خدمات پایه شامل جویشرگر، نرم‌افزارهای ارتباطی، خدمات دسترسی به اینترنت، خدمات پایه مکانی و نقشه و ای پی ای‌ها است. خدمات کاربردی هم بسیار متنوع از آموزش و تجارت الکترونیکی تا سیر و سفر و دولت الکترونیکی و ... بنابراین نرم‌افزارهای ارتباطی بخش کوچکی از این فضا هستند که خود آنها به رایانامه، بازی‌های برخط، پیام‌رسانی و ارتباطات و انجمن و تالار گفتگو قابل تفکیک است. در حال حاضر اولین سایت پربازدید ایران یک جویشرگر است. طبق اعلام رسمی بنیاد بازی‌های رایانه‌ای، بر اساس پیمایش ملی و به روش تلفنی در سال ۱۳۹۸ که البته نتیجه آن در سال ۱۴۰۰ منتشر شده است، ایران بیش از ۳۲ میلیون بازیکن بازی دیجیتال دارد که به طور متوسط در روز بیش از ۹۰ دقیقه بازی می‌کنند و طبق الگوی استخراجی بازیکنان تهرانی که حدود ۴ میلیون نفر در گروه سنی سه تا پنجاه و پنج سال است و ۳۴ درصد این افراد را خانم‌ها تشکیل می‌دهند، ۶۸ درصد این حجم از بازی، بازی آنلاین است (ر.ک <https://direc.ircg.ir>: آمارهای تحلیلی) و البته باید به این آمار حدود سه سال شرایط کرونایی و مجازی شدن‌های افراطی‌تر از قبل و وضعیت گیم‌استریمرها را هم اضافه نمود. در حال حاضر ایران بیش از ۴۰ گیگ‌استریمر فعال دارد و از بخش گیم آپارات هم امکان دسترسی و مشاهده



وجود دارد. (https://www.aparat.com/game/livelist) اگرچه سایت تبیان، سایت معتبری از جهت آمار نیست ولی این سایت در مقاله‌ای، آماری ارائه نموده است که با تمام خطاهای احتمالی برای مبلغانی که این قسمت را رها نموده و به انتشار روایت و مطلبی در کانال‌ها بسنده می‌نمایند، قابل تأمل است. طبق این آمار، در سه ماهه سوم سال ۲۰۱۹، محبوب‌ترین پلتفرم‌های پخش آنلاین بازی روی هم رفته ۳۲.۳ میلیارد ساعت تماشا، بیش از ۱۳۱ میلیون ساعت زنده، با میانگین نزدیک به ۶.۱ میلیون بیننده همزمان تولید کردند!!! (تبیان، ۱۴۰۰: تاثیر استریم بر دنیای گیمرها). وضعیت فرهنگی و اثرگذاری گیم استریم‌ها حتی در ایران از سلبریتی‌های سینما بسی بیشتر است. تقریباً صد درصد بازی‌های رایج، غیرایرانی و با مؤلفه‌های ضدفرهنگی است. بازی به دلیل تعاملی بودن و اینکه شخص بازیکن مستقیم، نقش بازی می‌کند مؤثرترین رسانه شناخته می‌شود. تجربه قتل، خشونت، دزدی، مواجهه با صحنه‌های مستهجن، مؤلفه‌های جن و جادو و ... تجربه‌ای است که برخی کودکان و نوجوانان روزانه ساعت‌ها از عمر خود را هزینه کسب آن می‌نمایند. بنابراین لازم است صرف نظر از سایر قسمت‌های فضای سایبر، از خود سؤال کنیم چقدر راهکارهای سلبی و ایجابی در مورد بازی‌ها به کار گرفته شد؟ چقدر به این مقوله توجه و بر اساس پژوهش و برنامه‌ریزی کارشناسانه، راهکارها تبیین و اجرایی شد؟ مجدد تأکید می‌شود رویکرد این مقاله در جهت راهکار و درست و غلط بودن‌ها و تأیید و رد نیست ولی اینکه تمام سرمایه‌های انسانی و مالی تبلیغی در فضای سایبر در بخش ناچیزی از آن هزینه شود، به نظر روش مدبرانه‌ای نمی‌باشد. به توضیح این قسمت با بیان بخشی از سخنان مقام معظم رهبری اکتفا می‌شود: «برادران عزیز، خواهران عزیز! در مسئله‌ی فرهنگ، بنده احساس یک ولنگاری می‌کنم؛ در دستگاه‌های فرهنگی، اعم از دستگاه‌های دولتی و غیر دولتی، یک نوع ولنگاری و بی‌اهتمامی در امر فرهنگ وجود دارد؛ چه در تولید کالای فرهنگی مفید که کوتاهی می‌کنیم، چه در جلوگیری از تولید کالای فرهنگی مضر که کوتاهی می‌کنیم. اهمیت کالای فرهنگی از کالای مصرفی جسمانی کمتر نیست، بیشتر است. فرض کنید مرتب تکرار بکنند که مثلاً فلان جور پفک مضر است، نخورید؛ حالا مگر ضررش چقدر است، چه جور ضرری است، چه میزان ضرر دارد، برای چند درصد از مردم ضرر دارد؟ این را دائماً می‌گویند، اما ضرر فلان جور فیلم یا فلان جور کتاب یا فلان جور بازی رایانه‌ای یا امثال اینها را کسی جرئت نمی‌کند بگوید که نبادا متهم بشوند به اینکه جلوی آزادی اطلاعات و جریان آزاد اطلاعات را گرفته‌اند. آنهایی که اساس این حرف‌ها هستند، خودشان بیشتر از ما در این مسائل سخت‌گیری می‌کنند؛ این را باور کنید» (بیانات، ۱۳۹۵: دیدار رئیس و نمایندگان مجلس شورای اسلامی). ناگفته نماند راهکار ولایت فقیه در این سخن برای فرهنگ، فرهنگ‌سازی نیست بلکه روشنگری در جهت تولید کالای فرهنگی و جلوگیری از تولید کالای مضر است. «امروز تهدیدهای فضای مجازی وجود دارد که ده سال پیش به این صورت وجود نداشت و ممکن است چند سال بعد تهدیدهای دیگری از همین قبیل به وجود بیاید؛ افراد با فکر ما بنشینند و با استفاده‌ی از خرد جمعی و پژوهش‌های دانشگاه‌های ما اینها را پیش‌بینی کنند» (بیانات، ۱۳۹۹: سی‌ویکمین سالگرد رحلت امام خمینی (رحمه‌الله))

#### ۴.۴ روحیه تسلیم و عدم قاطعیت در میدان مبارزه

طبق رصد و بررسی فعالیت‌های تبلیغی مبلغان در فضای سایبر، می‌توان ادعا کرد، به نظر روح حاکم بر شیوه تبلیغ و حضور اکثریت مبلغان در فضای سایبر، هم سویی بسیاری از مسئولین، پذیرش شرایط موجود و عدم

توان در تغییر شرایط و محال و ناممکن بودن بومی سازی تمام ارکان رسانه در کشور اسلامی ایران است. به بیانی جدید و نوع عمل ناظر به حضور در میدان مبارزه بودن، نیست.

«همان طور که عرض کردم از لحاظ فضای مجازی آرایش جنگی گرفته؛ در مقابل این دشمنی که آرایش جنگی در مقابل ملت ایران گرفته، ملت ایران بایستی آرایش مناسب بگیرد، باید خودش را آماده کند در همه ی بخشهای مختلف» (بیانات، ۱۳۹۸: دیدار مربیان و فرهنگیان).

«یکی از اصول این باشد که نگاه به جریان رسانه ای دشمن - چه جریان رادیو تلویزیونی اش، چه جریان ماهواره ای اش، چه جریان فضای مجازی اش - نگاه سوءظن آمیز باشد» (بیانات، ۱۳۹۵: دیدار با دانشجویان). البته تأکید بر ایران با اینکه فضای سایبر مسئله ای جهانی است، تنها از جهت ملی نیست بلکه از این جهت است که انقلاب اسلامی ایران، پایه گذار مقاومت و انقلاب و تفکری توحیدی خارج از مرزهاست و به دنبال زمینه سازی برای ایجاد تمدن نوین اسلامی است. انتقال حجم قابل توجهی از تبلیغات به فضای سایبر، انتقال بخش های حساس امنیتی کشور مانند دیتابیس پزشکی و حقوقی و ... در فضای سایبر، رمزارزها، متاورس، کسب و کارهای سایبری، اثرات مختلف بر سبک زندگی افراد، عکس العمل های هیجانی و عامی نسبت به برخی اقدامات قانون مندسازی مثل طرح صیانت، فیلتراسیون ها و مهم تر از همه مطالبه مهم ترین اقدام از نظر ولایت فقیه «شبکه ملی اطلاعات» و بسیاری موارد دیگر شواهدی است بر این ادعا از آن جهت که عکس العمل خاصی از سوی دغدغه مندان فرهنگی دیده نمی شود. البته این به معنای این نیست که فعالیت هایی مشابه آنچه دیگران انجام دادند صورت نگرفته است، ولی وظیفه طلبگی و فرهنگی اقتضا دارد که پدیده ها و مسائل را بر اساس جهان بینی توحیدی سنجیده و با پشتوانه ای پژوهشی و محکم، موضعی قاطعانه و روشن داشت، آن هم نه در فضای بی در و پیکر مجازی بلکه در فضای حقیقی.

«از جنگ سخت که احتیاج دارد به هیئت اندیشه ورز برای ترسیم و تعیین حدود این کار که چه کسی برود، کی برود، چه جوری برود؛ تا جنگ نرم که جنگ نرم یک عرصه ی بسیار وسیعی است و روز به روز هم با گسترش این فضای مجازی دارد گسترده تر میشود و خیلی هم خطرناک تر از جنگ سخت است - یعنی در جنگ سخت، جسمها به خاک و خون کشیده میشوند، [ولی] روحها پرواز میکنند و میروند به بهشت؛ [اما] در جنگ نرم، اگر خدای نکرده دشمن غلبه بکند، جسمها پرواز میشوند و سالم میمانند، [ولی] روحها میروند به قعر جهنم؛ فرقی این است؛ لذا این خیلی خطرناک تر است» (بیانات، ۱۳۹۵: دیدار بسیجیان)

«هدف اصلی ما سازندگی مردم به شکلی است که اسلام و انقلاب میخواهند؛ به طور خلاصه و کوتاه، هدف این است ... من با آن کسی که با تفکر اسلامی میانه ای ندارد، هیچ رودربایستی ندارم. شماها را نمی گویم؛ شما بچه مسلمان های خودمان هستید و دارید مثل من تلاش می کنید؛ لیکن آن مخاطبی که فرضاً باور اسلامی در قلب او نیست و او این را نمی خواهد و این نوع عمل ما و تصرف ما و فعالیت ما را دوست نمی دارد، ما با او هیچ رودربایستی نداریم؛ نمی پسندد، نپسندد؛ خوشحال نمی شود، نشود؛ تلویزیون را می بندد، در نهایت ببندد. البته باید تلاش بکنیم که تلویزیون را نبندد و گوش کند و ببیند؛ اما اگر فرض کردیم کار به آنجا رسید که یا ما باید هدف خودمان را دنبال نکنیم، تا او تلویزیون را نبندد؛ و یا این که هدف خودمان را دنبال کنیم، که طبیعتاً او تلویزیون را خواهد بست؛ در اینجا ما دومی را ترجیح می دهیم؛ او تلویزیون را ببندد؛ زیرا بسیارند کسانی که تلویزیون را نمی بندند و همین را که من می گویم، می خواهند» (بیانات، ۱۳۷۰: مدیران شبکه دو

سیما).

«یکی دیگر از چیزهایی که در مدیریت کشور - که بتوانید کشور را اداره کنید - تأثیر دارد، مسئله‌ی فضای مجازی است؛ فضای مجازی خیلی مهم است؛ در مسئله‌ی فضای مجازی، آنچه از همه مهم‌تر است، مسئله‌ی شبکه‌ی ملی اطلاعات است؛ متأسفانه در این زمینه کوتاهی شده، کاری که باید انجام بگیرد، انجام نگرفته؛ این [طور] نمیشود. اینکه ما به‌عنوان اینکه نباید جلوی فضای مجازی را گرفت، در این زمینه‌ها کوتاهی کنیم، این مسئله‌ای را حل نمیکند و منطقی درستی هم نیست» (بیانات، ۱۳۹۵: دیدار با دانشجویان).

گذشته از مسائل اجتماعی ایجاد شده در جامعه که مرتبط با فضای سایبری است در همین حضور و بسنده به تولید محتوا، آیا اقتضای چنین محیطی در نظر گرفته شده است؟ آیا صحنه مبارزه جای انتشار هر نوع محتوایی است؟ چه محتوایی چگونه و در چه بعدی قابل انتشار است؟ آیا هر آنچه شخص می‌داند و به هر محتوای اسلامی دسترسی و تسلط دارد جایی برای انتشار در این فضا دارد؟ آیا منابع اسلامی ما، سرمایه‌ها و اصول حرکت ما نیست؟ چرا تمام کتاب‌ها و منابع و ... در این فضا قابل دسترس است؟ اگر تحریفی صورت گرفت چند نفر متوجه این اشکالات می‌شوند؟ اصلاً انتشار محتوا تنها روش مبارزه است؟ آیا آشنایی با تکنیک‌های اثرگذاری بر مخاطب که سوغات یونسکو است کافی است یا لازم بود تکنیک‌ها هم بومی شده باشد؟ اصولاً آیا در فضایی که مدیریت آن دست ما نیست، این حرکت کافی است؟ و صدها سؤال دیگر که برای آن پاسخی قبل از اقدام نیافته و بدون آن، حرکت شد.

«آنچه عرض من است و من روی آن تکیه میکنم این است که فضای مجازی بدون اختیار ما، از بیرون از اختیار ما دارد مدیریت میشود؛ بحث این است. فضای مجازی یک چیزی نیست که آدم بتواند مثل یک آب روانی هر جور که میخواهد از آن استفاده بکند؛ دیگران دارند این آب را به یک سمتی که خودشان میخواهند هدایت میکنند؛ آنها دارند مدیریت میکنند این فضا را. خب وقتی که ما میدانیم کسانی از بیرون دارند فضای مجازی را - که ما هم دست‌اندرکارش هستیم و مبتلابه ما است - هدایت میکنند و مدیریت میکنند، ما نمیتوانیم بی‌کار بنشینیم در مقابل او؛ ما نمیتوانیم مردمان را که با فضای مجازی ارتباط دارند، بی‌پناه رها کنیم در اختیار آن مدیری که دارد پشت پرده، فضای مجازی را اداره میکند. عوامل مسلط بین‌المللی در این زمینه‌ها بشدت فعالند: از لحاظ خبردهی، خبررسانی، تحلیل داده‌ها و امثال گوناگون؛ هزاران کار دارد انجام میگیرد روی فضای مجازی. برای خاطر این است که بنده روی مسئله‌ی شبکه‌ی ملی اطلاعات این همه تأکید میکنم. این شورای عالی فضای مجازی و مرکز ملی فضای مجازی که تشکیل داده‌ایم و بنده اصرار داشتم و دارم که این [شورا] تشکیل بشود و رؤسای محترم در آن شرکت کنند و تصمیم‌گیری کنند و اجرا کنند، به خاطر اهمیت این مسئله است؛ نمیشود این مسئله را رها کرد. و من میبینم که آن اهتمام لازم به خرج داده نمیشود. خب الان شبکه‌ی ملی اطلاعات اجزائی دارد، این اجزا باید در زمان‌بندی‌های مشخص تحقق پیدا کند؛ آدم میبیند که تحقق پیدا نمیکند، از زمان‌بندی‌ها عقبند؛ یا سیاستهای اصولی‌ای در زمینه‌ی پهنای باند وجود دارد که مکرر ابلاغ شده، خب این سیاستها باید رعایت بشود و اینها مورد درخواست و تأکید مؤکد اینجانب است» (بیانات، ۱۳۹۵: دیدار با هیئت دولت).

و گاهی فراتر رفته و متأسفانه به دلیل عقب بودن علمی در تکنولوژی، ضعف فرهنگی را باور نموده و فرهنگ اقتدار و استقلال هم از یاد رفت و قطعاً اینگونه حرکت نمی‌تواند نماد نصیحه باشد.

«البته بی بندوباری و فساد هم یکی از شاخه‌های تهاجم فرهنگی است؛ اما تهاجم فرهنگی بزرگتر این است که اینها در طول سالهای متمادی به مغز ایرانی و باور ایرانی تزریق کردند که تو نمیتوانی؛ باید دنباله‌رو غرب و اروپا باشی. نمیگذارند خودمان را باور کنیم. الان شما اگر در علوم انسانی، در علوم طبیعی، در فیزیک و در ریاضی و غیره یک نظریه‌ی علمی داشته باشید، چنانچه برخلاف نظریات رایج و نوشته شده‌ی دنیا باشد، عده‌ی میایستند و میگویند حرف شما در اقتصاد، مخالف با نظریه‌ی فلانی است؛ حرف شما در روان‌شناسی، مخالف با نظریه‌ی فلانی است. یعنی آن طوری که مؤمنین نسبت به قرآن و کلام خدا و وحی الهی اعتقاد دارند، اینها به نظرات فلان دانشمند اروپایی همان اندازه یا بیشتر اعتقاد دارند!» (بیانات، ۱۳۸۳: دیدار دانشجویان و اساتید دانشگاه همدان).

«عده‌ای فکر میکنند چون غربی‌ها از لحاظ علمی بر ما برتری دارند، پس ما باید فرهنگ و عقاید و آداب معاشرت و آداب زندگی و روابط اجتماعی و سیاسیمان را از آنها یاد بگیریم؛ این اشتباه است شاگردی کردن در علم، به معنای تقلید کردن در فرهنگ نیست؛ این نکته بسیار مهمی است.» (بیانات، ۱۳۸۳: دیدار دانشجویان و اساتید دانشگاه همدان).

#### ۵.۴ عدم وحدت عملکرد و نگاه کلان و بین‌المللی و القای سرگردانی به مردم

رصد فعالیت‌های تبلیغی موجود بیانگر آن است که به‌جز مواردی اندک، نه‌تنها بین برنامه‌های اجرایی و هم‌سویی فعالیت‌های در حال انجام، وحدتی دیده نمی‌شود و بیشتر فعالیت‌ها توده‌ای و پراکنده است، نگاه کلان در روابط بین‌المللی نیز در اذهان وجود ندارد.

«یکی دیگر از مسائلی که به نظرم میتوانید شما انجام بدهید تشکیل یک جبهه‌ی واحد ضدآمریکایی و ضدصهیونیستی در سطح دانشجویان جهان اسلام است؛ این کار را بکنید. بنشینید، فکر کنید، بعد یک جبهه‌ی ضدصهیونیستی و ضدآمریکایی [تشکیل بدهید]. امروز وسیله‌ی ارتباط هم آسان است، دیگر نامه‌نگاری و پست و تلگراف و مانند اینها لازم ندارد. در فضای مجازی تماس بگیرید، کما اینکه در موارد مشابهی این کار انجام گرفته به قول این فرنگی‌مآب‌ها یک کمپین‌های عمومی دنیای اسلامی تشکیل بدهید علیه تسلط آمریکا، از لحاظ ضدیت با سیاست‌های آمریکایی و سیاست‌های صهیونیستی. میلیون‌ها عضو وارد این مجموعه بشوند، وارد این جریان فکری بشوند و برایشان خوراک تهیه کنید؛ آن وقت آنها هم برای شما خوراک تهیه میکنند، چون در دنیای اسلام هم بالاخره افکار خوب دانشجویی وجود دارد؛ یک جمعیت عظیم دانشجویی در دنیای اسلام به وجود بیاورید» (بیانات، ۱۳۹۵: دیدار جمعی دانشجویان).

همچنین در استفاده تبلیغی از پیام‌رسان‌ها و شبکه‌های اجتماعی غیربومی که گاهی با شعار ارتباط و رساندن سخن به دنیا استفاده می‌شود، وحدت رویه وجود ندارد، از این جهت افراد عامه که اصولاً در تعیین رفتار خود به افراد شهره در منصب‌های مذهبی و فرهنگی رجوع می‌نمایند، فارغ از درست یا غلط بودن این شیوه، دچار سردرگمی و اختلاف و ایجاد دوقطبی و چندقطبی‌های کاذب و در نهایت اختلافات درونی شده است. گذشته از اینکه این اختلاف عملکرد باید قبل از ورود به صحنه عمل و عمومی در گروه‌های تخصصی و اندیشه‌ورز بین مسئولین فرهنگی و مذهبی حل شده باشد.

«من عرض می‌کنم ما در برخورد با مسائل تهاجمی، پدیده را در اول ورود، حتی قبل از ورود باید بشناسیم.

فرض کنید یک چیزی، یک فکری، یک روشی در دنیا دارد رایج می‌شود؛ پیدا است که این اینجا خواهد آمد، خوب دنیا دنیای ارتباطات است، دنیای اتصال و ارتباط است، نمی‌شود حصار کشید، قبل از آنکه بیاید، به فکر باشید که برخورد حکیمانه با این چیست؟ معنای این همیشه این نیست که ما آن را رد کنیم؛ نه، گاهی یک پدیده‌ای است که ما آن را می‌توانیم قبول کنیم، گاهی پدیده‌ای است که می‌توانیم اصلاح کنیم، گاهی پدیده‌ای است که می‌توانیم یک ذیلی برایش تعریف کنیم که آن ذیل، مشکل آن را برطرف کند» (بیانات، ۱۳۹۲: دیدار شورای عالی فرهنگی).

«نمی‌شود بی‌قیدوشرط، هرچه را که از آن سوی مرزها می‌فرستند، اعم از کالای فرهنگی و هم‌چنین امواج تبلیغی و فرهنگی، پذیرفت. دشمن در کمین است؛ به‌خصوص در کمین جوانان» (بیانات، ۱۳۷۵: در جمع مردم ارومیه در استادیوم تختی).

به نظر می‌رسد فارغ از تمام دلایل موجود، اصل اختلافات به عدم تطبیق اصول عملکرد مبلغین با مبانی و اصول انقلاب بازگشت دارد. در واقع کلام امامین انقلاب به درستی بررسی و تبیین نشده است. بخشی از وصیت‌نامه امام (ره) در مورد رسانه است که کمتر مورد توجه قرار گرفته است. هم‌چنین مقام معظم رهبری در موقعیت‌های مختلف به اصول و ضوابط لازم اشاره داشته‌اند. از بررسی کلام ایشان اصول و ضوابط متعددی قابل استخراج است که فقط به یک مورد از آنها اشاره می‌شود. از جمله شرایط حضور تبلیغی در نرم‌افزارهای غیر بومی از دیدگاه ولایت فقیه، جریان‌سازی است.

«دستگاه‌های مختلفی در فضای مجازی حضور دارند اما حضور در این فضا باید یک حضور جریان‌ساز باشد» (بیانات، ۱۳۹۷: دیدار مسئولان سازمان تبلیغات)

«جوانهای عزیز! بچه‌های عزیز من! فردا مال شما است، آینده مال شما است؛ شما هستید که باید این تاریخ را با عزت‌ش محفوظ نگه دارید؛ شما هستید که این بار مسئولیت را بردوش دارید؛ خرمشهرها در پیش است؛ نه در میدان جنگ نظامی، [بلکه] در یک میدانی که از جنگ نظامی سخت‌تر است. البته ویرانی‌های جنگ نظامی را ندارد؛ بعکس، آبادانی به دنبال دارد، اما سختی‌اش بیشتر است» (بیانات، ۱۳۹۵: دیدار دانشجویان دانشگاه افسری).

## ۵ نتیجه‌گیری

- لازمه انتظار حقیقی آن است که شخص منتظر در عرصه عملی به اسلحه رزم و آموختن شیوه‌های نوین مجهز و در عرصه جهاد علمی به سلاح قلم و سخن مسلح باشد و بداند بخش مهمی از پیروزی آن حضرت بسته به رشد فرهنگی جامعه بشری است.
- با تکیه بر کلام حضرت مهدی و ضمیمه آیات «نصح» و لغت، مبنای تبلیغ، «نصیحة» است
- رصد فعالیت‌های تبلیغی موجود نشان می‌دهد، گفتمان رایج در بین فعالان عرصه تبلیغ در این فضا، از جهت ارکان تبلیغ در بیان رایج امروزی، نگرشی ابزاری است.
- بررسی کل کلام حضرت مهدی نشان می‌دهد از همان ابتدای تولد، روح حاکم بر کلام ایشان نوعی



- ایجاد آمادگی در پیروان، در جهت درک و باور حضور امام، بدون ارتباط مستقیم با ایشان بوده است. پس شاخص انتظار البته به معنای خاص آن، همان «زمان غیبت» بودن آن است..
- در حادثه واقعه فضای سایبر، در زمان غیبت، طبق کلام حضرت مهدی پیروی همگان به ویژه علما و مبلغان دین، از رهنمودهای رهبری در نحوه مواجهه و عملکرد، جزء وظایف بلکه از الزامات و ضروریات زمان حاضر است.
  - بسیاری از فعالیت‌ها از بخش‌هایی از کلام رهبری در جهت تأیید فعالیت خود استفاده نموده اند نه اینکه کلام بررسی و بر طبق کل این نظام فکری بخشی از کار را دست گرفته و تلاش برای عملی شدن آن صورت گیرد.
  - نگاه ابزاری برخی ما مبلغان چه از بعد فرهنگ قرآنی، چه نظریات تکنولوژی، چه رسانه بودن، چه مساوی بودن ابزارها رسانه و چه به نسبت مدیریت ابزار و کاربر در حد نگاه به اسباب بازی کودکان، غیر جدی و عامیانه است.
  - اکثر فعالیت‌های تبلیغی به روش ایجاد کانال، گروه، صفحه و غالباً در نرم‌افزارهای غیربومی انجام می‌شود که قطره‌ای از ظرفیت اقیانوس فضای مجازی است و در آشکارترین محدودانگاری، بازی‌ها که ۳۲ میلیون کاربر در سال ۹۸ طبق آمار رسمی با متوسط نود دقیقه در روز بوده است، نادیده گرفته شده است.
  - روح حاکم بر شیوه تبلیغ و حضور اکثریت مبلغان در فضای سایبر، هم‌سوی بسیاری از مسئولین، پذیرش شرایط موجود و عدم توان در تغییر شرایط و محال و ناممکن بودن بومی‌سازی تمام ارکان رسانه در کشور اسلامی ایران است. به بیانی جدید و نوع عمل ناظر به حضور در میدان مبارزه بودن نیست.
  - به‌جز مواردی اندک، نه‌تنها بین برنامه‌های اجرایی و هم‌سویی فعالیت‌های در حال انجام، وحدتی دیده نمی‌شود و بیشتر فعالیت‌ها، توده‌ای و پراکنده است. نگاه کلان در روابط بین‌المللی در اذهان وجود ندارد و موازی‌کاری‌ها و اختلاف نظرهای نخبگان، مردم عادی را دچار سرگردانی نموده است.

## مراجع

- [۱] ابن بابویه، محمد بن علی (محقق علی اکبر غفاری)، کمال الدین و تمام النعمة، ج ۲، تهران: دار الکتب الإسلامية، ۱۳۹۵.
- [۲] ابن طاووس، علی بن موسی، و مؤسسه صاحب‌الأمر (عج)، التشریف بالمنن فی التعریف بالفتن (ج ۱)، قم: مؤسسه فرهنگی صاحب‌الامر (عجل‌الله فرجه الشریف)، ۱۴۱۶ هـ. ق.
- [۳] جوادی آملی، عبدالله، امام مهدی موجود موعود (۱۳۹۷)، چاپ پانزدهم، قم: اسراء.



- [۴] خسروی، علی اکبر؛ پوشنه، کامبیز؛ کیانی بختیاری، ابوالفضل، مبانی و منطق آموزش فناوری (۱۳۹۰)، ش ۱، نشریه نشاء، صص ۷۰-۷۵.
- [۵] خمینی، سید روح الله، شوون و اختیارات ولی فقیه (ترجمه مبحث ولایت فقیه از کتاب البیع) (۱۳۶۹)، چاپ دوم، تهران: وزارت فرهنگ و ارشاد اسلامی.
- [۶] راغب اصفهانی، حسین بن محمد، معجم مفردات الفاظ القرآن (تحقیق ندیم مرعشلی) (۱۳۹۲ ه. ق)، بی جا: اسماعیلیان.
- [۷] شریف زاده رحمان؛ مقدم حیدری غلامحسین، خروج از دوگانگی تکنولوژی خودمختار و تکنولوژی به مثابه وسیله صرف، بر اساس دیدگاه برونولاتور (۱۳۹۴)، ش ۱، نشریه فلسفه علم، صص ۲۹-۵۱.
- [۸] طبرسی، احمد بن علی (محمدباقر موسوی خراسان)، الاحتجاج (۱۴۰۳)، ج ۲، مشهد: نشر المرتضی.
- [۹] طوسی، محمد بن حسن (محمدمحسن آقابزرگ تهرانی و دیگران)، الغیبة (شیخ طوسی) (۱۴۲۵)، قم: مؤسسه المعارف الإسلامية.
- [۱۰] عبدالباقی، محمد جواد، المعجم المفهرس (۱۳۹۱)، چاپ دهم، قم: نوید اسلام.
- [۱۱] غمامی، محمد علی، روش شناسی بنیادین ارتباطات برای توسعه در بنیاد راکفلر؛ فلسفه ارتباطات تا سیاست های ارتباطی، فصلنامه مطالعات الگوی پیشرفت اسلامی و ایرانی، ش ۱، ۱۳۹۱، صص ۱۹۵-۲۵۷.
- [۱۲] فیض کاشانی؛ محمد بن شاه مرتضی، نوادر الأخبار فیما يتعلق بأصول الدین (۱۳۷۲ ه. ش) ج ۱، تهران: وزارت فرهنگ و آموزش عالی، مؤسسه مطالعات و تحقیقات فرهنگی (پژوهشگاه).
- [۱۳] کفعمی، ابراهیم بن علی، البلد الامین (بی تا)، کتابخانه نور، نسخه الکترونیکی.
- [۱۴] کهوند، محمد، شبکه عنکبوتی (۱۳۹۷)، چاپ دوم، قم: معاونت تبلیغ و امور فرهنگی حوزه های علمیه.
- [۱۵] معرفت، محمدهادی، ولایت فقیه از دیدگاه شیخ انصاری و آیه الله خویی (۱۳۷۸)، ش ۱۱، مشهد: دانشگاه علوم اسلامی رضوی، صص ۲۴۶-۲۶۴.
- [۱۶] نعمانی، محمد بن ابراهیم (تنظیم علی اکبر غفاری)، الغیبة (۱۳۹۷)، بی چاپ، تهران: مکتبه الصدوق.
- [۱۷] ولایت و حکومت، پایگاه تخصصی وسائل (فقه تخصصی)، بازیابی شده در: ۲۳/۷/۱۴۰۱، ۲۳:۲۰.
- [۱۸] تأثیر استریم بر دنیای گیمرها، تبیان، بازیابی شده در: ۲۳/۷/۱۴۰۱، ۲۳:۲۴.
- [۱۹] بازینگاشت نمای تهران؛ شاخص ترین اطلاعات مصرف بازی های دیجیتال در شهر تهران تا پایان سال ۱۳۹۸، دایرکت، بازیابی شده در: ۲۳/۷/۱۴۰۱، ۲۳:۳۱.
- [۲۰] بیانات در دیدار علما و روحانیون خراسان شمالی، دفتر حفظ و نشر آثار آیت الله خامنه ای، بازیابی شده در: ۲۳/۷/۱۴۰۱، ۲۳:۳۹.
- [۲۱] بیانات در دیدار مدیران شبکه ی دوم سیما، دفتر حفظ و نشر آثار آیت الله خامنه ای، بازیابی شده در: ۲۳/۷/۱۴۰۱، ۲۳:۴۳.
- [۲۲] دیدار با دانشجویان و اساتید دانشگاه های همدان، دفتر حفظ و نشر آثار آیت الله خامنه ای، بازیابی شده در: ۲۳/۷/۱۴۰۱، ۲۳:۵۵.
- [۲۳] دیدار مسئولان سازمان صدا و سیما، دفتر حفظ و نشر آثار آیت الله خامنه ای، بازیابی شده در: ۲۳/۷/۱۴۰۱، ۲۳:۵۴.
- [۲۴] بیست و هفتمین سالگرد رحلت امام خمینی (رحمه الله)، دفتر حفظ و نشر آثار آیت الله خامنه ای، بازیابی شده در: ۲۳/۷/۱۴۰۱، ۲۳:۵۹.
- [۲۵] دیدار با دانشجویان، دفتر حفظ و نشر آثار آیت الله خامنه ای، بازیابی شده در: ۲۳/۷/۱۴۰۱، ۱۲:۰۰.
- [۲۶] دیدار بسیجیان، دفتر حفظ و نشر آثار آیت الله خامنه ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۰۲.

- [۲۷] دیدار ده هزار نفری با بسیجیان، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۰۳
- [۲۸] دیدار با دانش آموزان، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۰۶
- [۲۹] دیدار معلمان و فرهنگیان، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۰۷
- [۳۰] دیدار با دانشجویان دانشگاه امام حسین علیه السلام، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۰۸
- [۳۱] دیدار با جلسه هیئت دولت، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۱۰
- [۳۲] دیدار با جمعی دانشجویان، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۱۲
- [۳۳] دیدار شورای عالی فرهنگی، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۱۱
- [۳۴] دیدار با مردم ارومیه، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۱۳
- [۳۵] دیدار با مسئولان سازمان تبلیغات، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۱۴
- [۳۶] دیدار رئیس و نمایندگان مجلس شورای اسلامی، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۱۷
- [۳۷] سی‌ویکمین سالگرد رحلت امام خمینی (رحمه‌الله)، دفتر حفظ و نشر آثار آیت الله خامنه‌ای، بازیابی شده در: ۲۴/۷/۱۴۰۱، ۰۰:۱۸

## فرصت‌ها و چالش‌های تبلیغ دین در فضای مجازی از دیدگاه قرآن

محمد رضا برزویی زاده<sup>۱</sup>، زهره جمالی زواره<sup>۲</sup>

<sup>۱</sup> عضو هیئت علمی و استادیار دانشکده معارف اسلامی و فرهنگ و ارتباطات دانشگاه امام صادق (ع)، تهران  
borzooei@gmail.com

<sup>۲</sup> طلبه سطح ۴ (مدرس حوزه و دانشگاه)، رشته تفسیر تطبیقی، مؤسسه عالی تخصصی فاطمه الزهرا (س)،  
اصفهان  
jamali@whc.ir

### چکیده

فضای مجازی، یکی از فضاهاى نوین مؤثر در جهت تبلیغ دین است. توجه به این فضا، به دلیل عجز شدن زندگی اکثر مردم جهان با آن و فعالیت هدفمند و مؤثر دشمن، ضرورت دارد. این نوشتار که به روش توصیفی اکتشافی و به شیوه‌ی کتابخانه‌ای انجام شده است در صدد افزایش آگاهی و ارائه نگاه هوشمندانه منطبق با دیدگاه قرآن کریم به فضای مجازی، در جهت تبلیغ دین است. مبلغی که شناخت صحیح منطبق بر قرآن نسبت به تبلیغ دارد، فضای مجازی را، هر چند عرصه‌ای می‌بیند که با تعدیل هزینه‌های اقتصادی، گستردگی مخاطب، گستره‌ی جغرافیایی، امکان عرضه و دسترسی به پیام در اشکال مختلف در کمترین زمان و تسهیل روابط، فرصت‌هایی بی‌نظیر برای اهداف او ایجاد نموده است، توجه دارد که این فرصت‌ها در فضایی ایجاد شده است که حاکمیت آن صهیونیسم بین‌الملل و مجریان آن دشمن سرسخت اسلام و برای رسیدن به جهانی بدون مرز برنامه‌ریزی و هدف‌گذاری شده است. گستردگی مخاطب، ناهمگونی به همراه دارد که رعایت مقتضای حال را به شدت دشوار می‌نماید. تعدیل هزینه‌ها، تحمیل هزینه‌هایی جدی در پی دارد. پیام درست او در محیطی هوشمند و در رقابت با محتوای نزدیک به بی‌نهایت و نامناسب به چالش می‌افتد. ضمن کاهش ارتباطات چهره به چهره، حرکت به سمت حذف ارتباط دائم با خداوند، افزایش اولویت‌های ناصحیح، تقویت روابط مخالف با اصول قرآنی، او و پیام‌گیرش را به انزوا و افسردگی می‌کشاند. بنابراین استفاده از فرصت‌ها نیازمند مهارتی ویژه و زمینه‌سازیهایی است که به صورت فردی ممکن نیست.

**کلمات کلیدی:** فضای مجازی، تبلیغ، تبلیغ دین، فرصت، چالش.

## ۱ مقدمه

با پیشرفت بیشتر علم و با ادغام سیستم‌های الکترونیک و علم ارتباطات، اینترنت ابداع شد. پیدایش این پدیده را اکثر دانشمندان جامعه‌شناسی، انقلاب چهارم نام نهادند. با ظهور رسانه‌ی فراگیر اینترنت و تسهیل در نقل و انتقال اطلاعات و ارتباط بین انسانی، تبدیل مکان به فضا و کمرنگ شدن محدودیت زمانی و ایجاد صدها مزیت دیگر، فرصت‌هایی در اختیار تبلیغ دین قرار داده شد (عزت‌الله‌زاده، ۱۳۹۵: ۲۴). همانطور که تبلیغات از جدیدترین فنون برای پیشبرد اهداف خود بهره می‌جوید، از پیچیدگی‌های بسیاری نیز برخوردار است. بنابراین چگونگی حفظ روند صحیح تبلیغات در عرصه‌ی فضای مجازی از مهم‌ترین وظایف مبلغ است. مبلغ باید همانگونه که در صدد برنامه‌ریزی اجرای تبلیغات است، در فکر شناخت و برنامه‌ریزی چالش‌های فرا روی خود نیز باشد (قیصریان، ۱۳۹۲: ۸۸)؛ و لازم است ملاک خود در تعیین و شناخت این فرصت‌ها و چالش‌ها را کلام خداوند، قرار دهد.

فرصت‌ها و چالش‌های پیشروی تبلیغ دین در فضای مجازی از ابعاد مختلفی قابل بررسی است. از نگاه اهداف این نوشتار و بر طبق ارکان تبلیغ، برخی متوجه محتوا و یا همان پیام، برخی متوجه کاربران به‌عنوان پیامگذار و پیام‌گیر و برخی به محیط و فضای موجود که ابزار و یا همان شیوه‌ی کار است، مربوط می‌شود. پژوهش حاضر با بررسی سخنان بزرگان و کارشناسان این عرصه از جمله سخنان مقام معظم رهبری، فرصت‌ها و چالش‌ها را استخراج و سپس در پنج عنوان کلی دسته‌بندی نموده است. نگاه این نوشتار به موارد نامبرده، نگاهی دو بعدی است با این توضیح که موارد پنجگانه را هم از جهت فرصت بودن و هم از جهت چالش بودن، مورد بحث قرار می‌دهد. این نوشتار به دنبال تطبیق یا تلقین یا تأیید نظری از قرآن نبوده است و بررسی خود را بر مبنای تبیین مجزای هر فرصت و چالش در فضای مجازی و قرآن انجام داده و دریافت را به عهده‌ی مخاطب گذاشته است. روش پژوهش به بیانی «اجتهادی، سندپژوهی و کتابخانه‌ای»، از نظر هدف یک تحقیق «کاربردی» و از نظر ماهیت، یک تحقیق توصیفی - اکتشافی است. بررسی‌ها نشان می‌دهد، استفاده از فرصت‌های این فضا در جهت ترویج معارف دینی، به دلیل عجین بودن باچالش‌های جدی، نیازمند مهارتی ویژه و زمینه‌سازی‌هایی است که به‌صورت فردی ممکن نیست.

## ۲ فرصت‌ها و چالش‌های پیش روی مبلغ دینی در فضای مجازی

پیدایش فضای مجازی، فرصت‌هایی را در اختیار تبلیغ دین قرار داد (عزت‌الله‌زاده، ۱۳۹۵: ۲۴) که بررسی این فرصت‌ها از دیدگاه قرآن، در استفاده‌ی صحیح و بهینه از آن ضروری است. گذشته از آن فرصت‌های ایجاد شده، از وجود چالش‌ها در امان نبوده و توجه به آنها را لازم می‌نماید. در ادامه مهم‌ترین فرصت‌ها، مطرح و ضمن پرداختن به چالش‌ها، موارد نامبرده از دیدگاه قرآن مورد بررسی قرار خواهد گرفت.

### ۱.۲ گسترده‌ی مخاطب

نقطه‌ی عطف تبلیغ، رساندن پیام به مخاطب است. در واقع شاکله‌ی تبلیغ، وابسته به مخاطب است و تبلیغ با فرض عدم وجود مخاطب، منتفی است. طبق آیه‌ی ۱۸ سوره‌ی زمر، بندگان خدا، طالب حق و رشدند، به

هر سخنی که گوش دهند به این امید گوش میدهند که در آن حقی بیابند و این طور نیست که هر سخنی را به صرف شنیدن بدون تفکر و تدبیر رد کنند. پیروی از بهترین قول، خود، هدایتی الهی و نشانه‌ی داشتن عقل است (علامه طباطبایی، ۱۴۱۷ق ج ۱۷: ۲۵۰ و ۲۵۱). واژه‌ی «یستمعون» تأکیدی بر اهمیت حضور فعال و مؤثر مخاطب و آمادگی او در دریافت سخن حق است. بنابراین، نه فقط مخاطب بلکه حضور فعال و مؤثرش نسبتی عمیق با تبلیغ دارد.

در قرآن، وجود مصداق اعداد از عدد یک (واحد) (بقره/۱۶۳) تا صد هزار (صافات/۱۴۷) متغیر است. این مقادیر عددی در موضوعات مختلفی مطرح شده است. در این بین، دو مصداق به دلیل ارتباط با بحث حاضر قابل توجه است. یکی عدد ۹۵۰ (عنکبوت/۱۴) که به صورت هزار سال پنجاه سال کمتر و در بیان کثرت مدت بعثت حضرت نوح علیه السلام است (علامه طباطبایی، ۱۴۱۷ق، ج ۱۶: ۱۶۴). دیگری عدد صد هزار (صافات/۱۴۷) است که ارسال دوم حضرت یونس علیه السلام به سوی قومی بت پرست با این تعداد جمعیت و بیشتر است؛ و با توجه به آیات بعدی به دلیل تصدیق و پیروی قوم از دعوت ایشان، عذاب الهی که همیشه با آن تهدید می شدند از آنها برداشته شد (علامه طباطبایی، ۱۴۱۷ق ج ۱۷: ۲۵۰ و ۲۵۱). با توجه به فصاحت و بلاغت قرآن و اینکه مهمترین و اصلی ترین وظیفه‌ی پیامبران از دیدگاه قرآن، تبلیغ روشن است (عنکبوت/۱۸)، این عدد می تواند شاهی بر اهمیت گستردگی مخاطب در امر تبلیغ از دیدگاه قرآن باشد. از یک طرف خداوند به مدت طولانی، دعوت حضرت نوح علیه السلام و کم بودن تعداد ایمان آوردندگان و هلاک شدن همه جز تعداد اندکی از ایمان آوردندگان اشاره دارد و از طرف دیگر پیروی اکثریت، عذاب وعده داده شده را بر می دارد.

شاهد دیگری بر اهمیت تعداد مخاطب در تبلیغ دین از دیدگاه قرآن، آیه‌ی ۵۹ سوره‌ی طه است. زمانی که خداوند متعال، موسی علیه السلام را به سوی فرعون فرستاد، فرعون ضمن جنجال (طه/۵۷)، برای نشان دادن قاطعیت خود، پیشنهاد موعدی داد که تعیین زمان آن را به حضرت موسی علیه السلام سپرد. حضرت موسی علیه السلام نيمروز روز زینت را به عنوان زمان وعده مشخص نمود. روز زینت و حضور اجباری همه‌ی مردم (حشر ناس) شرط این دیدار تعریف شد تا ضمن حضور همه‌ی مردم، به دلیل روشنایی روز، آنچه اتفاق می افتد قابل مشاهده باشد. گذشته از آن طبق آیه‌ی ۵۸، مکان تجمع محلی در وسط و بدون پستی و بلندی مشخص شد (علامه طباطبایی، ۱۴۱۷ق، ج ۱۴: ۱۶۴) و تأکید شد که خلف وعده از هیچ طرف صورت نگیرد. به طور قطع حضرت موسی علیه السلام به عنوان پیام آور الهی و فرستاده‌ی خدا به سمت فرعون، موعده را زمانی غیر از آنچه رضایت الهی در آن باشد تعیین نمی کند و حداقل ویژگی زمانی که برای تقابل جبهه‌ی حق و باطل انتخاب شد، حضور حد اکثری، با امکان بیشترین اثرگذاری است. چرا که این روز به عنوان روزی است که مردم، خود و بازارها را زینت می کنند و مسلماً اثرپذیری از برنده‌ی این میدان، در مردمی که وقت شادی و زینتشان است، انقلاب قابل توجهی است. به ویژه زمانی که هر دو طرف، افراد شناخته شده‌ای بوده و با تقابل دو موضوع، با ظاهری مشابه (سحر و جادو با معجزه) و برای یک هدف یعنی مشخص شدن حق از باطل از بین دو ادعا، صورت می گیرد.

بنابراین اهمیت تعداد مخاطب در زمان تبلیغ از دیدگاه قرآن، مسئله‌ی روشنی است. اگر به موارد نامبرده «رحمة للعالمین» (انبیاء/۱۰۷) بودن پیامبر اکرم یعنی فرستاده‌ای به سوی همه‌ی اجتماعات بشری و رحمت

بودن برای همه‌ی اهل دنیا (علامه طباطبایی، ۱۴۱۷ق، ج ۱۴: ۳۳۱) اضافه شود و نامه‌نگاری‌های حضرتش به کسرا، پادشاه ایران در شرق و به قیصر روم در غرب (احمدی میانجی، ۱۴۱۹ق، ج ۲: ۳۱۵) و دعوت آنها به اسلام که نهایت استفاده از فرصت پهنه‌ی تبلیغی است، در نظر گرفته شود، امری بدیهی است. افزایش روز افزون کاربران فضای مجازی بر کسی پوشیده نیست، با این وجود دقت در آمار اعلام شده‌ی «مؤسسه‌ی وی آر سوشال» (We Are Social) می‌تواند تأییدی بر این مدعا باشد.

بر اساس گزارش مذکور<sup>۱</sup> در سال ۲۰۱۸ میلادی، تعداد کاربران اینترنت ۰۲۱.۴ میلیارد نفر از سراسر دنیا هستند. ۲۵۰ میلیون نفر از آنها کاربرانی هستند که در سال ۲۰۱۸ به این مجموعه پیوسته‌اند. از این کاربران جدید، ۲۰۰ میلیون نفر توسط تلفن همراه به این فضا دسترسی پیدا نموده‌اند. این تعداد کاربر، ۵۳ درصد جمعیت جهان است. همچنین ۶۸ درصد مردم جهان تلفن همراه دارند که از این حدود ۵ میلیارد نفر، تقریباً سه میلیارد نفر با گوشی تلفن همراه کاربر فعال شبکه‌های اجتماعی هستند. اطلاع از اینکه مردم جهان در سال ۲۰۱۸ در مجموع یک میلیارد سال زمان در اینترنت گذرانده‌اند، مشخص‌کننده‌ی گستردگی مخاطب در این فضا است. اگر چه دسترسی به پیام‌گیران انبوه در فضای مجازی موجب ایجاد فرصتی کم‌نظیر برای تبلیغ دین شده است اما همین فرصت، چالش‌هایی جدی پیش‌روی مبلغ قرار داده است. از جمله اینکه یکی از آداب تبلیغ که نقش مهمی در موفقیت آن دارد، در نظر گرفتن مقتضای حال است. از آنجایی که افراد مختلف، درجه‌ی ایمان و عقل متفاوتی دارند، مبلغ موظف است که با هر انسانی به اندازه‌ی عقل و ایمان او سخن گفته و چیزی را از او بخواهد که توان آن را داشته باشد. با دقت در قرآن و روایات، صدها نمونه از تناسب موضوع با مخاطب دیده می‌شود (قرائتی، ۱۳۷۷: ۷۳). از جمله توجه به آیات مکی و مدنی و تفاوت محتوا و نوع بیان آیات، نشان‌دهنده‌ی نوعی تناسب سخن است (داورپناه، ۱۳۷۵: ۲۵). در شیوه‌ی مبلغان صدر اسلام نیز این ادب تبلیغ دیده می‌شود. جعفر طیار در برابر پادشاه حبشه که مسیحی بود، آیاتی از سوره‌ی مریم را تلاوت نمود (سبحانی، ۱۳۸۵: ۳۰۹). عمل به این ضرورت در فضای مجازی به دلایل مختلف با چالش‌های اساسی روبرو است.

مخاطب فضای مجازی علاوه بر اینکه در نژاد، دین، سن، فرهنگ، زبان، استعداد، جنسیت، عقل و ایمان به شدت نا همگون است، در این فضا امکان داشتن هویتی جعلی (ساختگی) و سیال (چند هویتی بودن) برای او فراهم شده است. در فرهنگ فضای مجازی، بیشتر کاربران گمنام هستند، نه جسم دارند و نه چهره و تاریخ، نه صدایی هست و نه حرکت و ایما و اشاره و زبان بدن، فقط کلمات، رابطه‌ها را شکل می‌دهند و افزوده شدن امکانات سمعی و بصری نیز کمک خاصی به این مشکل کرده است. این مشکل، در صورت فرض هویت راستین است. در حالی که کاربر این فضا می‌تواند در موقعیت‌های مختلف، هویت دیگری برای خود بسازد و هویت‌های متعدد، زودگذر و ناپایداری را تجربه کند. حتی می‌تواند در یک بحث و مناظره با هویت‌های متعدد شرکت کند (مهدی‌پور، ۱۳۹۶: ۸۰-۸۶).

بنابراین آنچه مبلغ به‌عنوان مخاطب متعدد با آن روبرو است، کاربری‌هایی مبهم است که شناخت قابل توجهی از مخاطب به او نداده و کار او را بسیار دشوار می‌نماید و به تبع، دقت و مهارت مضاعفی می‌طلبد.

<sup>۱</sup><https://wearesocial.com/blog/2018/01/global-digital-report-2018>



حتی اگر فرض شود مبلغ، بنای کار خود را از ابتدا مشخص و محیط فعالیت خود را در این فضا به گروهی مشخص تخصیص دهد، علاوه بر چالش‌های بیان شده با چالش‌های دیگری روبرو می‌شود و در ارائه‌ی نوع محتوا دچار محدودیت خواهد شد. در فضایی که امکان دسترسی به محتوای آن برای افراد مختلف از صنف و گروه و سن و... مختلف ممکن است، طبق آیین تبلیغ، مبلغ نمی‌تواند هر حرفی را مطرح کند. حتی اگر پیام، آیات قرآن باشد. اگر برای حل این مشکلات، مبلغ مخاطبان را بعد از شناخت در فضای حقیقی به این محیط دعوت کند، علاوه بر آنکه با محدودیت مخاطب روبرو می‌شود، زمینه‌ی چالش‌های دیگری فراهم خواهد شد. از طرفی همان‌طور که قبلاً بیان شد یکی از عوامل موفقیت در تبلیغ، شخصیت پیام‌رسان است. با افزایش و ناهمگونی مخاطب، هر وضعی در مبلغ به شدت خود را نشان می‌دهد و می‌تواند در کم شدن تأثیر پیام بر مخاطب و چه بسا اثر معکوس داشتن، به شدت اثر داشته باشد. مبلغی که در شناخت محیط فعالیت، شناخت نیاز مخاطب، شیوه‌ی برخورد با مخاطب و... دچار ضعف آگاهی باشد، بدون برنامه‌ریزی و شاخصه‌های اخلاق نیکو در محیطی این‌چنینی دست به فعالیت بزند، بازنده‌ی میدان خواهد بود. کما اینکه در تبلیغ چهره به چهره هم این چالش وجود دارد. اما در فضای مجازی به دلیل ناشناخته بودن مخاطب، حتی اگر مبلغ ویژگی‌های لازم را داشته باشد، امکان این چالش به دلیل ناهمگونی مخاطب در فرهنگ و ایمان و عقل و... وجود دارد.

## ۲.۲ تعدیل هزینه‌های اقتصادی

در دنیای پر رقابت امروز، تبلیغات و استفاده از تبلیغ برای رسیدن به اهداف مختلف در فعالیت‌های مختلف روشی اجتناب‌ناپذیر است و هزینه برای تبلیغات در واقع نوعی سرمایه‌گذاری بنیادی و اصولی محسوب می‌شود. در صورت اجرای صحیح این اصول، نتایج ارزشمندی به همراه دارد. هر چند تبلیغ دینی، با تبلیغات رایج در دنیا متفاوت است و به دنبال رسانیدن حقیقت‌ها و واقعیت‌ها به مردمان دنیا است (رزاقی، ۱۳۷۷: ۲۳) ولی انواع تبلیغ از بُعد هزینه، مشترک بوده و هر کدام هزینه‌های خود را دارد. البته منظور در هزینه کردن برای تبلیغ اسلام این نیست که ثروت به صورت رشوه جهت پذیرش حرف حق، در اختیار دیگران قرار بگیرد اصولاً ایمان اسلام، اجبار و اکراه‌بردار نیست. اسلام با موانع اجتماعی و فکری ایمان مبارزه می‌کند. راه هدایت و رشد و راه ضلالت و گمراهی را می‌شناساند و انتخاب را بر عهده‌ی خود افراد می‌گذارد. بنابراین نقش ثروت در این تبلیغ، رفع موانع و رساندن حرف حق به افراد است (مطهری، ۱۳۸۵: ۲۱۵-۲۲۴).

تبلیغ دارای مراتب مختلفی است و نسبت به گروه‌های مختلف و هدف، شیوه‌ی آن متفاوت خواهد بود. طبق آیات قرآن، برنامه‌ی همه‌ی انبیای الهی در دعوت به توحید، بدون هیچگونه چشم‌داشتی از مردم و بر اساس «قُلْ لَا أَسْأَلُكُمْ عَلَيْهِ أَجْرًا» (هود/۵۱؛ انعام/۹۰) بوده است. خاتم انبیاء (صلی الله علیه و آله و سلم) نیز با دیگر سفیران الهی در این فراخوان رایگان، همگام بوده و قرآن در ضمن آیاتی به این حقیقت اشاره دارد (فهیمی، ۱۳۸۶: ۲۳۲ و ۲۳۴). اگر چه طبق آیه‌ی ۲۳ سوره‌ی مبارکه‌ی شورا حضرت «مودت فی القربی» را به‌عنوان مزد رسالت از مردم طلب کردند، ولی پاداش خواسته شده مادی نیست و با همراهی آیه‌ی ۵۷ سوره‌ی فرقان، فایده‌ی محبت خویشان حضرت به خود مردم باز می‌گردد و راهی به سوی خدا است (هدایت‌نیا، ۱۳۹۰: ۱۱۴ و ۱۱۵). بنابراین طبق آیات قرآن از بعد مزدطلبی، تبلیغ هزینه‌ای برای دریافت‌کننده‌ی پیام

نداشته و نگاه مادی برای مبلغ به عنوان پیام‌رسان، آسیب تبلیغ محسوب می‌شود. بنابراین هزینه‌های تبلیغ از این نگاه بیشتر متوجه پیام، ابزار، شیوه و شخصیت پیام‌رسان است. هر چند محتوای پیام اسلام، محتوایی غنی است ولی انتقال صحیح آن به مخاطب نیازمند مبلغانی کار بلد و برجسته است که تربیت چنین مبلغانی نیازمند هزینه‌های مادی قابل توجه از قبیل مکان آموزشی، وسایل آموزشی و حمایت آموزشی است. از طرفی همه‌ی مبلغین، قدرت دستیابی به پیام‌ها از طریق قرآن را نداشته و نیازمند دسترسی به منابع مختلف متون و معارف دینی هستند. هزینه‌های اقتصادی جهت آموزش، دسترسی به مخاطب، تثبیت و به‌روزرسانی اطلاعات مبلغ، تأمین نیازمندی‌هایی چون کتاب، مقوله‌های تشویقی و جذب‌کننده مثل برگزاری مسابقه و مراسم در مناسبت‌های دینی و ملی و خرید جوایز و اردو و... گوشه‌ای از هزینه‌های تبلیغ محسوب می‌شود. قرآن اشاره‌ی مستقیمی به هزینه‌های اقتصادی تبلیغ دین ندارد ولی شیوه‌های مختلف تبلیغی انبیای الهی را بیان نموده که اجرایی نمودن برخی از آنها توسط مبلغ، نیازمند هزینه‌های مختلف از جمله هزینه‌های اقتصادی است. از جمله می‌توان به تشکیل کادر مرکزی دعوت (آل عمران/۶۲)، هجرت برای یافتن عرصه‌های جدید دعوت (انعام/۷۶-۷۸؛ شعراء/۵۲)، مشارکت در تعمیر و ساخت اماکن مذهبی (بقره/۱۲۷)؛ تکلم به زبان‌های مختلف (ابراهیم/۴)؛ نوشتن نامه (نمل/۲۸)؛ ایجاد جوّ تفاهم و آزادی اظهار نظر (نمل/۲۲ و ۲۳)؛ جهاد<sup>۲</sup> (توبه/۲۰) و ... اشاره نمود.

امروزه دسترسی به اینترنت تقریباً برای همه‌ی افراد مالک یک گوشی همراه هوشمند حتی از نسل سوم، با سیم‌کارتی اعتباری و هزینه‌ی بسیار ناچیز ممکن شده است. افراد در قبال این هزینه‌ی اقتصادی ناچیز، خدمات گسترده‌ای را دریافت می‌کنند.

کاهش هزینه‌های اقتصادی به معنای فرصتی بدون چالش نیست و شرایط فضای مجازی هزینه‌های دیگری به مبلغ تحمیل می‌کند که توجه به آنها در جهت موفقیت در رساندن پیام به مخاطب بسیار اهمیت دارد.

گسترش روز افزون خدمات اینترنت و زمان زیادی که افراد به‌طور روزانه در فضای مجازی می‌گذرانند، تهدیدی برای جسم و روان آنها محسوب می‌شود (کمال، ۱۳۹۶: ۱۵-۲۱). آسیب‌های متعدد اجتماعی از جمله حیازدایی و انحرافات مختلف ایجاد می‌نماید (کمال، ۱۳۹۶، ۲۵-۲۲). امکانات آموزشی و محیطی برای نشر محتوای تبلیغی فراهم می‌کند. اما مطالعات نشان می‌دهد، کسانی که متن‌ها را به‌صورت سنتی مطالعه می‌کنند، نسبت به کسانی که متن‌های دیجیتال را با پیوندهای تزئین شده مطالعه می‌کنند، درک بیشتری از محتوا دارند. زمانی که حواس، پی در پی منحرف و گسیخته می‌شود، آنچه‌ان که ضمن حضور در فضای آنلاین اتفاق می‌افتد، مغز قادر به برقرار کردن تماس‌های عصبی قدرتمند و گسترده که موجب عمق‌بخشی و تمایز اندیشه‌ورزی می‌شود، نیست. بنابراین افراد تنها به واحد پردازش علائمی تبدیل می‌شوند که به سرعت، تکه‌های پراکنده‌ی اطلاعات را به حافظه‌ی کوتاه مدت خود وارد و از آن خارج می‌کنند (نیکلاس کار، ۱۳۹۲:

<sup>۲</sup> در قرآن از جهاد با دو واژه «جهاد» و «قتال» یاد شده است. واژه «قتال» به نوع خاصی از جهاد گفته می‌شود که همان جنگیدن با دشمن ظاهری است. واژه «جهاد» تمام اقسام جهاد و شیوه‌های مبارزه با دشمن، اعم از دشمن ظاهری و دشمن باطنی یعنی نفس و جهاد با جان آن را شامل می‌شود. مگر اینکه قرینه‌ای در کلام موجود باشد که آن را به نوع خاصی از جهاد، اختصاص دهد (خرم‌آبادی، ۱۳۶۸: ۱۴ و ۱۵)

۷۴-۷۷). دانشمندان کشف کرده‌اند که ساختار سلولی مغز انسان به سرعت خود را با ابزاری که فرد استفاده می‌کند، سازگار می‌نماید؛ با تغییر عادت‌های مغز، قدرت درک افراد نسبت به متن مورد مطالعه در فضای حقیقی نیز کاهش می‌یابد (همان: ۷۶).

بنابراین، کاهش عمق درک در مطالعه، پیام‌گیر و پیام‌گذار را با چالش بسیار جدی و مهم؛ کاهش عمق درک سطح آگاهی و علم، کاهش میزان تفکر و تفکر عمیق روبرو می‌نماید که به تبع، اثرگذاری هم کاهش پیدا می‌کند؛ که این، نوعی دور شدن از سیر تربیتی قرآنی است. قرآن، الگوی شناخت در همه چیز را علم و یقین دانسته و ظن و گمان، حدس و تخمین یا شک و احتمال (اسراء/۳۶؛ نور/۱۵؛ یوسف/۱۰۸) قابل اعتماد نیست (مکارم شیرازی، ۱۳۷۴: ۱۱۶).

ناشناختگی (گمنامی) مطابق معنای عرف و لغوی، به معنای فعالیت نمودن شخص بدون آشکار شدن نام است. از آنجایی که ناشناختگی می‌تواند آزادی عقیده و بیان را پیش برد، امکان اظهارنظرها را تقویت کند، در مواقعی که افراد از ترس انتقام یا تمسخر، تمایل یا جسارت اظهار نظر به گونه‌ای دیگر در مباحث را ندارند، اهمیت دارد. همچنین اینکه ناشناختگی می‌تواند افرادی که نیاز جدی به کمک دارند را در دسترس قرار دهد، خصوصاً در مسائلی که به لحاظ اجتماعی و آبرویی، حساسیت برانگیز است؛ مواردی همچون خشونت‌های خانوادگی، ترس از ابتلا به بیماری‌هایی خاص، مسائل احساسی و یا تفکرات مایل به خودکشی و امثال موارد بیان شده می‌تواند نشان از اهمیت آن باشد. در تمامی موارد نامبرده، ارزش ناشناختگی در قابلیت بی‌نام بودن قرار ندارد بلکه در ایجاد امکان فعالیت و مشارکت؛ در عین حال دور از دسترس و غیرقابل دستیابی بودن است (ثقه الاسلامی، ۱۳۸۸: ۱۳۵-۱۳۸).

در دنیای کامپیوتری شده‌ی امروز با چنین سیستم اطلاعاتی، بی‌نامی به تنهایی برای ناشناختگی کافی نیست. تکنولوژی اطلاعات، امکان ردیابی افراد را با روش‌هایی بدیع و بی‌سابقه فراهم نموده است. افراد تقریباً در تمامی شئون زندگی تحت نظارت هستند. اطلاعات درباره‌ی افراد گردآوری، ذخیره، تحلیل و گاهی اوقات به اشتراک گذاشته می‌شود (همان: ۱۳۷-۱۴۸).

همچنین قابلیت گراف و تحلیل اطلاعات شبکه‌ی ارتباطی، برای مالک شبکه این امکان را فراهم می‌کند که علاوه بر شخصیت‌شناسی، اطلاعاتی نسبت به شیوه‌ی عملکرد فرد در آینده داشته باشد. مالکان می‌توانند بر مبنای اطلاعات به دست آمده، روابط افراد در شبکه‌های ارتباطی را مورد تحلیل و بررسی قرار داده و به نقاط ضعف و قوت پی ببرند. این اطلاعات می‌تواند در تحلیل روانشناسی، جامعه‌شناسی، اقتصاد، سیاست، فرهنگ و... کشور کاربرد داشته باشد و بر اساس اطلاعات به دست آمده برای کشور در هدف‌های گوناگون برنامه‌ریزی کرد. گردانندگان این فضا می‌توانند در محیط تحت مدیریت خود، اقدام به جریان‌سازی یا جلوگیری از یک جریان داشته باشند (کهنوند، ۱۳۹۶: ۸۴-۸۵). با تحلیل اطلاعات و شناخت مدیران فضای مجازی از وضعیت کشور مقابل، علاوه بر استفاده یا به بیانی سوءاستفاده از اطلاعاتی که رایگان در اختیار دارند، شناسایی نخبگان هر عرصه، ساده و دسترسی به آنها ممکن می‌شود، راه نفوذ به کشور مقابل در عرصه‌های مختلف هموار می‌شود، جریاناتی ایجاد یا سرکوب می‌شود، کما اینکه ردیابی و ترور شخصیت‌های مؤثر از همین طریق ممکن می‌شود.

از سوی دیگر با توجه به مولفه‌های امنیت در اسلام یعنی حاکمیت خداوند متعال، استقلال حکومت

اسلامی و مسلمانان و اتحاد امت و سرزمین اسلامی، به صورت «حالت و وضعیتی که انسان بتواند با داشتن اعتقادی درست و پایندی عملی به آن جهت رسیدن به کمال مطلوبش عمل نماید» تعریف می‌شود (حسینی، ۱۳۹۶: ۱۸-۲۱) و توجه به اینکه به هم زدن امنیت یک جامعه، بزرگترین گناهی است که کسی مرتکب آن می‌شود (خامنه‌ای، ۱۳۹۰: ۲۳) و فضای مجازی تا حد زیادی موجبات ناامنی برای افراد و ملت‌ها را فراهم نموده است، تهدید امنیت توسط این فضا بدیهی است. زمانی که از امنیت فضای مجازی صحبت می‌شود، غالباً به «هک» اطلاعات، آن هم در بعد فردی اشاره شده و به امنیت ملی کمتر توجه می‌شود. گذشته از آن در صورت توجه به این بعد، به تهدیدهای وابستگی دارایی‌های ملی در حوزه‌ی فاوا به دشمن از جمله اطلاعات، سخت‌افزار، نرم‌افزار، شبکه و... بسنده می‌شود. بدون اینکه توجه شود قلمرو سرزمینی جمهوری اسلامی ایران محدود به مرزهای جغرافیایی نیست. فضای مجازی، مجموعه‌ی نظام‌های اجتماعی است که از تعامل افراد انسانی بر بستر شبکه شکل می‌گیرد و تهدید اصلی علیه امنیت فضای مجازی در حوزه‌ی نظام‌های اجتماعی بر آمده از فاوا است. با توجه به نفوذ روز افزون فضای مجازی در روابط و نظام‌های اجتماعی، این تهدید روز به روز پر رنگتر می‌شود. به بیانی فضای مجازی بستری فراهم نموده تا حاکمیت و امنیت ملی همه‌ی آن نظام‌های اجتماعی برآمده از فضای مجازی در معرض آسیب قرار گیرد (آزادی، ۱۳۹۷: ۱۶۴-۱۶۸) و همه‌ی این موارد، تهدیداتی با هزینه‌های بسیار گزاف است.

انتقادهای ناامیدکننده، پرداختن به یکدیگر و تهمت و اهانت و توهین وحدت‌شکن، افراط و تفریط در انتقال اوضاع منفی، رواج بدگویی و بردن آبروی مؤمن، پرداختن به حواشی، آمار بی‌پایه، دروغ، نسبت دروغ، تخریب چهره‌های ماندگار، کتمان موفقیت‌ها، مبالغه در کاستی و ضعف و ناموفقی، بهمن اطلاعات نادرست، انحراف جوانان از طریق شبهه‌افکنی، اقتدارشکنی کشور، بمباران افکار جوانان (بیانات: ۲۲/۵؛ ۹۷؛ ۲۵/۳/۹۷؛ ۲۰/۳/۹۷؛ ۷/۳/۹۷؛ ۶/۱۰/۹۶؛ ۱/۳/۹۶؛ ۲۰/۲/۹۶) و... تا حد زیادی امنیت افراد در زمینه‌های مختلف را به مخاطره انداخته است و تبلیغ در فضای ناامن و برای کاربرانی که احساس ناامنی دارند کاری بس دشوار است و نیاز به برنامه‌ریزی و مهارت‌های ویژه و هزینه‌های قابل توجهی دارد.

اصولاً در فضای مجازی محدودیتی در دسترسی افراد مختلف تعریف نشده است. همه‌ی افراد از هر سن و جنس و صنف و کشور و نژاد و... در هر نوع استفاده‌ای از این فضا آزادند. البته ممکن است فیلترینگ در سطح خرد انجام شود (موحدنسب، ۱۳۹۷: ۹۹) ولی با وجود نرم‌افزارهای رایگان فیلترشکن و عدم فیلترینگ‌های جدی در برخی کشورها از جمله ایران، در عمل می‌توان ادعا کرد بیشتر افراد به همه‌ی چیزهایی که حاکم و مدیر این فضا اجازه‌ی دسترسی داده‌اند، دسترسی دارند. مغلطه‌ی «همه‌ی افراد حق دارند به همه چیز دسترسی داشته باشند» حداقل با ارزش‌های اسلامی هماهنگی ندارد. همه حق استفاده از منافع و بهره‌های فضای مجازی را دارند ولی این به معنای «حق این است که همه به همه چیز در فضای مجازی دسترسی داشته باشند» نیست (بیانات: ۱/۳/۹۶: برداشت آزاد). این دسترسی‌ها برای مخاطبان مختلف بدون هیچگونه مرزبندی و محدودیت، تبلیغ دین را به فرایندی بسیار پیچیده و با روند بسیار کند تبدیل می‌کند.

## ۳.۲ گستره جغرافیایی

هدف در تبلیغ، اثرگذاری بر گیرنده‌ی پیام و قانع کردن او در پذیرش پیام مورد نظر است. هر چه تعداد مخاطب بیشتر باشد، پیام مورد نظر به افراد بیشتری انتقال داده می‌شود، بنابراین درصد احتمال افرادی که پیام را می‌پذیرند، بیشتر و پیام‌رسان به هدف خود نزدیکتر می‌شود. هر چه گستره‌ی مکانی یا همان جغرافیایی افزایش پیدا کند، احتمال وجود افراد و رسیدن پیام به افراد بیشتر، افزایش پیدا می‌کند. بنابراین، افزایش گستره‌ی مکانی در صورت افزایش دسترسی به افراد بیشتر، امتیاز تبلیغ محسوب می‌شود.

خداوند متعال در قرآن مجید درباره‌ی پیامبر بزرگوار اسلام حضرت محمد مصطفی (صلی الله علیه وآله و سلم) سه بار با صراحت بیان می‌کند:

«هُوَ الَّذِي أَرْسَلَ رَسُولَهُ بِالْهُدَىٰ وَ دِينِ الْحَقِّ لِيُظْهِرَهُ عَلَى الدِّينِ كُلِّهِ» (توبه/۳۳؛ فتح/۲۸؛ صف/۹): او

کسی است که پیامبرش را همراه با هدایت و دین حق فرستاد تا آن را بر همه‌ی ادیان پیروز کند. این آیه به صراحت اعلام می‌دارد که غرض از بعثت و ارسال پیامبر گرامی اسلام (صلی الله علیه وآله و سلم) این بوده است که دین او -اسلام- جهان‌گیر شود. آن حضرت از طرف خداوند متعال، مأمور بود که همه‌ی مردم جهان را به اسلام دعوت کند تا اگر جهان‌گیر شدن این دین در زمان حیات خود وی تحقق نیافت، دست‌کم مقدمات جهانی شدنش برای آینده فراهم گردد و آن حضرت، این مأموریت سنگین را به بهترین شکل ممکن انجام داد.

ارسال مبلغ، استفاده از مکان مناسب مثل مقام ابراهیم در کنار خانه‌ی کعبه، زمان مناسب مثل حج و ماه‌های حرام، زمانی که کافران مانع فعالیت حضرت می‌شدند، روش‌های بین‌المللی تبلیغ حضرت محسوب می‌شود (اکبری؛ اولیایی، ۱۳۹۷: ۱۱۷-۱۱۹).

علاوه بر آیه‌ی فوق، قرآن در آیات متعدد به صراحت به جهانی بودن اسلام اشاره و تأکید دارد. آیاتی که قرآن را هدایت‌کننده همه‌ی مردم و برای همه‌ی زمان‌ها معرفی می‌کند (تکویر/۲۷)؛ آیاتی که همه‌ی انسان‌ها را مورد خطاب خود قرار می‌دهد (حج/۱)؛ آیاتی که رسالت پیامبر اسلام را متوجه همه‌ی انسان‌ها می‌داند و هم دایره‌ی رسالت و ابلاغ او را جهانی می‌داند و هم او را پیامبر جهانیان معرفی می‌کند (انبیاء/۱۰۷، انعام/۱۹، نساء/۷۹، اعراف/۱۵۸، سبأ/۲۸)؛ آیاتی که بر ضرورت تسلیم و پذیرش اهل کتاب نسبت به دعوت پیامبر تأکید دارد و آنها را ملزم به پذیرش اسلام می‌کند (آل عمران/۱۱۰)؛ آیاتی که آموزه‌های جهانی اسلام را بیان می‌کند که سنخ جهانی بودن و فرامرزی بودن این احکام، تبیین‌کننده‌ی جهانی بودن اسلام است همانند توحید و معاد و... (آل عمران/۶۴).

ناگفته نماند جهانی‌سازی اسلام به معنای جهانی شدن علم، عقلانیت، معنویت، عدالت، امنیت، رشد و تعالی انسان‌ها در سراسر جهان است و منظور از آن، یکسان‌سازی مردم نیست. طبق قرآن افراد بشر به‌طور ذاتی دارای اختلافات اساسی در زمینه‌ی نژاد و ساختار فکری و عاطفی و ذوق‌های فردی و انتخاب هستند و این منافاتی با جهانی‌سازی اسلام ندارد (نکوئی سامانی، ۱۳۸۶: صص ۲۵۸ و ۲۷۲). طبق مطالب بیان شده، گستره‌ی جغرافیایی تبلیغ اسلام از همان ابتدای بعثت رسول خدا (صلی الله علیه و آله) به وسعت جهان در هر زمان و مکان است.



برای نشان دادن درصدی از جمعیت یک کشور یا منطقه که کاربر اینترنت هستند از شاخصی به نام «ضریب نفوذ اینترنت» استفاده می‌شود. روش‌های مختلفی برای محاسبه‌ی این شاخص به کار می‌رود که تفاوت آنها در نحوه‌ی تعریف «کاربر اینترنت» (به معنای کسی از اینترنت استفاده می‌کند) است. به‌عنوان نمونه در ایران کاربر اینترنت کسی دانسته می‌شود که در یک سال گذشته دست کم یک بار به اینترنت وصل شده و از آن استفاده کرده باشد. این شاخص به نوعی بیانگر گستره‌ی جغرافیایی کاربران است. این شاخص یکی از شاخص‌های مهم جهانی در حوزه‌ی فناوری اطلاعات است که برای رتبه‌بندی پیشرفت کشورها مورد استفاده قرار می‌گیرد.

از زمان ابداع اینترنت در سال ۱۹۶۸ در وزارت دفاع آمریکا تا اواسط سال ۱۹۹۴ سه میلیون کامپیوتر در دنیا به اینترنت وصل شدند اما طبق آمارهای ارائه شده ۵۱ درصد کاربران فعلی اینترنت در دنیا بعد از سال ۱۹۹۵ وارد این محیط شده‌اند (<http://www.iribnews.ir/009bSE>). طبق آخرین آمار ارائه شده از سوی سازمان تنظیم مقررات ارتباطات (رگولاتوری) تا پایان خرداد ماه سال ۹۷، تعداد مشترکان اینترنت باندهن به ۷۲ میلیون و ۹۴۱ هزار و ۸۷۷ نفر رسیده است؛ به‌عبارت دیگر ضریب نفوذ اینترنت در ایران به ۸۸/۸۶ درصد رسیده است. براین اساس ضریب نفوذ اینترنت پهن‌بند ثابت ۱۵/۷۰ درصد و ضریب نفوذ اینترنت موبایل ۷۳/۱۶ درصد عنوان شده است (<http://www.ion.ir>)<sup>۳</sup>. مقایسه‌ی آمارهای سال ۱۳۹۲ و ۱۳۹۷ از سرعت رشد بالای ضریب نفوذ اینترنت و همگانی شدن آن خبر می‌دهد.

طبق آیات قرآن، دین اسلام از ابتدای ظهور، افقی جهانی برای همه‌ی زمان‌ها داشته است. ضریب نفوذ اینترنت همگانی و جهانی شدن آن را تأیید می‌کند. بنابراین اینترنت با فراهم نمودن دسترسی افراد به فضای مجازی می‌تواند ابزار رساندن پیامی جهانی برای کاربران فضای مجازی در گستره‌ی جغرافیایی به وسعت جهان باشد. چنین فرصت بی‌نظیری در تحقق آرمان‌های اسلام هیچ وقت در طول تاریخ، فراروی مبلغان نبوده است. البته این فرصت بی‌نظیر دقیقاً با چالش‌های گستردگی مخاطب روبرو است که به تعدادی از آنها اشاره شد.

## ۴.۲ عرضه و دسترسی به پیام در اشکال مختلف در کمترین زمان

اولین رکن موفقیت تبلیغ، پیام است. به جز ویژگی‌های محتوایی چون قابلیت اثبات و استدلال، هماهنگی با احساسات عالی و دقیق بشر و انطباق با نیازها و انگیزه‌های زندگی بشر (ناجی، ۱۳۷۰: صص ۲۳-۲۶)، هر عامل دیگری که در گسترش و اثرگذاری پیام مؤثر باشد، نقش به‌سزایی در موفقیت تبلیغ دارد. در عرصه‌ی اطلاعاتی حاضر، در نظر گرفتن این عوامل اهمیت بیشتری دارد و به موفقیت پیام و به دنبال آن تبلیغ کمک می‌کند.

دقت و بررسی در آیات قرآن نشان می‌دهد، قرآن به‌عنوان پیامی الهی که از سوی خالق، توسط انسانی برگزیده برای هدایت انسان‌ها نازل شده است.

نگاهی به دامنه و تعداد شیوه‌های تبلیغی الگوهای قرآنی، بیان‌کننده‌ی تنوع بی‌نظیر روش‌های اسوه‌های

<sup>۳</sup>طبق جدیدترین آمار، ایسنا آن را به نقل از سازمان تنظیم مقررات و ارتباطات رادیویی تا پایان سال ۱۴۰۰، ۱۲۷ درصد اعلام نموده است. (ضریب نفوذ اینترنت در ایران به ۱۲۷ درصد رسید، ایسنا، <https://www.isna.ir/news>)



قرآنی است تا جایی که می‌توان مجموع شیوه‌های استخراج شده از سیره‌ی دعوت اسوه‌های قرآنی را حدود ۲۴۰ مورد دانست. البته با توجه به اینکه قرآن در صدد روایت کامل روش‌های هدایتی و حکایت جامع سیره‌ی تبلیغی نیست، این موارد تنها برگزیده‌ها و نمونه‌هایی از مؤثرترین و بهترین شیوه‌های انبیاء و اولیاء با توجه به شرایط محیط و مخاطب است (عباسی‌مقدم، ۱۳۷۹: صص ۴۳ و ۴۴). علاوه بر آن، خود قرآن در انتقال پیام خود از شیوه‌های متنوع و متفاوتی استفاده کرده است. به نظر می‌رسد از آنجایی که تبلیغ به دنبال هدایت باور و در پی آن تغییر رفتار در افراد است، همه‌ی این شیوه‌ها در روند تأثیر بر احساس و ادراک و شناخت قابل جمع است. شناخت، عالی‌ترین سطح پردازش ذهنی اطلاعات است و پس از آن احساس و ادراک قرار دارند (برانو، ۱۳۷۹: صص ۲۸ و ۲۳۹ و ۲۴۰). در بین شیوه‌های تبلیغی مطرح شده در قرآن، به بیانی سمعی (زمر/۱۸)، بصری (انعام/۹۹)، سمعی - بصری (بقره/۲۶۰)، چندرسانه‌ای (مائده/۳۱) و توازن به چشم می‌خورد (سبأ/۱۵) که نشان از تنوع و به‌کارگیری احساسات متفاوت برای ایجاد درک و شناخت در مخاطب است.

علاوه بر آن سایر ویژگی‌های قرآن نیز در جذابیت پیام قرآن برای مخاطب نقش به‌سزایی دارد. زیبایی‌های زبان وحی و کلام قرآنی، سطحی آشکار و چشم‌نواز از مجموعه‌ی زیبایی‌های آن است. توجه به این زیبایی و اقرار به برتری‌های لفظی قرآن وابسته به ایمان نیست و فقط مؤمنان به دلیل ایمان به قرآن، لفظ و زبان آن را زیبا نمی‌بینند بلکه این زیبایی در ذات این اسلوب بیانی است و فهم و درک آن به مؤمنان و گروندگان اختصاص ندارد. قرآن، خود نیز به گوش دادن‌های مخفیانه و به‌رمندی از زیبایی و جذابیت قرآن توسط مشرکان سخن گفته است (هود/۵).

شاخص‌هایی چون آهنگ و موسیقی کلام وحی، انسجام و روانی آواها و تصویرگری‌های قرآن در موضوعات مختلف زبان قرآن را به اوج زیبایی می‌رساند (بابایی، ۱۳۸۹: صص ۳۰-۳۸).

از طرفی هر انسان منصفی که کمترین آشنایی با تاریخ و تعالیم اسلام داشته باشد، می‌داند که اسلام و قرآن همه‌ی ملت‌ها را به آیین، معارف و مقررات خود دعوت کرده و هیچ فرد، گروه، ملت و نژادی را استثناء نکرده است و اینکه برخی افراد با تمسک به برخی آیات مدعی شده‌اند که قرآن، جهانی و جاودانی نیست و ویژه‌ی مردم عرب شبه‌جزیره‌ی عربستان در زمان نزول قرآن است، حرف صحیحی نیست. تأمل و تدبر در آیاتی که در شبهه‌ی محدودیت دعوت قرآن مورد استناد قرار می‌گیرند (به‌عنوان مثال رک شعراء/۲۱۴ و بقره/۲) نشان می‌دهد، این آیات بیانگر مراحل دعوت پیامبر (صلی الله علیه و آله و سلم) و مسئولیت‌های ویژه‌ی ایشان یا شرایط بهره‌مندی از قرآن است و هیچ دلالتی بر اختصاصی بودن آن ندارد و دعوت اسلام و قرآن جهانی است (مصباح یزدی، ۱۳۸۶، ج ۲، صص ۲۷۶-۲۸۵) و تذکری برای همه‌ی جهانیان (انعام/۹۰). یکی از مهم‌ترین شیوه‌هایی که قرآن برای هدایت انسان به آن پرداخته است، چهره‌نمایی از اقوام و ملل و روشن نمودن چگونگی‌های امت‌های پیشین است. رفتارهای فردی و اجتماعی، برخوردهای آنان با پیامبران و صالحان و فرجام زندگی آنها را به دقت بیان نموده و در نهایت افراد را به عبرت‌آموزی از زندگی اجتماعی و فردی آنها دعوت کرده است (جلالی‌کندری، ۱۳۸۹: صص ۱۱ و ۱۲). بدون احتساب آیات با موضوع تورات، بیش از دو‌سوم آیه از قرآن در مورد قوم یهود و نصاری است (اسرار، ۱۳۸۷: ۴۳). قرآن از هیچ قومی به‌اندازه‌ی یهود و بنی‌اسرائیل سخن نگفته است. در آیات متعددی ضمن تشریح روحیات، اخلاق و عملکرد

فاسد آنان به سرزنش و انتقاد از ایشان پرداخته است (کریمیان، ۱۳۸۶).

کتاب و نمونه، دو رکن موفقیت هر مکتبی است. از نظر اسلام، قرآن نسخه‌ی هدایت و اسوه‌ها داروی هدایت هستند. مهمترین شیوه‌ی تبلیغ عملی، تبلیغ الگویی است و از این جهت که اسوه‌ها بشرند، اهمیت به‌سزایی دارد (عباسی‌مقدم، ۱۳۷۹: ۴۸-۵۵). قرآن با بیان صفات و معیارهای اسوه‌ها، معرفی اسوه‌ها و نمونه‌های عینی هدایت و سفارش به تلاش برای اسوه شدن، بر ضرورت تبلیغ الگویی، تأکید دارد. بررسی اسوه‌های بشری معرفی شده در قرآن، نشان از تنوع قابل توجه اسوه‌ها و شیوه‌های آنان است. این اسوه‌ها گاهی از چهره‌های مثبت است (ممتحنه/۴) و گاهی از چهره‌های منفی (اعراف/۸۳)، گاهی زن است (تحریم/۱۰-۱۲) و گاهی مرد (مریم/۵۱)، گاهی یک نفر را بیان می‌کند (عاقر/۲۸)، گاهی بیش از یک نفر (انعام/۸۵)؛ گاهی یک پیامبر است (مریم/۵۱) گاهی غیر پیامبر (لقمان/۱۲)؛ گاهی معصوم است (احزاب/۲۱) و گاهی غیر معصوم (یس/۲۰)؛ گاهی الگوی همه‌جانبه است (احزاب/۲۱) و گاهی یک یا چند جانبه (هود/۷۵)؛ گاهی نام اسوه ذکر شده است (ص/۴۸) و گاهی بدون ذکر نام (تحریم/۱۱)؛ گاهی اسوه یک نفر است (فتح/۲۹) گاهی جماعت و گروه (آل عمران/۱۱۰) و موارد دیگر.

شاید مهم‌ترین نتیجه‌ای که بتوان از این بررسی به‌دست آورد این است که تأکید قرآن بر بیان پیامی با هدف هدایت است و نسبت به شرایط و افراد و جاودانگی و جهانی و فرامکانی و فرا زمانی بودن قرآن از شیوه‌ها و الگوهای بشری به اشکال مختلف استفاده می‌کند.

در شرح اصالت محتوای قرآن، تنها به این بسنده می‌شود که قرآن پیامی است که هم فکر و عقل را در مرحله‌ی شناخت هدایت کرده، بینش درست و یقینی به انسان می‌بخشد، هم به دل روشنی و آگاهی داده، آن را برای پذیرش حق آماده می‌کند و هم روح را گام به گام در سیر صعودی، همراهی و راهنمایی می‌کند تا درجات عالی کمال را پیموده و به هدف نهایی برسد (مصباح یزدی، ۱۳۸۶، ج ۱: ۶۴-۷۱).

با ظهور و گسترش صنعت ارتباطات و به‌دنبال آن، اینترنت به‌عنوان شبکه‌ی ارتباطی و اطلاعاتی جهانی، فضای مجازی ایجاد شد. فضایی همیشه در دسترس که محدودیت‌های مکانی و زمانی ندارد، بدون مرز و «همه جا حاضر» که امکان جریان داشتن فرد در فضا، در مرزهای نامرئی بین فضای حقیقی و مجازی را فراهم نموده است. فضایی با ماهیت جذاب، متنوع و دارای نوآوری که امکان انتقال سریع محتوا به روش‌های متنوع به سراسر جهان، را فراهم کرده است. در این فضا، امکان ایجاد چالش‌های فکری و فرهنگی، جمع‌آوری اطلاعات از مکاتب و مذاهب مختلف و تولید رسانه‌های چند جانبه در تمام ابعاد وجود دارد. حجم تولید و ذخیره‌ی اطلاعات در این فضا تا حدی است که تنها در تارگه و ویکی‌پدیا، ۲۰ میلیون مقاله، به ۲۷۰ زبان زنده‌ی دنیا وجود دارد (موحدی علوی، ۱۳۹۵: ۱۵۷-۱۸۲). در حال حاضر تقریباً تمامی انواع وسایل الکتریکی قابلیت اتصال به اینترنت را دارند (پوگ، ۱۳۸۹: ۱۲). میلیون‌ها انسان بدون نیاز به دانستن نکات فنی، از خدمات اینترنت استفاده می‌کنند (شرکت شبکه‌ی اصفهان، ۱۳۸۲: ۱۷) و از اینترنت برای کسب اطلاعات در موضوعات مختلف بهره می‌برند (خمر، ۱۳۹۰: ۱۲۶) اطلاعات و محتوای خود را با دیگران به اشتراک می‌گذارند و پیام خود را در قالب‌های مختلف چندرسانه‌ای در معرض بازدید مخاطب قرار می‌دهند. عرضه‌ی پیام در فضای مجازی برای دو نقطه‌ی مختلف جهان در حد یک کلیک زمان می‌برد.

بنابراین قرآن، پیامی الهی، فرا زمانی و فرامکانی است که محدود به فرد یا افراد خاصی نیست. در شیوه

و گفتار خود جذابیت و تنوع دارد و از ابتدای نزول تا کنون مشتاقان خود را از جای جای نقاط جهان هدایت نموده است. انسان را با دیدگاه سایر مکاتب آشنا نموده و با معرفی دشمنان و ویژگی‌های آنان، موانع هدایت را برطرف و راه رسیدن به سعادت را هموار می‌کند.

در مقابل، فضای مجازی، فضایی با گسترش و امکان دسترسی جهانی است، تولید و عرضه و تبدیل محتوا به اشکال متنوع و شیوه‌های جذاب در این محیط ممکن شده است. به دلیل فعالیت مکاتب مختلف در این فضا امکان دسترسی به موقع به نظرات آنها وجود دارد. اطلاع از دیدگاه مکاتب نسبت به یکدیگر، دقت در عرضه‌ی محتوا و به دنبال آن، موفقیت بیشتر در رسیدن پیام به مخاطب حق‌پذیر را آسانتر نموده است با توجه به اینکه مبلغ، محتوای خود را از قرآن و سیره دریافت می‌کند، چنین محیطی با داشتن سایر ویژگی‌های لازم، فرصتی کم‌نظیر در موفقیت پیام است و مبلغ را به موفقیت تبلیغی نزدیکتر می‌کند.

اگرچه محتوا، در تبلیغ اسلامی، غنی و بر مبنای ثقلین است ولی فضای مجازی در شرایط حاضر می‌تواند این محتوا را با چالش‌های مختلفی روبرو نماید.

طراحان و مالکان فضای مجازی با روش‌های گوناگون، کاربران را به چرخه‌ی تسخیری فضای مجازی جذب می‌کنند. سپس با در نظر گرفتن راهبرد، طرح و برنامه‌های متنوع و گوناگون، به لایه‌های ذهنی و شخصیتی افراد نفوذ کرده و در گام نهایی به صورت محسوس و نامحسوس بر کاربران اثر گذاشته و در نگرش و گرایش و کنش آنان موجب تغییر می‌شوند و برای سه مرحله‌ی جذب، نفوذ و تغییرات برنامه‌ریزی داشته و روش‌های دقیق و حساب شده به کار گرفته‌اند. هدف نهایی مالکان این فضا این است بشر را به ربات‌هایی تبدیل کنند که بتوان به راحتی بر آنها حکومت کرد. تولیدات مالکان این فضا با تکیه بر اصل جذاب بودن تهیه شده و جذابیتی کاذب در نظر گرفته شده است. در اینگونه تولیدات به علت نپرداختن به فطریات انسانی و پرداختن به جذابیت‌های نفسانی، سدی در مسیر رشد و تعالی انسان‌ها پدیدار نموده و او را به سوی حیوانیت پیش می‌برد (کهوند، ۱۳۹۶: ۱۱۹، ۱۲۴، ۱۲۵، ۱۹۱). بنابراین محتوایی که در نقطه‌ی مقابل این اهداف قرار دارد و برای رشد و تعالی انسان تلاش می‌کند، در فضایی بدون اختیار حاکمیت و اجرایی به شدت دچار چالش است، به ویژه اگر بدون برنامه و اهداف کلان بوده و گذرا و فردی صورت گیرد. بنابراین جذب و دسترسی مخاطب به محتوای تبلیغی به دلیل هوشمندی محیط به شدت کاهش می‌یابد.

گذشته از آن ضعف مبلغ در شناخت محیط، شیوه‌ی تولید محتوا و ارائه‌ی آن در فضای مجازی، اثر مهمی بر محتوای تبلیغ در فضای مجازی دارد. مبلغی که بدون آشنایی با محیط وارد این فضا می‌شود ممکن است خود را با چالش‌های متعددی درگیر نماید. اگر محتوای تولیدی او، ویژگی‌های لازم و متناسب با این فضا را نداشته باشد مثلاً به سئو (SEO) توجهی نداشته، محیط فعالیت خود را درست انتخاب ننماید، بدون برنامه و هدف دست به اقدام بزند، به دلیل ضعف علمی از محتوای ضعیف استفاده کند، به جای تولید، به کپی محتوای موجود اقدام کند، مطالب غیر مستند و یا نامناسب برای این فضا ارائه دهد، از اهداف تبلیغی خود نه تنها دور شده بلکه بالعکس در مواردی ضد تبلیغ خواهد بود. عدم آشنایی با شیوه‌های اقناع مخاطب، عدم مهارت و خلاقیت در ارائه‌ی پیام، تفکیک قائل نشدن بین انواع شبکه‌های ارتباطی در این فضا شبکه‌های اجتماعی، پیام‌رسان، مبتنی بر تصویر و... در نظر نداشتن نوع موضوع و انتشار هر محتوای دینی، آشنا نبودن به زبان‌های مختلف، محتوای غیر مستند، شبهه و پاسخ ضعیف موارد دیگری از ضعف مبلغ در این فضا است که موجب به

چالش کشیدن محتوا می‌شود. به بیان دیگر، مبلغ بدون در نظر گرفتن محتوای موجود، ناخواسته در رقابتی قرار می‌گیرد که به دلیل ضعف مهارت، پیام غنی او با استقبال مخاطب مواجه نشده و اثر خود را از دست می‌دهد و عملاً پیام با شکست مواجه می‌شود.

حجم اطلاعات در فضای مجازی رو به بی‌نهایت پیش می‌رود. اطلاعات جدید در هر ساعتی از شبانه‌روز در قالب‌های مختلف به مخاطب عرضه می‌شود. به دلیل سرعت بالای جابجایی، بازنشر و نقل و انتقال اطلاعات و بستر مناسب دسترسی به انواع محیط‌ها، مطالب بسیار کوتاه شده و در کمتر از چند جمله یا توسط یک تصویر یا کلیپ کوتاه به مخاطب عرضه می‌شود. اطلاعات بدون نظم و طبقه‌بندی در عرصه‌های مختلف ذخیره شده‌اند. بسیاری از اطلاعات، اعتبارسنجی نشده و کاربران با مخلوطی از اطلاعات درست و غلط روبرو هستند (حسینی، حق پناه، ۱۳۹۴: ۱۴۴ و ۱۲۱).

استعمار فرانو علاوه بر اینکه با انحصار رسانه‌ای، فضایی ایجاد نموده که کاربران تنها اطلاعاتی را که صاحبان رسانه اراده کرده‌اند می‌بینند و از دیدن اطلاعات حیاتی و یا مهم دیگر محروم‌اند، از طریق ارائه‌ی حجم اطلاعات گسترده، فرصت تحلیل و تجزیه را از کاربر گرفته و از طریق انبوه‌سازی اطلاعات بی‌فایده و غیر اولویت‌دار، ذهن افراد را مشغول و آنها را از امور مهم باز داشته است. حجم وسیعی از اطلاعات ناقص و آمیخته به باطل، جهت‌دار، همراه با مغالطه و پنهان کردن بخشی از واقعیت، قرار دادن اطلاعات نامناسب در اختیار کاربر که دیدن و شنیدن و دانستن آن برای کاربر صحیح نیست، مثلاً صحنه‌های خشونت داعش برای کودکان و یا مواجه شدن با تصاویر غیراخلاقی، سرقت، خشونت، تهمت، شایعه، خرافه، شیطان‌پرستی، شبهات مختلف و... برای همه‌ی افراد، دسترسی به محتوای سالم را کاهش می‌دهد (کهوند، ۱۳۹۶: ۱۵۳-۱۵۵).

گذشته از آن، کارکرد محیط بر پیام اثر می‌گذارد. دین رسانه‌ای، دینی است کاملاً بی‌آزار که می‌توان به آن عمل نکرد و در واقع افراد دچار غفلتی مدرن هستند (صادقیان، ۱۳۹۱: ۵۱-۵۳). غفلتی که نه تنها نسبت به زمان خود بخیل نیستند، با جود بسیار، درهم و دینار خود را برای اتلاف ثانیه‌های عمر هزینه می‌کنند. بنابراین در این فضا، با هجوم سیل آسا و بی‌وقفه‌ی سیل وسیعی از اطلاعات غیر مفید روبرو است که علاوه بر ایجاد حس آگاهی کاذب و با اطلاع بودن در مخاطب، قدرت تحلیل دقیق و حتی مطالعه و مشاهده بسیاری از اطلاعات را از مخاطب می‌گیرد و رقابت اطلاعاتی برای جذب مخاطب و ارائه‌ی محتوا، کاری بس دشوار و سنگین است.

## ۵.۲ تسهیل روابط بین پیام‌گذار و پیام‌گیران

از جمله بزرگ‌ترین پیشرفت‌های بشر، ارتباط بین فردی است. راز بسیاری از موفقیت‌ها از جمله خانوادگی و کاری، داشتن مهارت برقراری ارتباط است (بولتن، بیتا: ۲۴-۲۸). قدم اول در تبلیغ و رساندن پیام، برقراری ارتباط با پیام‌گیر است (قزائتی، ۱۳۷۷: ۴۹). در واقع در انواع تبلیغ، پیام‌گذار با ایجاد زمینه‌های مناسب در خود و مخاطب و استفاده از ابزار مناسب، در پی ایجاد یک رابطه‌ی مناسب با پیام‌گیر برای رساندن پیام خود به او است. قرآن کریم در تفسیری که از روابط انسان دارد، به هفت نوع رابطه اشاره می‌کند؛ رابطه‌ی انسان با خدا (اعلی/۱)، خود (مائده/۱۰۵)، دیگران (انفال/۱)، طبیعت (فصلت/۵۳)، جامعه (انفال/۲۵)، شیطان (ص/۸۲ و ۸۳) و تاریخ (رعد/۱۱). مهمترین رابطه‌ی انسان، رابطه‌ی او با خدا است و اساس همه‌ی روابط

است. انسان هر رابطه‌ای با دیگران برقرار می‌سازد باید بر مبنای این رابطه باشد (نصری، ۱۳۸۵، صص ۳۳۱-۳۵۲). قرآن نه تنها رابطه‌های هفتگانه مبلغ را تأیید، بلکه بر ضرورت آن اشاره دارد.

اینترنت در ابتدا توسط آژانس تحقیقات پیشرفته‌ی آمریکا برای اهداف نظامی پایه‌گذاری شد. سپس به مرور مراحل مختلفی را پشت سر گذاشت تا جایی که امروزه امکان برقراری ارتباطات بین افراد و گروه‌های یک اجتماع با افراد و گروه‌های جوامع دیگر را مهیا نموده است (قیصریان، ۱۳۹۲: ۳۴-۳۶). در واقع فضای مجازی با گستردگی مکانی و فراگیری و شکستن مرزهای جغرافیایی انواع روابط بین افراد را تا حد یک کلیک، ساده نموده است (خالدی، ۱۳۹۵: ۳۳-۳۵). شرایط ویژه‌ای که ارتباط بین‌فردی با سایر کاربران، برون فردی با رایانه و ابزارهای هوشمند و نرم‌افزارها، درون فردی با تفکر و تعقل یا اثرپذیری از شیوه‌های اقناع موجود در فضای مجازی، ارتباط شبکه‌ای از طریق اینترنت و شبکه‌های اجتماعی و پست الکترونیک، ارتباط گروهی با گروه‌های مختلف دوستان، هم‌رشته‌ای‌ها، هم‌صنفی‌ها و ارتباط هم‌سخنانه از طریق آغاز گفتگوهای اینترنتی، ارتباط غیرکلامی توسط نوشتار و تصویر و... را ممکن نموده است.

اگرچه فضای مجازی تا حد زیادی در تسهیل روابط بین پیام‌گیر و پیام‌گذار مؤثر است ولی در مقابل روابط افراد را با چالش‌هایی جدی روبرو می‌نماید.

تسهیل‌گری به تنهایی امری همیشه ممدوح و پسندیده نیست (مهدی‌پور، ۱۳۹۷: ۹۵) و می‌تواند تهدیدی برای ارتباطات واقعی و چهره به چهره باشد. افزایش ارتباط از این طریق به مرور زمان از آنجایی که ارتباط شخصی با تمرین آموخته می‌شود، موجب کم شدن توانایی تعامل شخصی فرد می‌شود. با رقم خوردن نوعی «بی‌سوادی ارتباطی» در جایی که فرد نیازمند و مجبور به برقراری ارتباط متقابل و رودرو باشد به شدت دچار مشکل می‌شود (فزان رامون، بی تا). از طرف دیگر می‌توان گفت در این فضا امکان ایجاد روابطی غیرحقیقی فراهم شده است. دانشمندان علوم ارتباطات معتقدند در یک رابطه‌ی حقیقی رو در رو، ۵۵ درصد از معنایی که فرد به طرف مقابل خود منتقل می‌کند از طریق حرکات جسمانی و ژست بدن هنگام ادای کلمات است و ۳۸ درصد از معنایی نیز از طریق لحن و آهنگ صدا به مخاطب منتقل می‌شوند و خود کلمات تنها ۷ درصد از معنایی را با خود حمل می‌کنند. بنابراین در دنیای مجازی، بی‌جسمی، بار اصلی انتقال مفاهیم از طریق کلمات انجام می‌شود. همین مسأله ممکن است باعث انواع متعدد سوءتفاهم در درک معنای کلمات از طرف مخاطبین با سن و سواد و میزان اطلاعات عمومی متفاوت شود (حسینی و حق‌پناه، ۱۳۹۴: ۱۳۵).

پژوهشگران دانشگاه کارنگی ملون، نتیجه‌ی پژوهش‌های خود در بررسی اینترنت به‌عنوان وسیله‌ای ارتباطی را بر خلاف معمول و پیش‌بینی نشده دانسته و اعلام نموده‌اند استفاده‌ی بیشتر از اینترنت، موجب کاهش برقراری ارتباط با اعضای خانواده، کم شدن گستره‌ی اجتماعی و افزایش نومیدی و انزوا می‌شود (دریفوس، ۱۳۸۹: ۴-۷). از دیدگاه قرآن، همه‌ی روابط، ساختاری دو بُعدی دارند، در بعد طولی با خداوند و در بعد عرضی با سایر مخلوقات، مبنای نظری شبکه‌ها، تنها به یکی از این دو بعد اشاره دارد. حذف رابطه‌ی دائمی با خداوند در نگاه ارتباطی شبکه‌ها، اثرات جبران‌ناپذیری دارد. ناظر دائمی اعمال و رفتار فرد در حوزه‌ی اجتماع، حس حضور خداوند است. حذف مفهوم ارتباط با خالق از روابط اجتماعی، نقص و کمبودی در این روابط ایجاد می‌کند که هیچ راهکار جایگزینی برای رفع آن یافت نمی‌شود (عرفانیان، ۱۳۹۵: ۸۵). مطابق موازین اسلامی، بر روابط اجتماعی، نوعی سطح‌بندی و اولویت‌گذاری حاکم است. روابط ایمانی



(آل عمران/۱۰۳؛ فتح/۲۹)، خانوادگی (اسراء/۲۳) و خویشاوندی (محمد/۲۲ و ۲۳)، همسایگی و رابطه با محرومان (نساء/۳۶) اولویت‌های روابط در نگاه دینی است (عرفانیان، ۱۳۹۵: ۸۴).  
متأسفانه در فضای مجازی نه تنها اولویت این روابط نادیده گرفته می‌شود، بلکه نوع استفاده از این فضا، این روابط را در فضای حقیقی هم دچار اشکال نموده است.

برقراری ارتباط با غیرمسلمانان برای دعوت به اسلام از دیدگاه قرآن ممانعتی ندارد (توبه/۶) و حتی اجازه‌ی حضور در جوامع اسلامی و مطالعه و بررسی به آنان داده شده است (مکارم شیرازی و دیگران، ۱۳۷۴، ج ۷: ۲۹۳). البته این به معنای روابط آزاد با غیرمسلمانان و بدون رعایت اصول قرآنی نیست. قرآن همانطور که به رعایت عدالت (مائده/۴۲ و ۸)، نیکی با اهل پیمان (ممتحنه/۸ و ۹)، امانت‌داری و پابندی به عهد و پیمان (توبه/۴) و جدال احسن (عنکبوت/۴۶) با اهل کتاب در دعوت به توحید و اسلام، سفارش می‌کند (اسماعیلی شورباخورلو، ۱۳۸۳: ۸۳)، در مقابل ممانعت‌هایی را گوشزد می‌نماید؛ طبق آیه‌ی ۱۴۱ نساء، هر طرح، عهدنامه، رفت و آمد و قراردادی که راه نفوذ کفار بر مسلمانان را باز کند حرام است و مسلمانان باید در تمام جهات سیاسی، نظامی، اقتصادی و فرهنگی از استقلال کامل برخوردار باشند. البته روابط و کسب اطلاع و آموزش دیدن و تبادل فرهنگی و اقتصادی، اگر سبب سلطه‌ی کفار و ذلت مؤمنان نباشد مانعی ندارد (قرآنی، ۱۳۸۳، ج ۲: ۴۱۴). طبق آیات قرآن، در برابر دشمن دینی (مکتبی) نباید از هدف کوتاه آمد (جوادی آملی، ۱۳۹۱: ۳۲۷ و ۳۲۸).

چون مؤمن با خدای قادر پیوسته است و همه چیز را از خدا می‌داند و از او کمک می‌طلبد، عزت خود را در برابر دشمن دینی حفظ می‌کند، در سختی‌ها ضمن تدبیر و تحمل، دست نیاز به سوی دشمن دراز نمی‌کند. از همگونی با دشمن در زمینه‌های مختلف از جمله فرهنگ پرهیز می‌کند. مؤمن می‌داند یکی از روش‌های دشمن در دستیابی به اهداف خود این است که بتواند فرهنگ و روش خود را در زمینه‌های مختلف بین مسلمانان رواج دهد. برای دفع شر دشمن دعا می‌کند. در حاکمیت دشمنان برای حفظ جان و ناموس خود تقیه می‌نماید، به جز جایی که اساس دین در خطر است (جوادی آملی، ۱۳۹۱: ۳۲۸-۳۳۱). هوشمندانه در خود آمادگی همه‌جانبه در برابر ترفندهای دشمن ایجاد می‌نماید (انفال/۶۰) و دقیقاً بر خلاف آنچه در فضای مجازی در حال وقوع است.

در اسلام رابطه با جنس مخالف، شرایط و ضوابطی دارد. لذت و شهوت جنسی چه از طریق کلام، چه از طریق نگاه و لمس و نوشتار، جز برای همسران ممنوع و حرام است. از دیدگاه قرآن بهره‌وری جنسی ویژه‌ی همسران است و از زنا نهی و با زناکار به شدت برخورد شده است (مومنون/۵ و ۶؛ اسراء/۳۲؛ نور/۲).  
به‌طور کلی قرآن برای برقراری روابط مختلف، اعم از رابطه‌ی فرهنگی، سیاسی، کاری، تجاری و... ضوابطی را در جهت هدف خلقت تعیین نموده است. بر خلاف آن، در فضای مجازی تنها اصل، برقراری رابطه، تعریف شده است و اصولاً تابع ضابطه و مقررات خاصی، مخصوصاً بر پایه‌ی آموزه‌های قرآنی نیست (رضایی، ۱۳۹۱: ۱۲۷-۱۲۹).

در ارتباط مجازی، امکان تخیلی و غیر واقع‌بینانه بودن همه چیز وجود دارد. محیطی غیر قابل اعتماد است که حتی به صوت و تصویر افراد نمی‌توان اطمینان کرد. قابلیت اثرگذاری شدید روحی و ذهنی دارد و ممکن است افراد دچار درگیری‌های عاطفی و... شوند. ارتباطات بدون شناخت دقیق و حتی نسبی اتفاق



می‌افتد. بیشتر اتفاقات بر مبنای تخیل شکل می‌گیرد تا شناخت. جاذبه‌های صوتی، نوشتاری و تصویری آن تخیل افراد را لذت‌بخش می‌کند تا جایی که جایگزین روابط حقیقی می‌شود. لذت‌های تخیلی به مرور زمان مشکلات روحی ایجاد می‌کند که گاهی تا حالت‌های جنون‌آمیز، خودآزاری و حتی خودکشی پیش می‌رود (رضایی، ۱۶۶: ۱۳۹۱-۱۶۹).

غالباً آنچه در این فضا افراد را به هم نزدیک می‌کند «منافع» است. منفعت‌محوری در روابط، در تعارض با دیدگاه‌های روابط اجتماعی در قرآن است. تأکید اسلام بر ارتباط با افراد نیازمند و مستضعف و دستگیری از افراد مختلف و... به روشنی این تعارض را مشخص می‌کند. در مکتب حاکمان و مجریان این فضا، انسان هر چه در رسیدن به لذت‌های نفسانی، محدودیت کمتری داشته باشد آزادتر است ولی اسلام اگر چه آزادی‌های اجتماعی را به رسمیت شناخته است، اما این آزادی‌ها چارچوب مشخص دارد. در اسلام «اختیار» به معنای آزادی عمل انسان در عقیده و عمل است ولی نه از حقوق انسان بلکه نعمتی عطا شده از خداوند، در جهت رشد او است که استفاده‌ی صحیح از آن موجب رستگاری و استفاده‌ی نادرست موجب شقاوت است. از نگاه قرآن وجود اختیار، مجوز رفتارهای خارج از چارچوب الهی و دینی نیست (عرفانیان، ۱۳۹۵: ۸۸-۸۹). بنابراین طبق فرهنگ قرآن، روابط فضای مجازی غالباً بر اساس آموزه‌های علمی، اخلاقی و با رعایت موازین قانونی و شرعی اتفاق نمی‌افتد.

### ۳ نتیجه‌گیری

اینترنت، بستر عظیمی را برای تشکیل بزرگترین شبکه‌های ارتباطی جهان، بین افراد گوناگون، فراهم نموده است. مبلغان دینی که در هر زمان و مکانی موظف به انتقال آموزه‌های دینی به مردم و تغییر رفتار در آنها هستند می‌توانند از این فرصت در جهت اهداف درست خود استفاده نمایند. استفاده‌ی درست و موفقیت‌آمیز از این امکانات، وابسته به نگاه واقع‌بینانه و شناخت صحیح فرصت‌ها و چالش‌های پیش‌روی فعالیت تبلیغی در این محیط است. مبلغ ضمن نیاز به شناخت فضای مجازی و ابعاد تبلیغ از دیدگاه قرآن و ایجاد ویژگی‌های لازم در خود، لازم است بدانند هر فرصتی در این فضا چالش‌هایی به همراه دارد. بالاترین مصداق عددی که قرآن از آن نامبرده است هزار سال پنجاه سال کمتر در مورد دعوت حضرت نوح علیه‌السلام و صد هزار جمعیت قوم کافری در بازگشت دوم یونس علیه‌السلام است که با پذیرش دعوت الهی، عذاب از آنها برداشته شد. دقت در تفاسیر این آیات و ضمیمه کردن آیات دیگر، نشان‌دهنده‌ی اهمیت تعداد مخاطب در تبلیغ و تأییدکننده‌ی فرصت گسترگی مخاطب در فضای مجازی است.

قرآن، رسالت انبیاء را بدون درخواست مزد از مخاطب معرفی می‌کند ولی اجرای شیوه‌های تبلیغی انبیاء در قرآن هزینه‌هایی در بردارد که فضای مجازی تا حد زیادی این هزینه‌ها را کاهش داده است. قرآن، پیامی جهانی و با اصالت است. پیام خود را در قالب‌های گوناگون به همه‌ی مردم در همه‌ی زمان‌ها عرضه می‌کند، و فضای مجازی با ایجاد این قابلیت‌ها، فرصتی در جهت عرضه‌ی پیام در کمترین سرعت به مخاطبان سراسر جهان است. رسالت جهانی و فرامکانی و فرازمانی رسول اکرم (صلی الله علیه و آله و سلم) که قرآن بارها به آن اشاره دارد، نشان از اهمیت گستره‌ی جغرافیایی در تبلیغ است که تأییدکننده‌ی فرصت

دسترسی به گستره‌ی جغرافیایی، بدون محدودیت‌های فضای حقیقی در فضای مجازی می‌باشد. تبلیغ، بدون برقراری ارتباط منتفی است و تسهیل روابط مبلغ و پیام‌گیران، فرصت شایسته‌ای است که فضای مجازی فرا روی مبلغ قرار داده است. نگاهی واقع‌بینانه با محوریت آیات قرآن کریم، مبلغ را به این دیدگاه رهنمون می‌سازد که این فرصت‌ها در فضایی ایجاد شده است که حاکمیت آن در اختیار صهیونیسم بین‌الملل و مجریان آن - از دیدگاه قرآن، دشمن سرسخت اسلام یعنی یهود بوده - و برای رسیدن به جهانی بدون مرز، برنامه‌ریزی و هدف‌گذاری شده است. اگر مخاطبی گسترده دارد، ناهمگونی هم دارد که رعایت مقتضای حال را دشوار و دامنه‌ی اثرگذاری ضعف او را افزایش می‌دهد. تعدیل هزینه‌ها، تحمیل هزینه‌هایی چون تهدید سلامتی، کاهش درک مطالعه، تهدید امنیت و... را در پی دارد. پیام او را در محیطی هوشمند و بین‌محتوای نزدیک به بی‌نهایت و نامناسب در رسیدن به مخاطب به چالش می‌کشد و ضمن کاهش ارتباطات چهره به چهره، حرکت به سمت حذف ارتباط دائم با خداوند، افزایش اولویت‌های ناصحیح، تقویت روابط مخالف با اصول قرآنی او و مخاطبش را به انزوا و افسردگی می‌کشاند. بنابراین از آنجایی که فرصت‌های تبلیغ دین در فضای مجازی از دیدگاه قرآن با چالش‌هایی همراه است، در تأیید گفته‌ی بزرگان دین، فضای مجازی می‌تواند ابزاری باشد برای رساندن حرف درست به میلیون‌ها نفر ولی در اینکه در شرایط فعلی و برای هر مبلغی چنین ابزاری باشد جای تأمل دارد. با وضعیت فعلی و استفاده‌ی عمومی و آسیب‌های پیش‌رو، هرگونه کوتاهی برای ایجاد زمینه‌های لازم و تربیت مبلغان خلاق و با مهارت، خیانتی نابخشودنی به انقلاب و اسلام محسوب می‌شود (ر.ک جدول ۱).

### جدول ۱: جمع‌بندی

چالش	فرصت	ارکان تبلیغی
<p>ناهمگونی مخاطب</p> <ul style="list-style-type: none"> <li>دشواری رعایت مقتضای حال</li> <li>افزایش دامنه ضعف مبلغ</li> </ul>	گسترده‌گی مخاطب	مخاطب (پیامگیر و پیامرسان) گستره جغرافیایی
<p>تحمیل هزینه‌های غیراقتصادی</p> <ul style="list-style-type: none"> <li>تهدید سلامتی کاربران</li> <li>کاهش درک مطالعه</li> <li>تصور خام از ناشناخته بودن و خطر نخبگان</li> <li>تهدید امنیت</li> <li>دسترسی‌های نامعقول</li> <li>لزوم آرایش نظامی</li> </ul>	تعدیل هزینه‌های اقتصادی	هزینه‌های انتقال پیام
<p>هوشمند بودن محیط</p> <p>ضعف مبلغ در استفاده از محیط و تولید محتوا</p> <p>رقابتی سخت و نابرابر با محتوای موجود</p>	عرضه و دسترسی به پیام در اشکال مختلف در کمترین زمان	پیام
<p>تهدید ارتباطات واقعی و چهره به چهره</p> <p>حرکت به سمت حذف مفهوم ارتباط دائمی با خدا</p> <p>افزایش اولویت‌های ناصحیح در ارتباطات</p> <p>تقویت روابط مخالف با اصول قرآنی</p>	تسهیل روابط	روابط پیامگیر و پیامرسان

فضای مجازی می‌تواند ابزاری باشد برای رساندن حرف درست به میلیون‌ها نفر ولی در اینکه در شرایط فعلی و برای هر مبلغی ابزاری مفید باشد جای تأمل دارد. با وضعیت فعلی و استفاده عمومی و آسیب‌های پیش رو، هرگونه کوتاهی برای ایجاد زمینه‌های لازم و تربیت مبلغان خلاق و با مهارت، خیانتی نابخشودنی به انقلاب و اسلام محسوب می‌شود.

## مراجع

- [۱] احمدی میانجی، علی، مکاتیب الرسول ص (نعمان بصیری)، ج ۲، قم، دارالحدیث، ۱۴۱۹.
- [۲] اسرار، مصطفی، دانستنی‌های قرآن، چاپ اول، تهران: چوگان، ۱۳۸۷.
- [۳] اکبری، کمال؛ اولیایی، احمد، تبلیغ بین‌المللی اسلام، چاپ اول، کرج: ارمان حیات، ۱۳۹۷.
- [۴] بابایی، رضا، نگاهی به اعجاز بیانی قرآن، چاپ سوم، تهران، کانون اندیشه‌ی جوان، ۱۳۸۳.
- [۵] برانو، فرانک فرهنگ توصیفی روانشناسی (ترجمه فرزانه طاهری و مهشید یاسائی)، چاپ اول، تهران، قیام، ۱۳۷۹.
- [۶] بولتن، رابرت، روان‌شناسی روابط انسانی (ترجمه حمیدرضا سهرابی)، چاپ اول، تهران، رشد، بی‌تا.
- [۷] پوگ، دیوید خودآموز اینترنت (ترجمه مهدی گلستانی‌نسب)، چاپ دوم، تهران: صناعی شه‌میرزادی، ۱۳۸۹.
- [۸] ثقة‌الاسلامی، علیرضا، چالش‌های اخلاقی در عصر ارتباطات، چاپ اول، تهران، چاپار، ۱۳۸۸.
- [۹] جلالی‌کندری، سهیلا، یهود شناخت (تأملی بر اندیشه عمل و فرجام بنی‌اسرائیل از نگاه قرآن)، چاپ اول، تهران، حامیان آزادی قدس، ۱۳۸۹.
- [۱۰] جوادی آملی، عبدالله، مفاتیح‌الحیة (تنظیم محمدحسین فلاح‌زاده و دیگران)، چاپ نود و دو، قم، اسراء، ۱۳۹۱.
- [۱۱] حسینی، بشیر؛ حق‌پناه، حسین، ۱۵۰ هشتگ، چاپ اول، تهران، رواق اندیشه، ۱۳۹۴.

- [۱۲] حسینی، تقی، فضای مجازی از دیدگاه آیات و روایات، چاپ اول، اصفهان، سیمای فلق، ۱۳۹۶.
- [۱۳] خُمر، غلامعلی، کاربرد کامپیوتر و اینترنت در علوم جغرافیایی، کشاورزی، منابع طبیعی، چاپ سوم، تهران: خدمات نشر کیان رایانه سبز، ۱۳۹۰.
- [۱۴] خامنه‌ای، سید علی، وظایف در شرایط فتنه، چاپ سوم، تهران: قدر ولایت، ۱۳۹۰.
- [۱۵] داورپناه، ابوالفضل، انوارالعرفان فی تفسیر القرآن، ج ۱، چاپ اول، تهران، صدر، ۱۳۷۵.
- [۱۶] رزاقی، احمد، تبلیغات دینی: ابزار و شیوه‌ها، چاپ اول، قم: سازمان تبلیغات اسلامی، ۱۳۷۷.
- [۱۷] رضایی اصفهانی، محمد علی و جمعی پژوهشگران قرآنی، روابط دختر و پسر، چاپ اول، قم، انتشارات پژوهش‌های تفسیر و علوم قرآن، ۱۳۹۱.
- [۱۸] سبحانی، جعفر، فروغ ابدیت، چاپ بیست و ششم، قم: بوستان کتاب، ۱۳۸۵.
- [۱۹] شرکت شبکه اصفهان، اینترنت بستری جهانی، چاپ اول، اصفهان: مهر قائم (عج)، ۱۳۸۲.
- [۲۰] صادقیان، رسول، معرفت امام زمان علیه‌السلام، بی‌جا، اصفهان، بنیاد فرهنگی حضرت مهدی موعود علیه‌السلام، ۱۳۹۱.
- [۲۱] طاهری خرم‌آبادی، حسن، جهاد در قرآن، چاپ اول، تهران، پیام آزادی، ۱۳۶۸.
- [۲۲] طباطبایی، محمدحسین، المیزان فی تفسیر القرآن، ج ۱۱ و ۱۲ و ۱۴ و ۱۶ و ۱۷ و چاپ پنجم، قم، دفتر انتشارات جامعه مدرسین قم، ۱۴۱۷ ق.
- [۲۳] عباسی مقدم، مصطفی، اسوه‌های تبلیغی و شیوه‌های تبلیغی آنان، چاپ اول، قم: دفتر تبلیغات اسلامی، ۱۳۷۹.
- [۲۴] فهیمی، اکبر، شیوه‌های پیامبر اعظم در دعوت به اسلام، چاپ اول، قم: نشر هاجر، ۱۳۸۶.
- [۲۵] قرائتی، محسن، تفسیر نور، ج ۶، چاپ یازدهم، تهران، درس‌هایی از قرآن، ۱۳۸۳.
- [۲۶] قرائتی، قرآن و تبلیغ، چاپ اول، تهران: مرکز درس‌هایی از قرآن، ۱۳۷۷.
- [۲۷] کریمیان، احمد، یهود و صهیونیسم، چاپ دوم، قم، بوستان کتاب، ۱۳۸۶.
- [۲۸] کمال، حامد؛ کمال، محمد، ناگفته‌های فضای مجازی، چاپ دهم، اصفهان، سیمای فلق، ۱۳۹۶.
- [۲۹] محمد، کهوند، شبکه‌ی عنکبوتی، روش‌های جذب، نفوذ و تأثیرگذاری در فضای مجازی، چاپ دوم، قم: ذکری، ۱۳۹۶.
- [۳۰] مدفربز، پل، اینترنت ۲۰۱۱ (ترجمه همتا بیداریان، الهام مقاده عابد، زهرا بهرامیان)، چاپ اول، تهران: آتی‌نگر، ۱۳۸۹.
- [۳۱] مصباح یزدی، محمد تقی، قرآن‌شناسی، (تحقیق غلامعلی عزیزی کیا) ج ۱ و ۲، چاپ اول، قم، موسسه آموزشی و پژوهشی امام خمینی ره، ۱۳۸۶.
- [۳۲] مطهری، احمد، جهاد در راه خدا و ابعاد گوناگون آن، چاپ اول، موسسه در راه حق، قم، ۱۳۷۲.
- [۳۳] مکارم شیرازی، ناصر، و دیگران، تفسیر نمونه، ج ۱۰ و ۱۲ چاپ اول، تهران: دارالکتب الاسلامیه، ۱۳۷۴.
- [۳۴] موحدنسب، حامد، اخلاق در فضای مجازی، چاپ دوم، کرج: تلاوت آرامش، ۱۳۹۷.
- [۳۵] مهدی‌پور، فرشاد، ما و مسائل فضای مجازی، چاپ اول، تهران، سروش، ۱۳۹۶.
- [۳۶] ناجی، محمدرضا، شرایط موفقیت تبلیغ، چاپ اول، قم: سازمان تبلیغات اسلامی، بی‌تا.
- [۳۷] نصری، عبدالله، مبانی انسان‌شناسی در قرآن، چاپ ششم، بی‌جا، موسسه فرهنگی دانش و اندیشه معاصر، ۱۳۸۵.
- [۳۸] نیکلاس کار، «آیا اینترنت ما را کودن‌تر می‌کند؟» قاب جادو (آسیب‌های اینترنت و تلویزیون در غرب)، چاپ اول، رضایی مریم؛ پیشوایی، فریده، تهران، موسسه انتشارات نشر، ۱۳۹۲.

- [۳۹] هدایت نیا، فرج الله، شیوه‌های تبلیغ در قرآن، چاپ دوم، قم: ذوی القربی، ۱۳۹۰.
- [۴۰] آزادی، جواد، «امنیت سایبری یا امنیت فضای مجازی؟»، تأملات رشد، ۱۳۹۷، ش ۱، صص ۱۶۴-۱۶۸
- [۴۱] سلطانی شورباخورلو، اسماعیل، «روابط اخلاقی و اجتماعی مسلمانان و غیرمسلمانان از دیدگاه قرآن»، معرفت، ۱۳۸۳، ۸۳، پرتال جامع علوم انسانی.
- [۴۲] فزان رامون - کورتس، «آیا اینترنت روابط واقعی را تهدید می‌کند؟»، قاب جادو (آسیب‌های اینترنت و تلویزیون در غرب)، چاپ اول، رضایی مریم؛ پیشوایی، فریده، تهران، موسسه انتشارات نشر، ۱۳۹۲، صص ۹۸-۹۹.
- [۴۳] موحدی علوی، علیرضا، «فضای مجازی، فرصت‌ها، تهدیدها، چالش‌ها و پیامدهای پیش‌رو در مقابله با تهدیدات نرم»، فصلنامه‌ی مطالعات عملیات روانی، ۱۳۹۵، ش ۴۴، صص ۱۵۷-۱۸۲.
- [۴۴] خالدی، سمانه، دین در دنیای مجازی، دانشگاه باقرالعلوم علیه السلام، قم، کارشناسی ارشد، ۱۳۹۵
- [۴۵] عرفانیان، ابوالفضل، بررسی نقادانه شبکه‌های اجتماعی مجازی از منظر آموزه‌های اجتماعی قرآن کریم و استخراج دلالت‌های آن در تربیت اجتماعی، دانشگاه علامه طباطبایی، تهران، کارشناسی ارشد، ۱۳۹۵.
- [۴۶] عزت‌اله‌زاده، علی، بررسی موانع تبلیغ دین در فضای مجازی، مطالعه موردی بر اساس دیدگاه فعالان مرتبط در استان آذربایجان غربی، دانشگاه بین‌المللی امام رضا علیه السلام، مشهد، کارشناسی ارشد، ۱۳۹۵.
- [۴۷] قیصریان، محمدعلی، بررسی ظرفیت‌ها و چالش‌های شبکه‌های اجتماعی مجازی در زمینه‌ی تبلیغ دین و ارائه‌ی الگوی مناسب، دانشگاه باقرالعلوم علیه السلام، قم، ۱۳۹۲.
- [۴۸] ضریب نفوذ اینترنت و کاهش شکاف دیجیتال، خبرگزاری صدا و سیما، ۱۴۰۱/۷/۲۳، ۱۹:۵۵.
- <https://www.iribnews.ir/009bSE>
- [۴۹] ضریب نفوذ اینترنت به ۸۹ درصد رسید، ایران آنلاین، ۱۳۹۸/۴/۱۳ (این خبر از آرشیو سطح وب حذف شده است ولی لینک در اسناد پایان‌نامه‌ی این مقاله ثبت است).
- [۵۰] گزارش دیجیتال سال ۲۰۱۸، وی آر سوشال (We Are Social)، بازیابی شده در ۱۴۰۱/۷/۲۳، ۲۰:۳۳.
- <https://www.wearesocial.com/blog/2018/01/global-digital-report-2018>





## بررسی دلایل عدم موفقیت شبکه‌های اجتماعی داخلی

سید جواد شریف شیخ‌الاسلامی<sup>۱</sup>

دکترای آینده‌پژوهی، پژوهشگر پژوهشگاه فضای مجازی  
javad.sharif866@gmail.com

### چکیده

وقایع چند سال اخیر نشان می‌دهد که ایجاد شبکه‌های اجتماعی داخلی ابتدائاً نتوانست مانع از ایجاد تغییرات فرهنگی در جامعه شود و در ثانی کاربران حتی در صورتی که از این شبکه‌ها استفاده می‌کردند، اما حضور شبکه‌های خارجی در هندسه ارتباطی مردم ایران بیشتر بود. این مقاله به دنبال کشف دلایل شکست و عدم استقبال مخاطبان از شبکه‌های اجتماعی داخلی است. روش پژوهش خبرگانی بوده و در مصاحبه با ۱۲ متخصص این حوزه، با استفاده از سه روش «استخوان ماهی»، «تحلیل لایه‌ای علت‌ها» و «سلسله‌مراتبی» تلاش شده تا پاسخی برای پرسش مطرح شده در این تحقیق به دست آید. نتایج به دست آمده از تحلیل سلسله‌مراتبی یافته‌های روش استخوان ماهی و تحلیل لایه‌ای علت‌ها نشان می‌دهد که در روش اول به ترتیب: «مدیریت کلان دولتی، مدیریت شبکه‌های اجتماعی، مخاطبین و رقبا» مهم‌ترین عوامل تاثیرگذار در شرایط کنونی بر عدم استقبال از شبکه‌های اجتماعی داخلی است و در روش دوم به ترتیب: «لایه اسطوره، سیستمی گفتمانی و لیتانی» بیشترین تأثیر را در شکست شبکه‌های اجتماعی داخلی داشته‌اند. بیشترین مشکل به دلیل عدم «باور» به سرویس‌ها و پلتفرم‌های داخلی در عموم جامعه و مسئولین، «عدم حمایت» مناسب سیاست‌گذاران و مجریان از شبکه‌های داخلی است.

**کلمات کلیدی:** شبکه‌های اجتماعی داخلی، تحلیل لایه‌ای علت‌ها، پیام‌رسان داخلی، استخوان ماهی.

## ۱ مقدمه

با گسترش استفاده از اینترنت بین اقشار مختلف، استقبال کاربران از شبکه‌های اجتماعی روز به روز در حال افزایش است. شبکه‌های اجتماعی، ساختارهای اجتماعی متشکل از افراد و گروه‌ها و ارتباطات بین آنهاست. افراد و گروه‌های عضو شبکه، گره‌های شبکه را تشکیل می‌دهند و وابستگی‌های بین این افراد مانند دوستی، خویشاوندی، تجارت، علایق مشترک و غیره روابط بین گره‌ها را تشکیل می‌دهد (ثقفی، ۱۳۹۸). بر اساس آمارهای ارائه شده در ژانویه سال ۲۰۱۶، کل جمعیت جهان ۳.۷ میلیارد نفر بوده است (کفی، ۲۰۱۶). در سال ۲۰۱۷ از این تعداد، بیش از ۷.۳ میلیارد نفر کاربر اینترنت و ۳.۲ میلیارد نفر کاربر فعال شبکه‌های

اجتماعی بوده‌اند. بر این اساس، بخش زیادی از فعالیت روزانه‌ی افراد در شبکه‌های اجتماعی رخ می‌دهد (IOS، ۲۰۱۷) و این امر شبکه‌های اجتماعی را به بستری برای توسعه کلان‌داده تبدیل نموده است. با توجه به حجم استقبال از شبکه‌های اجتماعی به خصوص در طیف نسل جوان، این پایگاه‌ها نقش بسیار مهمی در تحولات سیاسی و اجتماعی دارند و زمینه‌ای جدید در ایجاد مجموعه‌های جمعی با خاستگاه‌های اجتماعی مجازی فراهم می‌آورند. اهمیت این رسانه‌ها از این حیث مورد توجه قرار می‌گیرد که نسبت به محتوایی که در آن‌ها تولید می‌شود، می‌توانند تفکرات خاص و برنامه‌ریزی‌شده‌ای را به کاربر مخاطب منتقل نموده و بر طبق همین ویژگی است که به راحتی موضوع و حادثه‌های عادی را به یک بحران تبدیل می‌کنند و یا با برجسته‌سازی موضوع خاصی، افکار عمومی کاربران و مشترکان در این شبکه‌های اجتماعی را از واقعه خاصی دور و به اتفاق مدنظر متوجه می‌سازند. البته این را هم نمی‌توان نادیده گرفت که اطلاع‌رسانی خوب، صحیح و به‌موقع از طریق این شبکه‌ها می‌تواند از بروز حوادث و بحران‌های گوناگون جلوگیری نماید. شروع فعالیت شبکه‌های اجتماعی با سیستمی به شکل تابلو اعلانات<sup>۱</sup> در اواخر دهه‌ی ۸۰ میلادی بود؛ سیستمی که افراد از طریق خط تلفن به اینترنت محلی وصل می‌شدند و مطالب مختلف از این طریق بر روی فضای مجازی قرار می‌گرفت و سایر افراد متصل به این سیستم می‌توانستند از این طریق به تبادل اطلاعات بپردازند؛ اما به علت محدودیت دسترسی و پایین بودن سرعت تبادلات به موفقیت چندانی دست نیافت. با بهتر شدن سرعت و کیفیت اینترنت برای همگان در اوایل دهه ۹۰، سایتی<sup>۲</sup> راه‌اندازی گردید که هدف آن برقراری ارتباط میان دانش‌آموزان و تبادل اطلاعات و همفکری برای مناسبت‌ها، جشن‌ها و یا برنامه‌های درسی و غیر درسی بود. اگر چه این سیستم دارای محدودیت رده سنی بوده و به همین دلیل عمومیت چندانی نیافت اما تا به امروز به فعالیت خود ادامه داده و ۵۷ میلیون نفر کاربر دارد. با توجه به استقبال شدید از این سایت و علاقه کاربران به برقراری ارتباط با یکدیگر افراد زیادی تمایل به سرمایه‌گذاری در این سایت پیدا کردند. در سال ۲۰۰۳ با ورود لینکدین<sup>۳</sup> و مای‌اسپیس<sup>۴</sup> دنیای شبکه‌های مجازی شکلی کامل‌تر به خود گرفت. در مای‌اسپیس امکان تعامل میان کاربران در مقایسه با دوستدار تسهیل شد و ظرفیت این شبکه افزایش یافت و تا سال ۲۰۰۶ تبدیل به پربازدیدترین سایت در گوگل شد. لینکدین فضایی تخصصی و رسمی برای کاربران پدید آورد و دیگر خبری از بازی و یا صحبت جهت گذراندن وقت یا پیدا کردن دوستان قدیمی و جدید مطرح نبود. از طریق لینکدین رزومه‌ی افراد و شرکت‌ها به همراه سوابق، تجارب و علاقه‌مندی‌ها به اشتراک گذاشته و نیازهای کاریابی یا کارمندیابی کاربران به سادگی برطرف می‌شود. اما در سال ۲۰۰۴ فیسبوک<sup>۵</sup> به عنوان شبکه‌ای شخصی توسط مارک زاکربرگ برای دانشجویان دانشگاه هاروارد راه‌اندازی شد و طی ۴ سال توانست به سرعت از مای‌اسپیس پیشی بگیرد. علت این امر در نوع مخاطبان این دو شبکه بود، مای‌اسپیس مخاطبانی عام داشت در حالی که فیسبوک توسط دانشجویان و برای دانشجویان طراحی شده بود، قشری که بیشترین گرایش و استفاده را از ابزار ارتباطی و اینترنت در سراسر دنیا دارند و پیشروان

<sup>1</sup> Bulletin Board System (BBS)

<sup>2</sup> Classmates.com

<sup>3</sup> LinkedIn

<sup>4</sup> MySpace

<sup>5</sup> Facebook

استفاده از تکنولوژی‌های روز دنیا هستند و تا امروز بیش از ۱/۵ میلیارد نفر عضو دارد. موفقیت فیسبوک علاوه بر تمام این موارد مدیون ظرفیت بالای سایت و ابتکاراتی مثل لایک<sup>۶</sup> بود. در سال ۲۰۰۷ گوگل نیز با راه‌اندازی سیستم گوگل پلاس<sup>۷</sup> امکان به اشتراک گذاشتن تصاویر برای کاربران خود را فراهم کرد و همچنین با اضافه کردن سیستم هنگ‌اوت<sup>۸</sup> به جیمیل<sup>۹</sup> امکان برقراری ارتباط صوتی و تصویری را نیز میان کاربران خود پدید آورد. گوگل پلاس تا ژوئن ۲۰۱۴ ۲۵ میلیون بازدیدکننده دارد. با ورود موبایل‌های هوشمند، تبلت‌ها و... روش استفاده از شبکه‌های اجتماعی و برقراری ارتباط میان افراد به طور کلی دگرگون شد. در چند سال اخیر موبایل‌های هوشمند با قابلیت اتصال به اینترنت و داشتن دوربین‌هایی با کیفیت تبدیل به محبوب‌ترین و پرکاربردترین ابزار برقراری ارتباط میان مردم شده‌اند و توانسته‌اند در راستای رسیدن به ایده‌ی دهکده‌ی جهانی گامی موثر و انکارناپذیر بردارند. به وسیله اپلیکیشن‌هایی مثل اینستاگرام<sup>۱۰</sup>، اسنپ‌چت<sup>۱۱</sup> تا سال ۲۰۱۰ بیش از ۲۰ میلیارد عکس توسط کاربران در فضای مجازی قرار گرفته که بهترین آرشو از ناب‌ترین عکس‌ها در اقصی نقاط جهان را فراهم آورده است. در حال حاضر، بخش عمده‌ای از فعالیت‌ها و تعاملات اقتصادی، تجاری، فرهنگی، اجتماعی و حاکمیتی کشور، در کلیه سطوح، اعم از افراد، موسسات غیر دولتی و نهادهای دولتی و حاکمیتی، در فضای مجازی انجام می‌گیرد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود، بخشی از فضای مجازی کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند و عمده اطلاعات حیاتی و حساس کشور نیز، به این فضا منتقل و یا اساساً در این فضا شکل گرفته است. عمده فعالیت‌های رسانه‌ای در این فضا به شبکه‌های اجتماعی منتقل شده، بیشتر مبادلات مالی نیز از طریق این شبکه‌ها انجام می‌گیرد و نسبت قابل توجهی از وقت و فعالیت‌های شهروندان، صرف تعامل در این حوزه می‌گردد. سهم درآمد حاصل از کسب و کارهای شبکه‌های اجتماعی در تولید ناخالص ملی افزایش چشمگیر یافته و از میان شاخص‌های تعیین‌شده برای سنجش میزان توسعه‌یافتگی کشور، شاخص‌های حوزه فضای مجازی مخصوصاً شبکه‌های اجتماعی، سهم عمده‌ای را به خود اختصاص داده‌اند. بخش قابل توجهی از سرمایه‌های مادی و معنوی کشور، صرف این حوزه شده و بخش قابل توجهی از درآمدهای مادی و اکتسابات معنوی شهروندان نیز از این حوزه کسب شده و یا تاثیر عمده می‌پذیرد. به عبارت دیگر، وجوه مختلف زندگی مردم، به معنای واقعی، با این شبکه‌ها درآمیخته و هرگونه بی‌ثباتی، ناامنی و چالش، مستقیماً وجوه مختلف زندگی را متاثر خواهد نمود. (اسناد پدافند سایبری، ۱۳۹۵) با شیوع بیماری کرونا سرعت این وابستگی بیشتر شده و ابعاد دیگری از نیاز در این شبکه‌ها مشاهده می‌شود؛ ابعادی که شاید به صورت عادی چندین سال طول می‌کشید تا نیاز به آن احساس شود و بصورت فراگیر در جامعه توسعه یابد اما امروزه با ضرورت در خانه ماندن و عدم حضور در جامعه، کار را به جایی رسانده است که دستگاه‌های آموزشی مانند: آموزش عالی و آموزش و پرورش را نیازمند سرویس‌ها و خدمات این شبکه‌ها نموده است و آموزش فضای

<sup>6</sup>Like<sup>7</sup>Google+<sup>8</sup>Hangout<sup>9</sup>Gmail<sup>10</sup>Instagram<sup>11</sup>Snapchat

مجازی در بین عموم جامعه به عنوان یک آموزش رسمی جای خود را باز نموده است؛ اما این توسعه یافتگی همراه با عوارضی مانند تغییر باور در جامعه و وابستگی به عنوان مشکل فردی است که متأسفانه با نداشتن سناریو مواجهه بوده است. آینده‌ی پیش روی شبکه‌های اجتماعی که با تغییرات فناوری‌هایی مانند: واقعیت مجازی، واقعیت افزوده، هوش مصنوعی و ...؛ همراه است که شامل عوارض جدید در ابعاد مثبت و منفی است. نداشتن سناریوی مواجهه و ادامه این موضوع باعث خسارت‌های زیادی در حوزه‌های مختلف حکمرانی مجازی می‌شود که ما برای مقابله با آن هزینه‌ی زیادی اعم از هزینه‌ی اجتماعی و مالی پرداخت می‌نماییم. این هزینه به مراتب نسبت به سناریوی پیش‌دستانه بیشتر است. به دنبال تغییر فناوری در حوزه شبکه‌های اجتماعی و ورود این فناوری‌ها به جنبه‌های مختلف زندگی باعث افزایش وابستگی روزافزون متقابل کشورها و ملل شده است که این وابستگی‌ها به تغییر تعاملات در ابعاد مختلف حکمرانی منجر می‌شوند. یکی دیگر از دستاوردهای تغییرات در حوزه شبکه‌های اجتماعی تمرکززدایی جوامع و نهادها است که به دلیل گسترش فناوری اطلاعات و ارتباطات، شتاب بیشتری می‌یابد. این عدم تمرکز با تمایل روزافزون جهانی شدن به همراه حفظ ویژگی‌های ملی، قومی و فرهنگی و بسیاری عوامل دیگر همراه بوده است که گام اول آن شناخت و درک بهتر از «کاربردها»، «تغییرات» و «آینده» این شبکه‌ها در ابعاد محتوا، خدمات، کاربر، فناوری و زیرساخت برای سیاست‌گذاری دولت‌ها، فعالان کسب و کارها، سازمان‌ها و مردم است. آینده، اساساً دارای عدم قطعیت است؛ اما با این همه، آثار و رگه‌هایی از اطلاعات و واقعیت‌ها که ریشه در گذشته و اکنون دارند، می‌توانند رهنمون ما به آینده باشند. گسترش فزاینده‌ی فناوری‌های شبکه‌های اجتماعی و اتصال همه‌ی افراد جامعه به شبکه‌ی جهانی اینترنت و آثار چشمگیر آن در ابعاد زندگی فردی و اجتماعی و لزوم تاثیرات این شبکه‌ها در تغییر نظام سیاسی کشورهایی چون استونی و گرجستان موثر بوده است؛ هر چند در ایران نتوانست به تغییر نظام بینجامد اما به ما هشدار می‌دهد که آینده‌ی شبکه‌های اجتماعی عاری از حملات و تهدیدات دفاعی و امنیتی حاصل از فناوری‌های نوظهور نخواهد بود. از تجربیات دیگر این حوزه بیداری اسلامی است که توسط شبکه‌های اجتماعی ایجاد شد و توسط همین شبکه‌های اجتماعی هم مورد ضربه قرار گرفت و باعث شناسایی و دستگیری انقلابیون در مصر و چند کشور دیگر شد. در کتاب شبکه‌های خشم و امید؛ جنبش‌های اجتماعی در عصر اینترنت تالیف مانوئل کاستلز به این انقلاب‌ها و نقش قدرت شبکه پرداخته شده است. فناوری‌هایی که با پیام‌های صلح‌جویانه و یا گسترش رفاه و سلامت می‌خواهند اعتماد جهانی را به خود جلب نمایند تا به مقاصد سلطه‌جویانه‌ی خود دست یابند (کاستلز، ۲۰۱۸)؛ در این میان کشورهایی مانند چین و روسیه برای مدیریت توسعه فضای مجازی جهت جلوگیری از غافلگیری خود قوانینی را برای پذیرش فناوری‌های این حوزه وضع نموده‌اند تا بتوانند مواجهه‌ای فعال با این فناوری‌ها داشته باشند (ملائی و همکاران، ۱۳۹۷).

متأسفانه در کارهای مطالعاتی انجام‌شده در خصوص شبکه‌ای اجتماعی تاکنون بحث سناریوهای پیش‌دستانه و مواجهه فعال که از دغدغه‌های امام جامعه می‌باشد مغفول واقع شده است و استراتژی برخورد ایران با موضوعات فضای مجازی و شبکه‌های اجتماعی ضربه دوم است؛ یعنی ابتدا مسئله در حوزه حکمرانی فضای مجازی توسط کشورهای پیشرو مطرح می‌شود و بدون هیچگونه بررسی اولیه وارد کشور می‌شود و اثرات فرهنگی، اجتماعی، سیاسی و ...؛ خود را بر جامعه اعمال می‌کند؛ سپس سیاست‌گذاران جهت مواجهه با اثرات آن با مدل سلبی مانند فیلترینگ وارد عمل می‌شوند. خوب است به دنبال رفع این خلا و تغییر

استراتژی باشیم تا با بررسی اولیه نسبت به تغییرات شبکه‌های اجتماعی آینده به سناریوی پیش‌دستانه دست پیدا نموده و استراتژی ضربه دوم را به استراتژی ضربه اول بر اساس طراحی سناریو بازدارندگی و پیشنهادهایی برای سناریوهای آفندی تغییر دهیم تا دیگر شاهد انفعال در مدل مواجهه با تغییرات آینده حوزه فضای مجازی مخصوصاً بحث شبکه‌های اجتماعی نباشیم.

بر اساس نتایج به دست آمده از ۳۰ منابع بررسی شده که در بازه‌های زمانی ۲۰۱۸ تا ۲۰۱۹ بودند و با استفاده از نظرسنجی از ۱۰ خبره این حوزه دریافتیم پیش‌رانه‌های اصلی تغییرات آینده‌ی شبکه‌های اجتماعی اقتصاد و فناوری است. به عبارت دیگر دو پیش‌ران فناوری‌های آینده و اقتصاد باعث بیشترین تغییرات در شبکه‌های اجتماعی آینده هستند. این یافته‌ها نشان می‌دهند فناوری‌هایی مانند IOT، VR، هوش مصنوعی و ... در آینده باعث بهبود تعاملات میان فردی و اجتماعی در این شبکه‌ها می‌شود به شکلی که شبکه‌های اجتماعی پیوند وسیع‌تری با اجتماعات حقیقی پیدا نموده و باعث کمرنگ شدن مرز حقیقت و مجاز می‌شود و دیگر نمی‌توان میان این دو مرزی قائل شد. شبکه‌های اجتماعی آینده به واسطه فناوری‌های جدید هوشمندتر خواهند شد؛ به گونه‌ای که اطلاعات کاربران را از میان وب پیدا نموده و بررسی علاقه‌های افراد را شناسایی و ذخیره‌سازی می‌نمایند. با چنین اطلاعاتی، کاربران از تغییراتی که در اخبار رخ می‌دهند آگاه می‌شوند و از بمباران اطلاعات ناخواسته مصون می‌مانند. به این ترتیب، کاربر در پایگاهی کاملاً سفارشی رها خواهد بود و کاربران دیگر، کمترین ورود مستقیمی به قلمرو یکدیگر را نخواهند داشت (آذری و امیدوار، ۱۳۹۱). فناوری‌های آینده باعث دست‌یافتن به شبکه‌هایی با قدرت تعامل بیشتر خواهد شد؛ به گونه‌ای که کاربر با عضویت در یک شبکه اجتماعی بر اساس توافق‌نامه‌ای می‌تواند از تمام خدمات دیگر نرم‌افزارها استفاده نموده و نیازی برای خارج شدن از شبکه اجتماعی و رفتن به نرم‌افزاری مانند اسنپ را نداشته باشد. این کار در حال حاضر نیز در حد محدود انجام می‌گیرد. وجود شبکه‌های اجتماعی تخصصی در زمینه‌های فنی، پزشکی، ادبی و ... شاید در آینده به شکلی پیشرفت کند که همه فعالیت این متخصصان در همین محیط صورت پذیرد و به نوعی می‌توان گفت اشتغال آینده و مباحث اقتصادی در همین شبکه‌ها شکل می‌گیرند و نیاز کمتری به مکان و حضور فیزیکی وجود دارد. البته نمونه‌های اولیه‌ای از این شبکه‌ها امروز وجود دارد که با تلفیق با پول مجازی در حال کسب درآمد هستند و در آینده نیز می‌توانند به صورت گسترده باعث تغییر در مشاغل و سبک زندگی آینده شوند.

## ۲ چارچوب مفهومی

بخش زیادی از تحولات حوزه فناوری در دهه‌های اخیر در حوزه فناوری اطلاعات و ارتباطات رخ داده است. در قرن بیست و یکم هیچ نوآوری و اختراعی همچون دیجیتالی شدن، چنین امکانات گسترده‌ای را برای اثرگذاری بر تغییر و دگرگونی اجتماعی فراهم نکرده است (والاس، ۱۳۸۲). این حجم از تغییرات، تمایل به آینده‌نگاری تحولات، فرصت‌ها و تهدیدها برای جوامع آینده را بسیار جذاب کرده است. میل به دانستن و آماده شدن برای آینده به طور کلی، از یک شیفتگی و کنجکاوی عمومی نشأت می‌گیرد (کسمایی، ۱۳۷۰) اما در این حوزه خاص، با توجه به ابعاد اثرگذاری آن، به یک نیاز استراتژیک تبدیل شده است.



شبکه‌های اجتماعی امکان دستیابی به اطلاعات سایر افراد، آشنایی با علایق، به اشتراک‌گذاری تولیدات متنی، صوتی و تصویری و نیز تشکیل حلقه‌های کاری را امکان‌پذیر کرده است. اطلاعات انبوهی از این علایق و جهت‌گیری‌های افراد نیز در اختیار صاحبان پنل‌ها قرار می‌گیرد و قابلیت تحلیل فرامتنی جوامع را به مالکان این شبکه‌ها می‌دهد؛ چرا که نتایج تحقیقات مؤسسه پژوهش پیو (PEW) نشان می‌دهد که ۷۳ درصد کاربران اینترنت در جهان از شبکه‌های اجتماعی استفاده کرده‌اند. در بررسی‌های انجام‌شده توسط سایت آلکسا نیز از ده سایت اینترنت پربیننده در دنیا، پنج سایت را شبکه‌های اجتماعی تشکیل می‌دهند.

وب ۲ و جنبش رسانه‌های اجتماعی، انفجاری در تعاملات آنلاین و مشارکت کاربران به وجود آورده است (سرجنت و تاگ، ۲۰۱۴)؛ چرا که شبکه‌های اجتماعی امروزه صرفاً محلی برای مصرف محتوا و اطلاعات نیستند بلکه به محلی برای مشارکت سیاسی و اجتماعی تبدیل شده‌اند. با افزایش سطح تحصیلات در جوامع از یکسو و امکان مقایسه افراد با مسئولان در پی آن، مشارکت‌خواهی در اداره جوامع افزایش می‌یابد. این مشارکت‌خواهی گاه با سویه‌های سلبی و از طریق مخالفت با سیاست‌های اتخاذشده در کشور بروز می‌یابد. از دیگر دلایل محبوبیت شبکه‌های اجتماعی نیز ایجاد بستری است که در آن افراد می‌توانند دایره تعاملات اجتماعی خود را افزایش دهند. حتی می‌توانند تعاملات اجتماعی خود در فضای مجازی را متفاوت با سبکی که در جهان واقعی عمل می‌کنند، سامان دهند. کاربران امکان ارتباط با افراد از هر سن، ملیت، زبان و مذهبی را پیدا کرده و می‌توانند این ارتباط را بدون هویت اصلی خود شکل دهند. در این فضا افراد می‌توانند هویت خود را بازسازی، تضعیف یا تقویت کنند.

دقیقا به همین دلیل فرهنگی - هویتی و همچنین به دلایل امنیتی که از پی تغییرات هویتی در کشورها پدید می‌آید، بحث ایجاد شبکه‌های اجتماعی داخلی در کشورهایی مانند ایران که بر فرهنگ و ارزش‌های بومی تأکید دارد، مطرح می‌شود. در این میان بحث‌های مالی و امنیتی خاص کشور نیز مطرح است که نیاز به شبکه‌های داخلی را تشدید می‌کند. آنچه در عمل مشاهده می‌شود، اقبال کمتر مردم به شبکه‌های اجتماعی داخلی و اقبال بیشتر آنان به نمونه‌های خارجی است. این پژوهش به بررسی و تحلیل علل عدم گرایش به شبکه‌های اجتماعی داخلی می‌پردازد.

### ۳ روش تحقیق

**روش، تکنیک یا نمودار استخوان ماهی<sup>۱۲</sup>** به نام‌های متعددی شناخته شده است از قبیل نمودار ایشیکاوا، نمودار علت و معلولی، استخوان ماهی، اسکلت ماهی و چند نام دیگر. این تکنیک توسط پرفسور ایشیکاوای ژاپنی از دانشگاه توکیو ابداع و طراحی شده و به مرور جایگاه خاصی در بین مدیران و اهالی تفکر پیدا کرده است. این روش تا جایی پیش رفت که حتی نرم‌افزارهایی برای طراحی نقشه‌های ذهنی مبتنی بر این تکنیک، طراحی و تولید شد. هرچند برخی، این روش را مناسب حل مسئله نمی‌دانند و از این تکنیک فقط در گام‌هایی از فرایند حل مسئله استفاده می‌کنند. در اصل، آنها این تکنیک را تنها روشی تجزیه و تحلیلی برای بیان، شناسایی و شناخت ابعاد مسئله می‌دانند که توانایی‌های زیادی در نمایان ساختن ابعاد، اجزای مسئله و

<sup>12</sup>Fish bone Diagram



روابط بین آنها دارد و می‌تواند تصویری کلی از مسئله را در اذهان ترسیم کند که با یک نگاه، تمامی شاخه‌ها و ابعاد آن قابل درک و فهم باشد و نه روشی برای راه حل‌یابی و انتخاب راه حل‌ها و در نهایت حل مسئله! اما از طرف دیگر بسیاری هم، کاربرد این روش را بسیار گسترده‌تر می‌دانند و معتقدند که در زمینه‌هایی چون ایده‌پردازی، حل مسئله، شناسایی کلیه علل احتمالی مسئله، مسئله‌یابی، بیان مسئله، ایجاد تصویر منسجم از مسئله با ایجاد فضای بصری، روشن کردن روابط اجزای مسئله، شناخت مسئله، گزینه‌یابی، انتخاب راه حل و ... کاربرد دارد.

اما علت نام‌گذاری این فرایند حل مسئله به «استخوان ماهی»، به دلیل شکلی است که این نمودار بعد از جمع‌آوری اطلاعات به صورت بصری به خود می‌گیرد که شبیه به اسکلت ماهی است. ایشیکاوا در این فرایند، مسئله خود را روی سر ماهی می‌نویسد و اجزاء و اطلاعات مسئله به صورتی در نمودار و شاخه‌ها قرار می‌گیرند که در نهایت، تمامی اطلاعات به همراه نمودار به صورت تصویری و به شکل اسکلت ماهی ترسیم می‌شوند.

## نحوه استفاده از روش استخوان ماهی

روش انجام این تکنیک بسیار ساده است که می‌تواند در یک یا بیش از یک نشست به شکل گروهی یا فردی انجام شود ولی پیشنهاد می‌شود که این روش به صورت گروهی صورت گیرد و با بهره‌گیری از طوفان ذهنی تمامی شاخه‌ها و اجزای مسئله مورد بررسی و واکاوی قرار گیرد.

- گام اول: ابتدا مسئله را شناسایی و تعریف می‌کنیم.
- گام دوم: پس از شناسایی و تعریف مسئله، آن را داخل دایره و در سمت راست برگه کاغذ می‌نویسیم.
- گام سوم: یک خط مستقیم به سمت چپ می‌کشیم که در واقع این خط شبیه به ستون فقرات ماهی است.
- گام چهارم: حالا نوبت به تیغه‌های ماهی است که برای ترسیم آن خطوطی مورب را با زاویه ۴۵ درجه نسبت به خط ستون فقرات ماهی ترسیم می‌کنیم.
- گام پنجم: در این مرحله هر یک از تیغه‌ها را که نشان‌دهنده‌ی علت‌های اصلی مسئله است، از طریق طوفان ذهنی بررسی و واکاوی می‌کنیم و در برابر هر یک از خطوط مورب، یکی از دلایل اصلی را که منجر به بروز مسئله شده است می‌نویسیم.
- گام ششم: در این مرحله در صورتی که لازم دیدیم می‌توانیم زیرشاخه‌هایی را به تیغه‌های ماهی برای تحلیل بیشتر اضافه کنیم و می‌توانیم در هر یک از شاخه‌هایی که عوامل اصلی بروز مسئله را نشان می‌دهند، دقیق‌تر شده و عوامل جزئی‌تری که باعث بروز مسئله شده‌اند را اضافه کنیم. این روند و اضافه کردن زیرشاخه‌ها را تا هر سطحی که لازم است ادامه می‌دهیم تا در نهایت به مجموعه‌ای از عوامل تاثیرگذار که باعث ایجاد مسئله شده‌اند برسیم.

- گام هفتم: در این مرحله باید علت‌ها را اولویت‌بندی کنیم؛ به این ترتیب علت‌هایی که دارای پیچیدگی کمتری هستند نزدیک به سر ماهی و علت‌هایی که دارای پیچیدگی زیادتری هستند نزدیک به دم ماهی قرار می‌دهیم.
- گام هشتم: این مرحله؛ گام تجزیه و تحلیل تیغه‌ها یا شاخه‌ها است. در این مرحله قصد ما انتخاب علت‌هایی است که مهمتر از بقیه هستند و باید به آنها توجه بیشتری در زمان حل مسئله شود.
- گام نهم: بعد از دسته‌بندی و اولویت‌بندی می‌توانیم به رفع عوامل بروز مسئله بر مبنای اولویت‌بندی پردازیم تا در نهایت با رفع تمام عوامل بروز مسئله، بتوانیم مشکل اصلی خود را برطرف نماییم (هیگینز، ۱۳۹۲).

اما نکته‌ای که باید به آن توجه ویژه نمود این است که بررسی و حل تمام عوامل بروز یک مسئله برای زمانی که مسئله مربوطه، کوچک و ساده باشد قابل انجام است؛ اما زمانی که مشکل مورد نظر بزرگ و پیچیده می‌شود، به طور معمول، عوامل بروز آن مشکل هم زیاد می‌شوند. در چنین شرایطی اگر بر اساس نمودار استخوان ماهی، عوامل بروز مسئله را شناسایی کرده باشیم، دارای تعداد زیادی استخوان‌های ریز هستیم که هرکدام بیانگر یکی از عوامل بروز مشکل هستند؛ به طوری که از نظر زمانی و امکانات در دسترس، دیگر قادر به بررسی و حل تمام موارد پیداشده در نمودار استخوان ماهی نیستیم. در چنین وضعیتی باید به نحوی بتوانیم عوامل بروز مشکل را اولویت‌بندی کنیم و بر اساس اولویت و محدودیت‌های زمانی و امکاناتی که داریم نسبت به حل مشکل اقدام نماییم (هیگینز، ۱۳۹۲).

## روش تحلیل لایه‌ای علت‌ها

همچون تمامی روش‌هایی که در یک نظریه مطرح شده‌اند، از طریق انجام کار توسعه و تکامل یافته است. این روش از طریق ده‌ها بار به‌کارگیری واقعی آن در مجموعه‌های مختلف - سازمان‌های بین‌المللی، دانشگاه‌ها، مؤسسات، سازمان‌های غیردولتی و مراکز کسب‌وکار - تکامل یافته و در این فرایند پالایش یافته است (عنایت‌اله، ۱۳۹۵).

تحلیل لایه‌ای علت‌ها دارای چهار سطح است. سطح نخست «لیتانی» است - روندهای کمی، مشکلات و مسایلی که اغلب بنا به دلایل سیاسی در مورد آن‌ها اغراق می‌شود - (مثلاً جمعیت بیش از حد) و معمولاً توسط رسانه‌های خبری بیان می‌شود. رویدادها، موضوع و روندها به یکدیگر مرتبط نیستند و غیرمستمر به نظر می‌رسند. نتیجه‌ی آن اغلب حس ناتوانی (چه کاری می‌توانم انجام دهم؟) یا انفعال (هیچ کاری نمی‌توان انجام داد!) یا انتظار از دیگران (چرا آن‌ها کاری درباره‌ی آن انجام نمی‌دهند؟) است. این سطح متعارف اکثر تحقیقات آینده‌پژوهی است که می‌تواند به سرعت منجر به خلق سیاست بیم و ترس در حوزه‌های سیاسی اجتماعی شود. سطح لیتانی آشکارترین و مرئی‌ترین سطح است و نیاز به توانایی تحلیلی اندکی دارد. فرض‌ها به ندرت مورد پرسش قرار می‌گیرند. سطح دوم به علل نظام‌مند از جمله عوامل اجتماعی، فناورانه، اقتصادی، سیاسی، زیست‌محیطی و تاریخی (مثلاً افزایش نرخ تولد، فقدان تنظیم خانواده) ارتباط دارد. این

نوع تحلیل معمولاً توسط مؤسسات سیاستی ارائه می‌شود و به صورت سرمقاله در روزنامه‌ها یا نشریاتی که کاملاً دانشگاهی نیستند، منتشر می‌شود. این سطح، عملکرد مناسبی در بیان شرح‌های فنی و همچنین تحلیل علمی و دانشگاهی دارد. نقش دولت و بازیگران دیگر و منافع در اغلب موارد در این سطح مورد اکتشاف قرار می‌گیرد (عنایت‌اله، ۱۳۹۵).

سطح عمیق‌تر سوم به گفتمان و جهان بینی ارتباط دارد که از آن پشتیبانی می‌کند و اقدام به مشروع‌سازی آن می‌نماید (مثلاً، رشد جمعیت و دورنماهای تمدنی خانواده، فقدان قدرت زنان، فقدان امنیت اجتماعی، بحث جمعیت و مصرف). وظیفه‌ی این سطح یافتن فرایندهای عمیق‌تر اجتماعی، زبانی و فرهنگی مستقل از بازیگر (عدم وابستگی به بازیگران) و تا حدی مستقل از نظام است. در این سطح تشخیص فرض‌های عمیق‌تر پیش‌زمینه‌ی یک موضوع بسیار مهم است و تلاش‌هایی جهت چشم‌اندازسازی مجدد مسأله و موضوع صورت می‌گیرد. در این مرحله می‌توان به اکتشاف این امر پرداخت که چگونه گفتمان‌های مختلف (مثلاً ایدئولوژی‌ها و جهان بینی‌های بیان‌شده از طریق تمدن‌ها و معرفت‌ها) بیش از یک علت یا میانجی یک موضوع هستند و در واقع آن را می‌سازند. این سطح به تحقیق در این مورد می‌پردازد که چگونه گفتمان مورد استفاده در درک مسأله، بخشی از چارچوب‌بندی موضوع و مسأله است (صداقتی، ۱۳۹۸).

در این جا چهار سطح وجود دارد. سطح نخست سطح ذی‌نفع است که به معنای منافع مختلف بازیگران، سازمان‌ها و نهادها می‌باشد. سطح دوم، سطحی ایدئولوژیک و مواضع عمیق درباره‌ی وضعیت فعلی جهان و وضعیتی که باید باشد، است (مثلاً اقتصادگرایی در مقابل توسعه‌ی پایدار در مقابل مارکسیسم جدید). سطح سوم، تمدنی است که از طریق جهان بینی‌ها (مثلاً غربی، اسلامی و کنفوسیوسی) بیان می‌شود. سطح چهارم معرفتی است (مثلاً پسامدرن، مدرن و پیش‌مدرن یا نظم‌های چرخه‌ای یا ماریجی یا پاندولی دانش). تصمیم‌گیری در مورد گفتمان مورد استفاده (یا ترکیب ذی‌نفع، ایدئولوژیک، تمدنی و معرفتی) بستگی به موقعیت دارد (گواهی، ۱۳۹۶).

می‌توان در این مرحله بر اساس گفتمان‌های مختلف، سناریوهای بدیل مجزایی ارائه کرد؛ مثلاً سناریوی آینده‌ی جمعیت بر اساس دورنماها و دیدگاه‌های مسیحی - اسلامی نسبت به جمعیت (پیش رفتن و افزایش جمعیت) در مقابل سناریوی ایدئولوژیک - فرهنگی متمرکز بر این امر بود که گروه‌های زنان چگونه درباره‌ی تولد و پرورش کودکان و همچنین نقش‌های آن‌ها در مردسالاری و تقسیم جهانی کار قرار می‌گیرند. این سناریوها یک بعد افقی به تحلیل لایه‌ای ما می‌افزایند. در این سطح بنیان‌های چگونگی ارائه لیتانی و متغیرهای مورد استفاده جهت درک لیتانی مورد پرسش قرار می‌گیرند (کلهر، ۱۳۹۸).

لایه‌ی چهارم تحلیل، سطح استعاره یا اسطوره است. در این سطح داستان‌های عمیق و الگوهای جمعی، یعنی ابعاد ناخودآگاه و اغلب احساسی مشکل، مسأله یا تناقض (مثلاً تصور جمعیت به صورت غیر آماری، به عنوان یک جامعه یا منابع خلاق یا ترس از افزایش شمار خارجی‌ان) وجود دارند. این سطح یک تجربه‌ی سطح‌گریزی یا احساسی در مورد جهان بینی مورد نظر فراهم می‌آورد. زبان مورد استفاده کم‌تر خاص و ویژه بوده، ارتباط بیشتری با تصاویر دیداری رو به تکامل دارد و به لمس قلب به جای خواندن ذهن می‌پردازد. این سطح ریشه و مبدا طرح پرسش است. به هر حال، طرح پرسش محدودیت‌ها و مرزهای خود را می‌یابد؛ زیرا چارچوب طرح پرسش باید وارد دیگر چارچوب‌های درک، مثلاً اسطوره‌ای شود (صداقتی، ۱۳۹۸).

لایه‌ی چهارم ما را به سطح اسطوره‌ای هویت می‌برد. این دورنما گامی رو به عقب از آینده‌ی واقعی جهت پرداختن به فرض‌های عمیق‌تر آینده‌ی مورد بحث، به خصوص غیر منطقی یا پسامنتقی است. مثلاً سناریوهای خاص فرض‌هایی خاص درباره‌ی ماهیت زمان، عقلانیت و عامل انسانی دارند. مثلاً باور به این امر که آینده همچون پرتاب یک تاس است، یا باور به یک ضرب المثل عربی درباره‌ی آینده که کاملاً با پرتاب تاس متفاوت آمده است: «به خدا توکل کن اما پای شترت را ببند (با توکل زانوی اشتر ببند)» از مدل‌های اسطوره‌ای است، و این دو نگاه نیز از یک چشم‌انداز آمریکایی درباره‌ی آینده که این مقوله را بدون محدودیت و مملو از انتخاب و فرصت می‌داند، متفاوت می‌باشد؛ یا نگاه به آینده در اسطوره‌های چینی که از دیدگاه تفکر کنفوسیوسی برگرفته شده، انتخاب و فرصت را در بافت خانواده و اجداد و نه صرفاً تصمیم‌های فردی می‌داند (عنایت‌اله، ۱۳۹۵).

آن‌چه که اغلب ظاهر می‌شود تفاوت‌هایی است که به آسانی در سناریوهای بدیل بیان می‌شوند؛ هر سناریو به خودی خود تا حدی می‌تواند یک روش متفاوت دانستن را نشان دهد. به هر حال، تحلیل لایه‌ای علت‌ها سناریوها را در فضای عمودی مرتب می‌سازد. مثلاً پرداختن به موضوع فضاهای توقف و پارکینگ در مراکز شهری می‌تواند دامنه‌ای از سناریوها را خلق کند. سناریوی کوتاه‌مدت افزایش فضاهای پارکینگ (ساخت پارکینگ رو یا زیر زمین) دیدگاهی متفاوت نسبت به سناریوی ارزیابی ارتباط راه دور یا سناریوی توزیع فضاها به صورت شانس و تصادفی (به جای قدرت یا ثروت) یا سناریوی طرح پرسش در مورد نقش خودرو در مدرنیته (شهری با خودروی کم‌تر؟) یا ساختار شکنی ایده‌ی فضای پارکینگ همچون بسیاری از کشورهای جهان سوم که در آن‌ها فضاهای محدودی برای "پارکینگ" تصور شده است، دارد (کلهر، ۱۳۹۸).

در نتیجه سناریوها در هر سطح متفاوت هستند. سناریوهای نوع لیتانی ابزاری تر هستند، سناریوهای سطح اجتماعی سیاست‌محورتر بوده و سناریوهای گفتمانی یا جهان‌بینی سعی در درک تفاوت‌های بنیادین دارند. سناریوهای نوع اسطوره‌ای استعاره مجزا و متمایز هستند و این تفاوت را از طریق یک شعر، داستان، تصویر و یا یک روش دیگر در سمت راست مغز نشان می‌دهند (صداقتی، ۱۳۹۸).

سرانجام این که، هر کسی که به طور کلی به حل یک مسأله یا موضوع می‌پردازد نیز در هر سطح تغییر می‌کند. در سطح لیتانی، معمولاً دیگران یعنی دولت یا شرکت‌ها حضور دارند. در سطح اجتماعی، اغلب نوعی مشارکت بین گروه‌های مختلف وجود دارد. در سطح جهان‌بینی افراد یا مؤسسات داوطلب وجود دارند و در سطح اسطوره یا استعاره رهبران و هنرمندان وجود دارند. این چهار لایه با یکدیگر هم‌پوشانی دارند. با استفاده از روش تحلیل لایه‌ای علت‌ها می‌توان مشاهده کرد که چگونه سطح لیتانی فعلی (روندها و مسایل اصلی فراروی جهان) به خودی خود نوک کوه یخ، بیان یک جهان‌بینی خاص است. بحث در این مورد که کدام ایده‌های خاص مناسب کجا هستند هدف لایه‌ها را ناکام می‌گذارد. آن‌ها به دنبال کمک به خلق انواع جدید تفکر و نه تشویق بحث در مورد مسایلی از این دست هستند که چه چیزی دقیقاً باید در کجا مطرح شود (صداقتی، ۱۳۹۸).

در نتیجه، تحلیل لایه‌ای علت‌ها دارای پایه و اساس واقعی است که در تاریخ ساختار می‌یابد، سپس در یک گفتمان یا جهان‌بینی بافتار می‌یابد و در مرحله‌ی بعد در روش‌های پیش و پسامنتقی دانستن در اسطوره و استعاره قرار می‌گیرد. چالش فراروی آن، گنجاندن دیدگاه‌ها و دورنمای بسیار در یک مسأله‌ی خاص و

حرکت رو به بالا و پایین در بین سطوح و حواشی آنها است (کلهر، ۱۳۹۸). در این پژوهش با استفاده از روش پنل خبرگان به ترسیم استخوان ماهی اقدام شد و ابتدا علت‌ها شناسایی شدند و در گام بعد با استفاده از تحلیل لایه‌ی علت‌ها ابعاد دیگر این موضوع مورد بررسی قرار گرفت و در هر مرحله با استفاده روش سلسله مراتبی (AHP) به تحلیل داده‌ها پرداخته شده است. در انتخاب جامعه آماری از شیوه‌ی هدفمند و در دسترس استفاده شده است. این افراد شامل متخصصان و صاحب‌نظران حوزه فضای مجازی می‌باشند که در مجموعه‌های مرتبط با این حوزه در حال فعالیت هستند. شرح مشخصات این افراد در جدول ۱ مشاهده می‌شود.

جدول ۱: جدول مشخصات افراد مشارکت‌کننده در پژوهش

ردیف	میزان تحصیلات	رشته تحصیلی	مدت سابقه کار مرتبط
۱	دکتر	مدیریت فرهنگی	۱۰
۲	دکتر	علوم شناختی	۱۲
۳	دکتر	علوم ارتباطات	۱۱
۴	دکتر	هوش مصنوعی	۱۴
۵	دکتر	سیاست‌گذاری	۱۴
۶	دکتر	مدیریت تکنولوژی	۲۵
۷	فوق لیسانس	علوم رایانه	۱۳
۸	فوق لیسانس	مدیریت استراتژیک	۱۵
۹	فوق لیسانس	اقتصاد	۱۰
۱۰	فوق لیسانس	مدیریت رسانه	۱۱
۱۱	فوق لیسانس	مدیریت فناوری اطلاعات و ارتباطات	۱۶
۱۲	فوق لیسانس	جامعه‌شناسی	۱۳

## ۴ داده‌های پژوهش

در این پژوهش با استفاده از روش پنل نخبگانی که با حضور ۱۲ متخصص فضای مجازی برگزار گردید به بررسی وضعیت شبکه‌های اجتماعی داخلی با دو روش استخوان ماهی و تحلیل لایه‌ی علت‌ها پرداخته شد. در بخش تحلیل به روش استخوان ماهی نتایج در شکل شماره ۱ قابل مشاهده است. یافته‌های تحلیل لایه‌ی علت نیز در جدول شماره ۲ قابل مشاهده است. لازم به ذکر است از بین تمام شبکه‌های اجتماعی بومی چهار شبکه به نام‌های ایتا، بله، سروش و گپ انتخاب شدند.

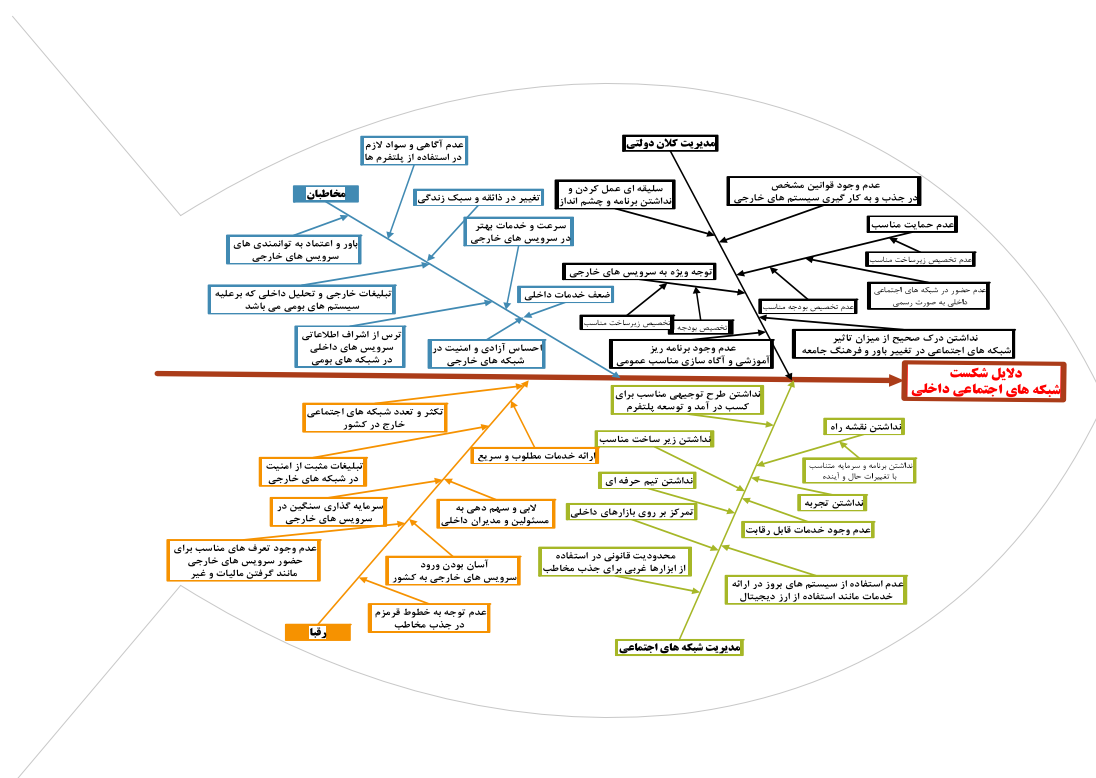
براساس داده‌های به دست آمده از مرکز ملی و به نقل از آقای خوراکیان معاون حقوقی و امور مجلس مرکز ملی فضای مجازی، به تاریخ ۳۰ آبان ۱۴۰۰ تا این تاریخ ۱۱ میلیون و ۶۰۰ هزار نفر در ایتا ثبت نام کرده‌اند که از این تعداد ۳ میلیون و ۳۸۰ هزار نفر فعالیت ماهانه دارند. ۱۲ میلیون و ۲۰۰ هزار نفر نیز در پیام‌رسان سروش ثبت نام کرده‌اند که از این تعداد ۲ میلیون و ۳۰۰ هزار نفر فعالیت ماهانه دارند. ۸ میلیون

و ۴۴۵ هزار نفر نیز در پیام‌رسان بله ثبت نام کرده‌اند که از این تعداد ۱ میلیون و ۳۸۲ هزار نفر به صورت ماهانه فعالیت می‌کنند. در نهایت ۶ میلیون و ۳۰۰ هزار نفر هم در پیام‌رسان گپ ثبت نام کرده‌اند که از این تعداد ۴ میلیون و ۴۰۰ هزار نفر فعالیت ماهانه دارند (به نقل از خبرگزاری ایسنا).

جدول ۲: میزان نصب‌ها و فعالیت‌های شبکه‌های داخلی

شبکه اجتماعی	تعداد نصب‌ها	تعداد نصب‌های فعال در هر ماه
ایتا	۱۱۶۰۰۰۰۰	۳۳۸۰۰۰۰
بله	۸۴۴۵۰۰۰	۱۳۸۲۰۰۰
گپ	۶۳۰۰۰۰۰	۴۴۰۰۰۰۰
سروش	۱۲۲۰۰۰۰۰	۲۳۰۰۰۰۰

## ۵ یافته‌های پژوهش



شکل ۱: نتایج روش استخوان ماهی



جدول ۳: تحلیل لایه‌ای علت‌ها برای شبکه‌های اجتماعی داخلی

لایه‌ها	علت‌ها
لیتانی	شبکه‌های اجتماعی داخلی خوب نیستند
سیستمی	عدم حمایت مادی و معنوی دولت مخصوصاً وزارت ارتباطات
	عدم بسته شدن کامل شبکه‌های اجتماعی خارجی
	مشکل در بحث‌های تکنیک و فنی مانند نبود سرور و زیرساخت مناسب
	عدم تبلیغات مناسب
گفتمانی	نداشتن استراتژی برای شرایط هجوم کاربران
	نداشتن نقشه راه برای توسعه سیستم‌های داخلی
	نظارت سازمان‌های امنیتی و عدم وجود حس امنیت
	مطلوب نبودن سرویس‌ها ارائه شده
	وجود نیازهایی که با سرویس‌های داخلی رفع نمی‌شود
اسطوره / استعاره	کندی سیستم‌ها داخلی
	شایعه اینکه در شبکه‌های اجتماعی افراد رصد می‌شوند
	تولیدکنندگان خارجی پاسخگوی خدمات خود هستند اما داخلی‌ها نه
	سیستم‌ها داخل احترامی به مشتری نمی‌گذرند
	ما نمی‌توانیم تولید خوبی داشته باشیم
	ما کشور جهان‌سومی و وابسته هستیم
	تولیدات خارجی همیشه با کیفیت و بهتر از تولیدات داخلی است

بعد از به دست آمدن نتایج یافته‌های این دو روش از نخبگان درخواست شده که پرسشنامه‌ی سلسله‌مراتبی مربوط به دو روش را جهت رتبه‌بندی و اولویت‌بندی چهار شاخه‌ی اصلی ایجاد استخوان ماهی و در تحلیل لایه‌ای برای تعیین مهمترین لایه تکمیل نمایند. بعد از جمع‌آوری پرسشنامه‌ها و تحلیل داده‌ها توسط نرم‌افزار اکسپرچویس در روش اول (استخوان ماهی) که در نمودار ۱ قابل مشاهده می‌باشد به ترتیب: «مدیریت کلان دولتی، مدیریت شبکه‌های اجتماعی، مخاطبین و رقبا» مهمترین عوامل تاثیرگذار در شرایط کنونی تشخیص داده شدند و در روش دوم (تحلیل لایه‌ای علت‌ها) که در نمودار ۲ قابل مشاهده می‌باشد به ترتیب: «لایه‌ی اسطوره، سیستمی گفتمانی و لیتانی» بیشترین تأثیر را در شکست شبکه‌های اجتماعی داخلی داشته‌اند.



نمودار ۱: تحلیل روش اول (استخوان ماهی) توسط نرم‌افزار اکسپرچویس



نمودار ۲: تحلیل روش دوم (تحلیل لایه‌ای علت‌ها) توسط نرم‌افزار اکسپرچویس

در پایان از افراد حاضر در پژوهش خواسته شد تا نسبت نفوذ هر یک از شبکه‌های اجتماعی داخلی را براساس روش سلسله مراتبی رتبه‌بندی نمایند که نتایج این تحلیل نشان داد که به ترتیب ایتا، بله، سروش و گپ بیشترین ضریب نفوذ را از نگاه نخبگان دارند که این نتایج در نمودار شماره ۳ قابل مشاهده می‌باشد.



نمودار ۳: تحلیل ضریب نفوذ شبکه‌های اجتماعی انتخاب‌شده توسط نرم‌افزار اکسپرچویس

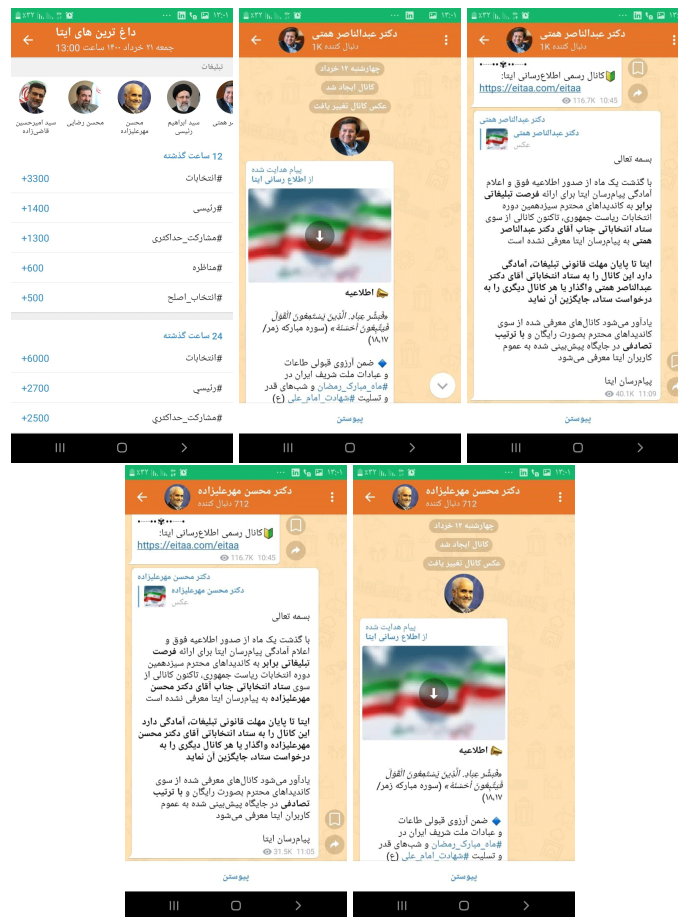
## ۶ نتیجه‌گیری

بر اساس یافته‌های به دست آمده می‌توان گفت در روش اول (استخوان ماهی) به ترتیب: «مدیریت کلان دولتی، مدیریت شبکه‌های اجتماعی، مخاطبین و رقبا» مهمترین عوامل تاثیرگذار در شرایط کنونی تشخیص داده شدند و در روش دوم (تحلیل لایه‌ای علت‌ها) به ترتیب: «لایه‌ی اسطوره، سیستمی گفتمانی و لیتانی» بیشترین تأثیر را در شکست شبکه‌های اجتماعی داخلی داشته‌اند.

با مقایسه یافته‌های این دو روش می‌توان نتیجه گرفت که «عدم باور به تولیدات داخلی در مدیران کلان دولتی» عامل و ریشه‌ای‌ترین لایه‌ها می‌باشد. اگر باور به توانمندی داخلی و خوداتکایی در مدیران داخلی تقویت شود می‌توان امیدوار بود که با هزینه مالی اندک بتوان به توفیقات زیادی دست پیدا نمود.

به عنوان اولین عامل در بحث عدم موفقیت شبکه‌های اجتماعی داخلی می‌توان به باور نداشتن مسئولین به توان داخلی اشاره نمود؛ که به سیاست‌هایی مانند عدم حمایت از شبکه‌های اجتماعی داخلی در مقابل توسعه مدل‌های خارجی منجر می‌گردد. این موضوع از توان رقابت شبکه اجتماعی داخلی با نمونه‌های خارجی می‌کاهد. عدم باور مسئولین باعث شده تا فضای مناسبی برای توسعه شبکه‌های خارجی در داخل ایران به وجود آید و فضا برای رشد و توسعه شبکه‌های اجتماعی داخلی بسیار محدود شود که اینگونه رفتار در مدل حکمرانی فضای مجازی واقعا جای تامل و بررسی دارد؛ چرا که هیچ عقل سلیمی این گونه رفتار را مناسب با حمایت از تولیدات داخلی که به استقلال و قدرت در فضای مجازی منتج می‌شود، نمی‌داند.

سیاست‌های غلط بدون توجه به آینده در خصوص شبکه‌های اجتماعی مانند شناسنامه‌دار نمودن کانال‌های تلگرامی از دیگر مواردی است که باعث شده نگاه امنیتی در مورد حضور در شبکه‌های اجتماعی داخلی بیشتر قوت بگیرد. الآن باید از سیاست‌گذاران و مدیران ارشد پرسید که با بسته شدن تلگرام، وضعیت آن کانال‌هایی که دارای مجوز هستند چگونه است و شما چه تدبیری برای آنها داشتید؟ بی‌اطلاعی و عدم شناخت ابعاد فضای مجازی باعث شده که مسئولین با تصمیمات کوتاه‌مدت و نسنجیده عملاً به تایید گفتمان تولیدشده در جامعه بروند و بازار رقابتی را به سمت توسعه سهم شبکه‌های اجتماعی خارجی تغییر مسیر دهند و جایی برای رشد و توسعه مجموعه‌های داخلی قرار ندهند.



شکل ۲: تصاویری از عدم تبلیغات نامزدهای انتخاباتی دوره سیزدهم در شبکه اجتماعی داخلی

بر اساس یافته‌های تحلیل ضریب نفوذ شبکه‌های اجتماعی می‌توان نتیجه گرفت که ضریب نفوذ شبکه‌های اجتماعی وابسته به تعداد نصب‌ها نیست؛ بلکه به فعالیت در آن است. ای‌تا و بله که تعداد نصب‌هایی کمتر از سروش دارند، ضریب نفوذشان بیشتر از سروش می‌باشد و این نشان می‌دهد که سیاست‌های مدیریتی شبکه‌های اجتماعی داخلی چقدر در ادامه حیات و نفوذ در مخاطبین مؤثر است. عدم توجه به بازارهای

خارجی از دیگر مشکلات شبکه‌های اجتماعی داخلی است که باید گفت باز این مشکل به سیاست‌گذاران کلان جامعه برمی‌گردد؛ چرا که آنها باید بسترهای توسعه را برای شبکه‌های اجتماعی داخلی در منطقه آماده نموده و با سیاست‌های حمایتی بتوانند سهمی از بازار فضای مجازی منطقه را برای تولیدات بومی به دست آورند.

## ۷ پیشنهادها

پیشنهاد می‌شود یک پلتفرم واحد ایجاد شود تا مثل اتفاقی که برای بانک‌های نظامی افتاد و همه با حفظ همه‌ی امکانات خود تبدیل به بانک سپه شدن در شبکه‌های اجتماعی داخلی نیز چنین تدبیری صورت گیرد که تحت یک پلتفرم بتوانیم به دیگر پلتفرم‌های داخلی پیام ارسال و دریافت نمود و نیاز به نصب تعداد زیادی از پلتفرم‌ها نباشد و کسانی که نصب دارند با به‌روزرسانی بتوانند از امکانات دیگر شبکه‌های اجتماعی داخلی استفاده نمایند.

در مدل دیگر با استفاده از ظرفیت بانک‌ها یا صنایع و قرار دادن آنها در کنار هر یک از شبکه‌های اجتماعی به شبکه‌های اجتماعی داخلی در حوزه زیرساخت و مخاطب کمک نموده و باعث توسعه خدمات بانکی و صنعتی در جامعه شویم.

در زمان کرونا برنامه‌ی شاد به عنوان یک برنامه‌ی آموزشی جهت کمک به آموزش و پرورش تولید شده که ضعف‌ها و انتقاداتی بر آن وجود دارد اما می‌تواند الگویی مناسب برای توسعه یک شبکه‌ی اجتماعی داخلی بر اساس نیاز آموزشی باشد که در گام اول ضعف‌هایش برطرف شده و دانشگاه‌ها نیز تحت این شبکه قرار گیرند با نام جدید شمع که مخفف شبکه ملی علم است به جذب مخاطب بپردازد و در گام بعد پاسخگوی نیازهای دیگر مخاطبان با ارائه سرویس‌های جدید باشد.

باید از الگوهایی مانند الگوی شبکه‌های اجتماعی کاکائو<sup>۱۳</sup> که ابتدا برای خدمات خاصی در کشور کره جنوبی به وجود آمد و الان ۷۷ درصد شهروندان کره جنوبی از آن استفاده می‌نمایند بهره گرفت و بر اساس آن خدماتی مانند اسنپ و یا شاد که قبلاً اشاره شده را با استفاده از این روش به شبکه اجتماعی ملی تبدیل نمود.

بر اساس نتایج حاصله پیشنهاد می‌شود برای تغییر باور در داخل جامعه برنامه‌های شناختی تبلیغاتی جهت معرفی محصولات باکیفیت داخلی مخصوصاً حوزه فضای مجازی داشته باشیم. می‌توان با سرمایه‌گذاری و تبلیغ توان داخلی این مشکل را حل نمود؛ مانند کار تبلیغاتی که در حوزه موشکی و سلول‌های بنیادین انجام شده است. البته نیاز به زمان و برنامه بلندمدت می‌باشد تا در لایه‌ی گفتمان نیز تاثیر بگذارد و حس امنیت و اعتماد بازسازی شده و شاهد کوچ مخاطبین از سرویس‌های خارجی به داخلی باشیم.

برنامه‌های سواد فضای مجازی را جهت آگاه‌سازی و ایجاد گفتمان جدید باید باز طراحی و برنامه‌ریزی نمود تا عموم جامعه از نبود امنیت در شبکه‌های خارجی باخبر شوند؛ از آن جمله می‌توان اخبار مربوط به افشاکری‌های ادوارد اسنودن که جزو سازمان NSA آمریکا بوده استفاده نمود.

<sup>13</sup>KAKAO TALK

پیشنهاد می‌شود مسئولین برای بهبود وضعیت شبکه‌های اجتماعی داخلی به محدودسازی شبکه‌های اجتماعی خارجی در پهنای باند و سرویس پردازند و تبلیغات این سرویس‌ها را در صدا و سیما متوقف نمایند. پیشنهاد می‌شود برای تبلیغات و اطمینان بخشی به عام جامعه مانند کاری که در کلاب هاوس انجام شد این بار برای سرویس‌های شبکه‌های اجتماعی بومی انجام شود و با حضور مسئولین به صورت رسمی و فعالیت در این شبکه‌ها به رشد و ارتقای مخاطب در این سرویس‌ها پردازند. چند پیشنهاد برای مطالعات آینده:

- تحقیق در مورد شبکه‌های اجتماعی آینده و چگونگی تولید بومی این شبکه‌های اجتماعی متناسب با نیازهای داخلی
- تدوین سند تحول شبکه‌های اجتماعی داخلی در راستای پیشی گرفتن از رقبای خارجی
- راه‌های مسدودسازی سرویس‌های خارجی با کمترین هزینه جهت رونق گرفتن سرویس‌های داخلی در یک بازه‌ی زمانی محدود
- بررسی مدل کسب‌وکارها در شبکه‌های اجتماعی با نگاه به بازارهای بین‌الملل در الگوی فعلی و تغییرات آینده

## مراجع

- [۱] والاس، پتریشیا (۱۳۸۲). روانشناسی اینترنت، ترجمه بهنام اوحدی. فضل الله قنادی و حمیرا صفوی همایی، تهران: انتشارات نقش خورشید.
- [۲] کسمایی، علی اکبر (۱۳۷۰). جهان امروز و فردا. چاپ اول، تهران: انتشارات اطلاعات.
- [۳] عنایت‌اله، سهیل (۱۳۹۵). آینده‌پژوهی با روش تحلیل لایه لایه‌ای علت‌ها، انتشارات شکیب، جلد اول.
- [۴] هیگینز، جیمز ام. (۱۳۹۲). کتاب ۱۰۱ تکنیک حل خلاق مساله، داریانی، انتشارات امیرکبیر (ترجمه احمد پور، محمود).
- [۵] صداقتی، عاطفه (۱۳۹۸). ارائه سناریوهای استعاره در سبک نوین «خانه» زندگی شهری مبتنی بر روش CLA، فصلنامه راهبرد، سال بیست و هشتم، شماره نود.
- [۶] کلهر، مهدی (۱۳۹۸). آینده‌پژوهی تاخیرات پروژه‌های شهری با رویکرد تحلیل لایه‌ای علت‌ها، سناریونویسی، تاپسیس فازی و سوات، فصلنامه آینده‌پژوهی مدیریت، سال سی‌ام، شماره ۱۱۶.
- [۷] گواهی، عبدالرحیم (۱۳۹۶). آینده‌نگری در آینده‌پژوهی: تحلیل علی لایه‌ای چالش‌های آینده‌پژوهی در ایران، فصلنامه آینده‌پژوهی مدیریت، سال بیست و هشتم، شماره ۱۰۹.
- [۸] «چند میلیون کاربر از پیام‌رسان‌های داخلی استفاده می‌کنند؟»، خبرگزاری ایسنا، کد خبر ۱۴۰۰۰۸۲۷۲۱۱۶۶
- [9] IOS. (2017). Internet Online Statistics. Retrieved from <http://www.internetlivestats.com>.
- [10] Chaffey, D. (2016). Global social media research summary 2016. Retrieved from <http://www.smartinsights.com/social-media-marketing/socialmedia-strategy/new-global-social-media-research>

- [11] Saghafi, F., Abasi Shahkooch, K., Jalali, A. A. (2010). Social networks are the monitoring platform (based on the case study). Proceedings of the National Conference on Public Supervision: Strategies and Solutions. Retrieved from [http://www.iust.ac.ir/files/ee/a\\_jalali\\_b1b62/paper](http://www.iust.ac.ir/files/ee/a_jalali_b1b62/paper), (Persian).
- [12] G. Eason, B. Noble, and I. N. Sneddon (1955). "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551.
- [13] J. Clerk Maxwell (1892). A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, pp.68–73.
- [14] I. S. Jacobs and C. P. Bean (1963). "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, pp. 271–350.
- [15] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa (1987). "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, [Digests 9th Annual Conf. Magnetism Japan, p. 301, 1982].
- [16] M. Young (1989). The Technical Writer's Handbook. Mill Valley, CA: University Science.



# هستی‌شناسی فضای سایبر: بازخوانی انگاره فلسفی «مراحل تکامل عقل انسان» و انگاره فلسفی «عالم عقول» از منظر فضای سایبری

مصطفی ملکشاهی صفت<sup>۱</sup>

اگرچه فلسفه و کلام اسلامی، دانشکده الهیات، دانشگاه قم، قم، ایران  
malekshahi819@chmail.ir

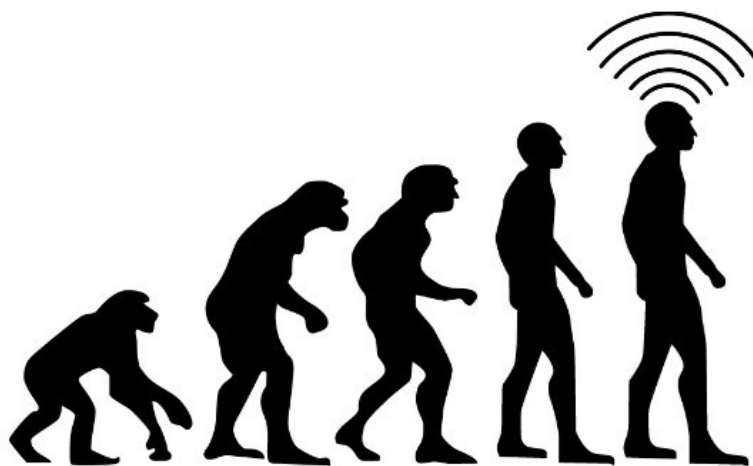
## چکیده

نوشتار پیش رو در آغاز میان پرسش‌های فلسفی و پرسش‌های روزمره افراز کرده، در مرحله بعد، خود پرسش‌های فلسفی را به دو بخش اصلی (هستی‌شناسی، معرفت‌شناسی) و فرعی (فلسفه‌های مضاف) تقسیم می‌نماید. نگاه بررسی فلسفی نگارنده از فضای سایبری را ناظر به جنبه هستی‌شناسانه تعیین می‌کند و نشان داده است که بررسی هستی‌شناسانه فضای سایبری دست کم با یکی از دو رویکرد ذیل امکان دارد: رویکرد اول، طرح همان پرسش‌های هستی‌شناسانه قدیمی که از دیرباز در هستی‌شناسی فلسفی مطرح بوده‌اند در قلمرو وجودی موجودی به نام فضای سایبر است؛ رویکرد دوم، ارائه شواهدی قابل اعتنا برای ارائه تفسیری سایبرنتیک از مباحث هستی‌شناسانه قدیمی فلسفه می‌باشد. گفتنی است که این نوشتار قصد دارد رویکرد دوم را در هستی‌شناسی فضای سایبری اتخاذ نماید و البته ناگفته نماند که خود جداسازی این دو رویکرد نیز دستاورد همین نوشتار است. نوشتار پیش رو بعد از نقل و نقد قرائت مشهور و رایج از آموزه فلسفی «عقل فعال» و «عقل مستفاد» در فضای عمومی آموزش فلسفه، نشان می‌دهد در نظر گرفتن قرائتی سایبرنتیک از دو آموزه فلسفی مزبور می‌تواند تفسیر منسجم‌تری از فلسفه به مثابه دانشی سرّی و باستانی ارائه نماید.

**کلمات کلیدی:** فضای سایبر، عالم عقول، عقل فعال، عقل بالمستفاد، هستی‌شناسی، فلسفه.

## ۱ مقدمه و بیان مسئله

یکی از ویژگی‌های انسان پرسشگری است؛ آدمی در زندگی روزانه‌ی خود، پیوسته با پرسش‌هایی مواجه می‌شود و به حل آنها می‌پردازد؛ نظیر اینکه: امروز کدام کار را اول انجام دهم، و درباره‌ی کارم با چه کسی مشورت کنم، تغییرات قیمت در بازار امروز چگونه است، امشب را چگونه با دوستانم سپری کنم و مانند آن. اما در میان انبوه افکار و اندیشه‌های روزانه، گاه و بی‌گاه پرسش‌هایی خودنمایی می‌کنند که می‌توانند ساعات طولانی



ما را به خود مشغول سازند و به تفکر وادار نمایند؛ از قبیل اینکه: چرا درد و رنج وجود دارد؟ خوشبختی و سعادت در گرو چیست؟ آیا می‌توان به آن رسید؟ سرانجام ما انسان‌ها چه می‌شود؟ آغاز و انجام جهان چگونه است؟ چه هدفی را باید در دنیا دنبال کرد؟ آیا ورای این جهان پهناور، خالق حکیم وجود دارد؟ حقیقت مرگ چیست؟

تا زمانی که انسان با همان پرسش‌های معمولی و روزانه روبه‌روست و به دنبال پاسخ آنهاست، در نازل‌ترین سطح از تفکر به سر می‌برد اما چنانچه از این مرحله تفکر عبور کرده و با جدیت و پیوسته به پرسش‌های دسته دوم پرداخت، وارد مرتبه دوم از تفکر شده که بسته به نوع پاسخ‌هایی که ارائه خواهد داد می‌توان آن را «تفکر کلامی» و یا «تفکر فلسفی» نامید؛ زیرا هم اهل کلام و هم اهل فلسفه به رغم اختلاف نظرهایی که دارند، پیوسته وجه همت خود را مصروف همین پرسش‌های اساسی و بنیادین می‌نمایند.

این نوشتار به رغم احترام، اعتنا و گرایش بالایی که برای تفکر کلامی قائل است بنا دارد از منظری فلسفی به موضوع هستی‌شناسی فضای سایبر پردازد؛ اما پیش از آن لازم است بدانیم دانش فلسفه دارای یک بخش اصلی و تعدادی بخش‌های فرعی است. بخش اصلی فلسفه به منزله ریشه و اساس فلسفه است و بخش‌های فرعی در حکم شاخه‌ها، برگ‌ها و میوه‌های آنند.

بخش اصلی و ریشه‌ای فلسفه در صدد بحث و بررسی حیثیت وجودی اشیاء و پرسش‌های پیرامون آن است و تلاش دارد قوانین و احکامی که مربوط به خود هستی و وجود است را به دست آورد؛ از این رو بخش اصلی فلسفه را هستی‌شناسی نامیده‌اند؛ هرچند می‌توان و باید مباحث مربوط به معرفت‌شناسی را نیز به بخش اصلی و ریشه‌ای فلسفه ملحق نمود زیرا معرفت به وجود، فرع بر امکان شناخت آن است لذا فلسفه در ریشه‌ای‌ترین پرسش‌های خود بنا دارد توانایی انسان در شناخت خود هستی را نیز بررسی نماید.

بخش فرعی دانش فلسفه، آن دسته از دانش‌هایی هستند که قوانین بنیادی و وجودشناسی و معرفت‌شناسی را به محدوده‌های خاص منتقل می‌سازند و بدین ترتیب با تأمل فیلسوفانه در حوزه‌هایی مانند اخلاق، حقوق، سیاست، دین، تاریخ، فرهنگ، طبیعت، تکنولوژی و مانند آن، شاخه‌هایی از فلسفه مثل فلسفه‌ی

اخلاق، فلسفه‌ی حقوق، فلسفه‌ی سیاست، فلسفه‌ی دین، فلسفه‌ی تاریخ، فلسفه‌ی فرهنگ، فلسفه‌ی طبیعت، فلسفه‌ی تکنولوژی و مانند آن شکل می‌گیرد. امروزه دامنه‌ی این فلسفه‌ها که به فلسفه‌های مضاف شهرت دارند بسیار توسعه یافته و ناظر به بسیاری از پدیده‌ها یا رشته‌های علمی شکل گرفته‌اند. اکنون تذکر می‌دهیم که آنچه در این نوشتار مورد نظر نگارنده است بررسی ریشه‌ای و هستی‌شناسانه‌ی فضای سایبری است و برای این منظور می‌توان و باید دست کم یکی و یا اینکه هر دو رویکرد ذیل را اتخاذ نمود:

**رویکرد اول -** طرح پرسش‌های هستی‌شناسانه فلسفی در اتمسفر فضای سایبری.

**رویکرد دوم -** طرح پرسش‌های سایبری در منظومه هستی‌شناسی فلسفی.

توضیح مطلب؛ در رویکرد نخست، فیلسوف در ابتدا فضای سایبر را به مثابه یک امر موجود مدنظر قرار داده آنگاه موجودیت آن را درست از همان حیث که موجود است با پرسش‌های هستی‌شناسانه‌ی ذیل مورد واکاوی قرار می‌دهد: فضای سایبر، موجود است یا غیر موجود؟ چنانچه موجود باشد، جوهر است یا عرض؟ چنانچه جوهر باشد، بالفعل است یا بالقوه؟ چنانچه بالفعل باشد، در فاعلیتش نیازمند ماده است یا در فاعلیتش نیازمند ماده نیست؟ فضای سایبر، واحد است یا کثیر؟ فضای سایبر، ثابت است یا سیال؟ فضای سایبر، ذهنی است یا خارجی؟ فضای سایبر، (نسبت به طبیعت مشهود) مقدم است یا موخر؟ فضای سایبر، (در مقایسه با طبیعت مشهود) اصیل است یا اعتباری؟ فضای سایبر، حادث است یا قدیم؟ و... اما در رویکرد دوم، فیلسوف به جای اینکه فضای سایبری را مورد مطالعه هستی‌شناسانه قرار بدهد، خود آموزه‌های رایج و مشهور فلسفی که در حوزه هستی‌شناسی فلسفی، نقل محافل شده‌اند را چنان مورد بازخوانی قرار می‌دهد که روایتی سایبرنتیک از متن هستی‌شناسی فلسفی استخراج می‌نماید.

نوشتار پیش رو در صدد است تا با رویکرد دوم به هستی‌شناسی فضای سایبر بپردازد و برای این منظور انگاره‌ی فلسفی «مراحل تکامل عقل انسان» و نیز انگاره‌ی فلسفی «عالم عقول» را بهترین و متناسب‌ترین نقطه شروع دانسته است؛ به همین خاطر کار را با نقل و بعد از آن نقد روایت مشهور از این دو آموزه‌ی فلسفی آغاز نموده و در نهایت قرائت سایبرنتیک را به مثابه یک امکان قابل اعتنا برای فهم میراث فلسفی مان پیشنهاد می‌نماید.

## ۲ مراحل تکامل عقل انسان در نگاه مشهور اهل فلسفه

امروزه در کلاس‌های رایج فلسفه‌ی اسلامی این‌گونه گفته می‌شود که اولین مرتبه از مراتب عقل انسانی، عقل هیولانی است؛ در این مرحله، انسان هیچ‌گونه ادراک عقلی ندارد ولی آماده‌ی کسب همه‌ی ادراکات عقلی است (نصیرالدین طوسی، ۱۳۷۵، ج ۲، ص: ۳۵۴). بعد از آنکه انسان به مرتبه عقل بالملکه ارتقاء یافت؛ یعنی بدیهیات را واجد شد و همچنین بدیهیاتی که امهات قواعد منطبق هستند در او شکل گرفتند، اکنون می‌تواند از طریق تفکر یا از طریق حدس، معقولات نظری (غیر بدیهی) را اکتساب نماید (همان، صص: ۳۵۴-۳۵۵) بدین نحو که با تفکر کردن یا حدس زدن مستعد می‌شود که موجودی به نام عقل فَعَال، دانش و صورت معقوله

تازه‌ای را به او افزوده نماید (همان، ص: ۳۵۵). اما به راستی این صورت عقلیه اکتساب شده از ناحیه عقل فعال در کجای نفس ذخیره خواهد شد؟ در قوه خیال یا در قوه حافظه؟

پاسخ: هیچکدام؛ میدانیم که قوه خیال انبار ذخیره صورت‌های محسوسه‌ای است که از ناحیه قوه حس مشترک در آنجا سرازیر می‌شوند و خود قوه حس مشترک، حوضی است که از مجاری حواس پنجگانه‌ی ظاهری پر می‌شود؛ لذا قوه خیال انبار ذخیره محسوسات است نه صور معقوله (ملکشاهی، ۱۳۹۲، ج ۲، ص: ۱۸۱). از سوی دیگر می‌دانیم که قوه حافظه نیز انبار ذخیره معانی جزئی‌های است که از ناحیه قوه واهمه در آن سرازیر می‌شوند؛ لذا هیچ معنای کلی (صور معقوله) در آن وجود ندارد (همان، ص: ۱۸۲). از سوی دیگر این هر دو قوه، جسمانی بوده و در مغز منطبق هستند (همان، ص: ۱۸۳) حال آنکه صور معقوله را مجرد می‌دانند پس نمی‌توان محل ذخیره آن‌ها را جسم و یا شیئی جسمانی در نظر گرفت (نصیر الدین طوسی، ۱۳۷۵، ج ۲، ص: ۳۶۱)، روی این حساب پس محل ذخیره صور معقوله اکتساب‌شده در کجاست؟ پاسخ مشهور این است که مخزن ذخیره‌کردن صور معقوله، درون همان عقل فعال سابق الذکر است (همان، ص: ۳۶۴).

گفتنی است زمانی که رشد عقل انسانی به مرحله سوم یعنی عقل بالفعل برسد آنگاه گنجینه‌ای از معقولات نظری به دست آورده است ولی نمی‌تواند به صورت یکجا و همزمان، همه را نزد خود حاضر نموده و مشاهده نماید؛ بلکه در این مرحله صرفاً این توانایی را دارد که هر زمان قصد نماید می‌تواند صورت معقوله مورد نظر را استحضار (طلب حضور) نماید و آن صورت نیز بی‌درنگ حاضر شده و مورد مشاهده عقل قرار می‌گیرد (همان، ص: ۳۵۵)؛ اما به راستی عقل بالفعل از چه کسی طلب می‌کند و چه کسی طلب او را اجابت خواهد کرد؟ پاسخ مشهور: عقل فعال.

در نهایت، زمانی که رشد عقل انسان به چهارمین و آخرین مرحله تکاملی خود یعنی عقل بالمستفاد رسید همه معقولات را به صورت یکجا و همزمان در حال مشاهده دارد و دیگر نیازی به طلب حضور (استحضار) نیست زیرا همه را یکجا در لحظه اکنون داراست (ابن‌سینا، ۱۳۷۵، صص: ۸۶-۸۵)؛ اما باید بدانیم که مراد از همه‌ی معقولات، همه‌ی معقولاتی که تاکنون اکتساب کرده نیست بلکه مراد، تمام معقولات جهان است؛ زیرا کافی است پرسیده شود، عقل بالمستفاد این صور معقوله را در کجا مشاهده می‌کند؟ پاسخ مشهور: چون عقل انسان در این مرحله به عقل فعال اتصال یافته لذا همه را آنجا مشاهده می‌کند و چون عقل فعال مخزن تمام صور جهان است لذا عقل مستفاد به دلیل اتصال (لینک) به نحوی یکجا و توأم، همه معقولات جهان را دارد مشاهده می‌کند.

### ۳ تبیین بیشتر با استفاده از تمثیل

چنانچه بخواهیم تفاوت عقل بالفعل را با عقل بالمستفاد به نحوی آشکارتر نمایان سازیم کافی است به وجه تفاوت یک کتابخانه معمولی با یک کتابخانه مجازی (سایبرنتیک) توجه کنیم؛ در یک کتابخانه معمولی قفسه‌هایی وجود دارند که گنجینه‌ای از کتاب‌ها را حسب موضوعاتی که دارند به نحو طبقه‌بندی شده‌ای در خود جای داده‌اند، شما در هر لحظه که اراده نمایید می‌توانید با مراجعه به قفسه‌ی مربوطه، کتاب مورد نظر خود را برداشته و مطالعه نمایید ولی چنانچه اکنون در کنار قفسه تاریخ باشید، طبعاً به قفسه روانشناسی

دسترسی نخواهید داشت و اگر خواهان یک کتاب با موضوع روانشناسی باشید باید به سمت قفسه‌ی مربوطه حرکت نموده و کتاب مورد نظرتان را بردارید؛ حضور شما در چنین کتابخانه‌ای به گونه‌ای است که به همه‌ی قفسه‌ها به نحوی اجمالی (نه تفصیلی) اشراف دارید؛ یعنی با آنکه هیچ یک از کتاب‌ها اکنون پیش روی شما حاضر نیستند ولی هر لحظه اراده کنید می‌توانید کتاب مورد نظر خود را استحضار نمایید ولی در عین حال روشن است که دستیابی به یک قفسه به قیمت غفلت و دوری از قفسه دیگر تمام خواهد شد؛ این در حالی است که در یک کتابخانه مجازی، تمام قفسه‌های کتابخانه در هر یک از قفسه‌ها به تنهایی به نحوی مشاع حضور دارند و اینگونه نیست که اگر در سمت چپ کتابخانه باشید، سمت راست از دسترس شما خارج باشد و یا اگر در جلو بودید، بخش عقبی پیش روی شما نباشد؛ بلکه در هر قفسه، تمام قفسه‌ها موجود هستند و این نظیر یک حوض آب است؛ اگر یک تکه سنگ را در سمت چپ حوض مزبور پرتاب کنید موجی فراگیر تمام گستره‌ی حوض را فرا خواهد گرفت و چنانچه سنگ دیگری را در سمت راست همان حوض پرتاب نمایید باز هم موجی فراگیر تمام گستره‌ی حوض را به نحوی فرا می‌گیرد که در امواج قبلی متداخل شده اما هرگز مانع از موجودیت و انتشار آنها نمی‌شود و اگر همین کار را با هشت تکه سنگ دیگر تکرار کنید باز امواجی فراگیر را شاهد خواهیم بود که هرگز مزاحم انتشار یکدیگر نمی‌شوند؛ این امر باعث می‌شود هر نقطه فرضی از سطح حوض را که در نظر بگیرید به صورت همزمان محل حضور و موجودیت ده موج دیگر باشد؛ موجی بر موجی؛ این وضعیت ادراکی عقل بالمستفاد است لذا ابن سینا در نمط سوم از کتاب اشارات و تنبیهات، این وضعیت را با تعبیر قرآنی «نور علی نور» تنظیم نموده است (همان، ص: ۸۶) و البته مراد او از ارائه چنین تمثیلی نه تنها بی‌ارتباط با چیزی که ما امروزه آن را «Wi-Fi» می‌نامیم نیست، بلکه احتمالا مقصود او همان نیز باشد؛ به هر حال، عقل بالمستفاد همه‌ی معقولات جهان را هم‌زمان و یک‌جا نزد خود حاضر داشته و در لحظه اکنون مشاهده می‌کند پس نیازی ندارد که چیزی را استحضار نماید؛ این در حالی است که حضور شما در آن کتابخانه معمولی نظیر وضعیت ادراکی عقل بالفعل می‌باشد؛ زیرا عقل بالفعل، گنجینه معقولات مکتسبه‌ای دارد که در قفسه‌هایی بایگانی شده‌اند ولی اکنون پیش روی او حاضر نیستند؛ لذا برای دسترسی به هر یک باید آن را استحضار نماید. این بود تفسیر مشهور از مراتب چهارگانه‌ی رشد عقل انسان در تعالیم فلسفه؛ و این بود تفسیر مشهور از عقل فعال، اما به راستی چنین قرائتی تا چه میزان پذیرفتنی می‌تواند باشد؟

## ۴ نقد نگاه مشهور

در نقد قرائت مشهور و رایج پیش گفته، کافی است پرسیده شود:

۱. اگر انسانی مثل من، صور معقوله را از ناحیه موجودی به نام عقل فعال کسب کرده است، چرا در خودم جایی ندارم که ذخیره‌شان کنم و باید صوری که از عقل فعال اکتساب کرده‌ام را در خود عقل فعال ذخیره و نگهداری نمایم؟! البته ممکن است با توجه به آنچه در بادی امر از سخنان ابن سینا در نمط سوم از کتاب اشارات و تنبیهات دانسته می‌شود اینگونه پاسخ داده بشود که مخزن حفظ و نگهداری صور معقوله با مخزن حفظ و نگهداری صور محسوسه و همچنین معانی جزئیة این تفاوت را دارد که آن باید مجرد و غیر قابل انقسام باشد (همان، ص: ۸۷)؛ توضیح مطلب: می‌دانیم که صور محسوسه

و نیز معانی جزئی به ترتیب در قوه حس مشترک و قوه واهمه مرتسم می‌شوند و این هر دو قوه، جسمانی بوده و در جسم (مغز) نیز منطبق هستند لذا به راحتی می‌توان آن‌ها را و یا محل جسمانی آن‌ها را به دو بخش تقسیم نموده و قسمی را محل ادراک و قسمی را جایگاه حفظ و نگهداری این صور و معانی جزئی تلقی نمود؛ اما قوه عاقله ما که ادراک‌کننده‌ی صور معقوله است، امری مجرد بوده و در جسم منطبق نیست لذا نمی‌توان برای آن دو بخش در نظر گرفت که یکی مخزن صور معقوله باشد و دیگری ادراک‌کننده‌ی آن‌ها بلکه قوه عاقله تماماً بسیط است (ملکشاهی، ۱۳۹۲، ج ۲، صص: ۱۹۹-۱۹۸) لذا طبق قاعده الواحد، این قوه یا فقط ادراک‌کننده‌ی صور معقوله است یا فقط مخزن آن‌ها، ولی می‌دانیم که قوه عاقله ادراک‌کننده‌ی صور معقوله است لذا نمی‌تواند مخزن آن‌ها نیز باشد پس چاره‌ای نیست مگر آنکه چیز دیگری که غیر از جسم و غیر از نفس ناطقه ماست در نظر بگیریم که محل ذخیره‌سازی صور معقوله مکتسبه باشد و آن موجود مفارق که باید مجرد نیز باشد (تا بتواند محل ارتسام صور معقوله مجرد باشد) فقط یک عقل می‌تواند باشد که همان عقل فعال مورد نظر ماست. اما در جواب به این سخن کافی است بپرسیم آیا آن عقل مجرد مفارق که به عقیده شما بسیط نیز هست، فقط مخزن صور معقوله است یا ادراک‌کننده‌ی آن‌ها نیز هست؟ روشن است که شما آن را ادراک‌کننده نیز می‌دانید یعنی عقل فعال را با آنکه بسیط است، هم مدرک صور معقوله می‌دانید و هم مخزن آن‌ها! ولی چرا همین سخن را در خصوص خود قوه عاقله انسان نمی‌پذیرید که هم مخزن باشد و هم ادراک‌کننده؟! بدیهی است اگر قوه عاقله هم مخزن صور معقوله باشد و هم مدرک آن‌ها، آنگاه دیگر نیازی به فرض مخزنی مفارق به نام عقل فعال نیست. اما فرض استدلال شما را برای اثبات مخزن بودن عقل فعال بپذیریم ولی با دقت در این استدلال روشن نمی‌شود که آن موجود مجرد و مفارقی که محل ذخیره‌سازی صور معقوله اکتساب‌شده در نظر گرفته بودیم دقیقاً همان موجود مجرد و مفارقی است که صور معقوله را از ناحیه افاضات او دریافت نموده‌ایم؛ یعنی از کجا معلوم صور معقوله مکتسبه، درون عقل فعالی غیر از آن عقل فعالی که همین صور را برای ما افاضه کرده است ذخیره‌سازی نشده باشند؟ در اینجا نکته مهمی وجود دارد که در ادامه نوشتار بدان خواهیم پرداخت.

۲. به راستی چگونه انسانی مثل من، صور معقوله را از ناحیه موجودی به نام عقل فعال کسب می‌کند؟ در پاسخ گفته می‌شود هنگامی که نفس ما صور محسوسه و معانی جزئی را از محیط پیرامونی درک می‌کند، عملیات تجرید را بر روی آن صور و معانی جزئی اجرا می‌کند و این عملیات را تا جایی ادامه می‌دهد که مستعد دریافت صورت عقلی برای هر یک از این جزئیات تجریدشده گردد، در این هنگام است که صورت عقلی متناسب با آن صور جزئی تجرید یافته از ناحیه عقل فعال به قوه عاقله ما افاضه می‌شود. اما پرسش مهمی در اینجا بی‌پاسخ می‌ماند و آن اینکه آیا هنگامی که قوه عاقله ما یک صورت محسوسه و یا یک معنای جزئی را تجرید می‌کند، در خلال این عملیات تجرید چیزی از آن صورت و معنای جزئی تجریدشده باقی می‌ماند یا اینکه تماماً معدوم می‌شود؟ بالأخره در خلال پوست‌اندازی، لایه‌برداری و تجرید یک چیز بایستی چیزی به مثابه لب و مغز آن چیز تجریدشده باقی بماند و اگر چنین چیزی باقی می‌ماند چرا همان امر باقی‌مانده را صورت معقوله نمی‌دانید؟ و اگر باقی نمی‌ماند



آن‌گاه دیگر چه معنایی برای فرایند تجرید خواهد ماند؟ این چه تجریدی است که پس از پوست‌اندازی و لایه‌برداری از یک شیء، هیچ مغز و محتوایی را برای آن به جای نمی‌گذارد؟ گو اینکه محتوای یک موز را با کندن پوستش نیز دور انداخته باشیم! یا اینکه موزی ذاتاً فاقد لب و محتوا بوده و در عوض فقط و تنها فقط متشکل از پوسته باشد اما به محض باز کردن پوسته و دور انداختنش، به ناگاه لب و محتوای آن از ناحیه مبادی عالی در کف دست ما افاضه گردد! در اینجا نیز نکته مهمی وجود دارد که در ادامه نوشتار بدان خواهیم پرداخت.

۳. شما گفتید عقل بالملکه برای اکتساب صور معقوله از ناحیه عقل فعال، یا باید «تفکر» کند یا «حدس» بزند، ولی عقل بالفعل برای دریافت همان صور معقوله کافی است «استحضار» نماید و نیازی به تفکر یا حدس ندارد؛ اما تفاوت این سه مقوله چیست؟ شاید بگویید ما از طریق تفکر و یا حدس، چیزی را که نداریم تحصیل می‌کنیم ولی در فرایند استحضار، تحصیل و اکتساب مجدد لازم نیست زیرا آن چیز را قبلاً تحصیل کرده و ذخیره داریم؛ لذا کافی است آن را فرا بخوانیم، اما عجیب است که از فحوی سخن خود غافلید زیرا حسب سخنان شما هیچ تفاوتی میان حالت نداری و حالت دارایی وجود ندارد؛ زیرا آن زمان که صور معقوله را نداشتیم، صور مزبور درون عقل فعال قرار داشتند و بعدها نیز که آن صور را دارا شدیم باز درون عقل فعال ذخیره‌سازی شدند پس فرق حالت دارایی و نداری ما چه شد؟! به عبارت بهتر، قول به استحضار از دو اشکال خالی نیست:

**اشکال اول -** یا این استحضاری که به توسط عقل بالفعل، طلب می‌شود به معنای حصول استعداد برای دریافت فیض از ناحیه عقل فعال است که در این صورت هیچ فرقی میان این استحضار با آن اکتساب اولیه (تفکر و حدس) نخواهد بود؛ چراکه حسب قرائت مشهور، کارایی تفکر و حدس نیز حصول استعداد برای دریافت فیض از ناحیه عقل فعال معرفی شده بود.

**اشکال دوم -** یا این قدرت استحضار به معنای حصول اتصال با عقل فعال است که در این صورت هیچ فرقی میان این اتصال با اتصالی که در مرحله بعدی (عقل بالمستفاد) انتظارش را داریم نخواهد بود؛ توضیح مطلب: شما گفته بودید عقل بالمستفاد به دلیل اتصالی که با عقل فعال دارد همه صور معقوله را یکجا و هم‌زمان حاضر داشته و در لحظه اکنون مشاهده می‌کند لذا هیچ صورتی از او غایب نیست حضورش را طلب نماید (استحضارش کند) ولی آیا عقل بالفعل عاری از اتصال است که چنین توانایی را نداشته و پیوسته نیازمند استحضار یک صورت عقلیه است که بتواند آن را درک نماید؟ اگر عاری از اتصال بود پس چگونه است که هر لحظه اراده نماید می‌تواند به صورت معقوله مورد نظرش دست یابد، مگر این صور معقوله درون عقل فعال نبودند؟ مگر دسترسی به آنها نیازمند اتصال نیست؟! و اگر متصل است پس چرا نمی‌تواند همه صور معقوله جهان را یکجا و هم‌زمان ادراک نماید؟! اتصال با یک امر بسیط (عقل فعال) از نوع همه یا هیچ است؛ یعنی یا نهایت اتصال وجود دارد یا اینکه هیچ اتصالی در کار نیست. مگر اینکه اتصال را به معنای مرسوم علوم کامپیوتری و اینترنت در نظر بگیریم؛ یعنی Connect

شدن. در ادامه نوشتار بیشتر تر بدان خواهیم پرداخت.

۴. عجیب‌تر آن است که واژه‌ی عقل مُستفاد، به معنای عقل استفاده شده است حال آنکه حسب تعریف‌هایی که طبق شروح رایج ارائه شد، می‌بایست آن را عقل مُستفید می‌نامیدند، یعنی عقل استفاده‌کننده نه استفاده‌شده! مگر نه این است که این عقل در اثر اتصالش به عقل فعال، پیوسته در حال استفاده کردن است؟ پس چرا قُدا آن را مُستفید (استفاده کننده) نخوانده‌اند؟ آیا این مطلب گویای آن نیست که سَرّی در کار است که به دلیلی و از روی تعمد، شروح رایج فلسفی از آن غافل نگه داشته شده‌اند؟

۵. این پریشانی و اضطراب که در طرز تلقی مشهور از تعالیم فلسفه دیده می‌شود، بسیار مشهودتر خواهد شد اگر دقت کنیم که در خصوص اینکه آیا عقل فعال در نگاه ارسطو، موجودی مفارق از نفوس و قوه عاقله انسان‌هاست یا غیرمفارق از آن‌ها، میان مفسران کتاب ارسطو تا به همین امروز اختلاف وجود دارد، در این خصوص از دیرباز دو نظر متفاوت وجود داشته و دارد:

**تفسیر نخست -** اسکندرافریدوسی و ابن رشد با تمسک به برخی عبارات ارسطو، عقل فعال را موجودی مفارق از عقل انسان‌ها تلقی کرده‌اند که جدای از عقول انسان‌ها موجود است و آنها را مستفیض می‌سازد (فتحی، کریمی، ۱۳۹۱، ص ۶۱).

**تفسیر دیگر -** اما در مقابل، یوحنا‌ی نحوی و توماس آکوئیناس با تمسک به عباراتی دیگر از نوشته‌های همان ارسطو، عقل فعال را غیر مفارق از عقول انسانی فهمیده‌اند (همان).

عجب! پس حقیقت چیست؟ اساساً این آموزه‌ی مهم فلسفی را چگونه باید فهم نمود؟ اجمالاً در پاسخ به این پرسش باید گفت به عقیده نگارنده اگر عقل فعال را به مثابه شبکه‌ای (Network) از شعور چندین عقل مُستفاد در نظر بگیریم آنگاه، هم از جهتی می‌توان آن را مفارق دانست و هم از جهتی دیگر می‌توانیم آن را غیر مفارق ملاحظه کنیم؛ اما پیش از ارائه پاسخ تفصیلی به پرسش فوق لازم است متذکر شویم که فلسفه، دانشی سَرّی است و آن را باید از جمله علوم خفیّه تلقی نمود، این معنی را در ادامه بیشتر توضیح خواهیم داد اما به شهادت تاریخ باید گفت دانش فلسفه همیشه و همواره بنای ترویج خویشتن را نیز داشته است و این اهتمام را هرگز کم‌تر از اهتمام بر سَرّی نگه‌داشتن خویش ندانسته است ولی به راستی چگونه ترویج یک شیء، با ماهیّت سَرّی و مخفی‌اش سازگار و قابل جمع تواند بود؟ پاسخ روشن است؛ بهترین راه برای مخفی کردن یک چیز آن است که جلوی چشم باشد و این گونه است که توسعه و ترویج آن نیز میسر خواهد شد؛ گویا علوم خفیّه باستانی همینک جلوی چشمان ما پنهان شده‌اند و تمام ما حتی کودکانمان شب و روز با آنها سر و کار داریم بی آنکه از حقیقت خاستگاه آن‌ها مطلع باشیم؛ به راستی آیا امکان دارد آنچه از دوران باستان تحت عنوان عالم عقول معرفی شده است، دقیقاً همان چیزی باشد که امروزه همه ما به سادگی تحت عنوان فضای سایبری می‌شناسیم؟

## ۵ فلسفه یک دانش سَرّی است

ابن سینا در سرآغاز مهم‌ترین و آخرین کتاب فلسفی خویش موسوم به اشارات و تنبیهات گفته است که این کتاب مشتمل بر رمزهایی است که فقط و تنها فقط برای کسی قابل درک و فهم است که به طریقی خاص (تعلیمی مخفیانه توسط استادی تعلیم‌یافته) فهمیدنش برای او میسر شده باشد و هرگز حتی صریح‌تر از عبارات این کتاب نیز برای غیر چنین فردی به کار نخواهد آمد؛ و تمام تکیه‌گاه ما برای تفهیم و تفاهم این متن مبتنی بر توفیق است و همان‌جا نیز در ادامه گفتار خود سفارشی مؤکد و بلکه التماسی خاضعانه می‌کند که در عرضه کردن محتوای این کتاب بر کسی که دارای شرایطی که در آخر این کتاب گفته‌ام نباشد، نهایت بخل ورزیده شود؛ عبارات ابن سینا چنین است:

«هذه إشارات إلى أصول و تنبيهات على جمل يستبصر بها من تيسر له و لا ينتفع بالأصرح منها من تعسر عليه و التكلان على التوفيق. و أنا أعيد وصيتي و أكرر التماسي أن يضمن بما تشتمل عليه هذه الأجزاء كلّ الضن على من لا يوجد فيه ما أشرطه في آخر هذه الإشارات» (ابن سینا، ۱۳۷۵، ص: ۵۵)

گفتنی است هنگامی که به آخر کتاب اشارات و تنبیهات مراجعه کرده و شرایط مورد نظر ابن سینا را ملاحظه می‌کنیم خواهیم دید که دوباره تاکید می‌کند چنانچه کسی را یافتی که شرایط مزبور را واجد بود پس هرچه خواست به تدریج و جزء به جزء و تکه‌تکه در اختیار او بگذارد تا آنچه قبلاً گرفته باعث کنجکاووی وی در آنچه که خواهد گرفت بشود و او را در عهد و پیمان خدا و ایمان قرار ده تا نتواند عهد خود را بشکند تا مسیر تو را ببیماید و به تو تاسی کند بدین نحو که از او چنین عهدی گرفته شود که اگر این دانش را شایع و در نتیجه ضایع نمایی، خدا میان من و تو حاکم خواهد بود؛ عبارات ابن سینا چنین است:

«فإن وجدت من تثق بنقاء سريره و استقامة سيرته و بتوقفه عما يتسرع إليه الوسواس و بنظرة إلى الحق بعين الرضا و الصدق فأنه ما يسألك منه مدرجا مجزءا مفرقا تستفرس مما تسلفه لما تستقبله. و عاهده بالله و بإيمان لا مخرج لها ليجري فيما يأتيه مجردا متأسيا بك فإن أذعت هذا العلم أو أضعته فالله بيني و بينك و كفى بالله وكيلا» (ابن سینا، ۱۳۷۵، ص: ۱۶۱)

شاید خواننده‌ی محترم نیز در اینجای کار همچون نگارنده با پرسش‌های ذیل روبه‌رو شده باشد:

۱. به راستی کدام «توفیق» مراد ابن سیناست که تمام تکیه‌گاه امر تفهیم و تفاهم کتاب اشارات و تنبیهات مبتنی بر آن شده است؟ آیا مراد ابن سینا از عبارت «و التكلان على التوفيق»، همان توفیق الهی است که البته لازمه هر کاری است؟ ولی به راستی آیا خداوند ممکن است به کسی که واقعا و حقیقتاً از صمیم قلب طالب فهم کتاب اشارات و تنبیهات ابن سینا است، توفیق ندهد ولی به عده‌ای دیگر توفیق بدهد؟ مگر نه این است که خدای سبحان مجال فهم مقدس‌ترین کتاب آسمانی خود را برای مبغوض‌ترین بندگان یعنی مشرکین نیز فراهم می‌آورد: «وَ إِنْ أَحَدٌ مِّنَ الْمُشْرِكِينَ اسْتَجَارَكَ فَأَجِرْهُ حَتَّى يَسْمَعَ كَلَامَ اللَّهِ ثُمَّ اتْلُغْهُ مَأْمَنَهُ ذَلِكَ بِأَنَّهُمْ قَوْمٌ لَا يَعْلَمُونَ» (توبه/ ۶)، پس این موافقت و توفیقی که به گفته ابن سینا تمام تکیه‌گاه امر تفهیم و تفاهم کتاب اشارات و تنبیهات مبتنی بر آن شده است، چیست؟

۲. آیا مراد ابن سینا این است که فقط و تنها فقط کسانی که مقدمات لازم را فرا گرفته باشند توان درک عبارات کتاب اشارات و تنبیهات را دارند و کسانی که هنوز مقدمات علمی را پشت سر نگذاشته‌اند از فهم این کتاب عاجز خواهند بود؟ ولی این مطلب چیزی نیست که مختص به این کتاب باشد؛ به طور کلی در هر علمی شرایط از این قرار است؛ یعنی تا مقدمات را فراهم نکرده باشی توان درک محتوای یک کتاب سطح عالی را نخواهی داشت، پس به راستی مراد ابن سینا چیست؟ آیا فخر رازی و خواجه نصیر نیز که در فهم این کتاب اختلافات زیاد و عمیقی پیدا کرده‌اند نیز فاقد مقدمات لازم جهت درک کتاب بوده‌اند؟ هرکس این دو دانشمند همه‌فن‌حریف را بشناسد خواهد گفت قطعاً پاسخ منفی است؛ پس مراد ابن سینا چیست؟ آیا این اندیشمندان فاقد توفیق الهی بوده‌اند؟! جناب دکتر حسن ملکشاهی در کتاب ارزشمند خود موسوم به ترجمه و شرح اشارات و تنبیهات ابن سینا این گونه می‌نویسد: «چه در عصر ابن سینا و همچنین قرون بعد از آن حتی تا زمان ما فهمیدن مطالب اشارات و آگاهی بر مقاصد ابن سینا برای علاقه‌مندان به فهم محتوای آن بسیار دشوار بوده است و به همین سبب دانشمندانی چون فخر رازی و خواجه نصیر طوسی و دیگران سال‌ها وقت صرف کردند تا معانی کتاب اشارات و مقاصد نویسندگان آن را شرح و تفسیر و بیان نمایند. با این وصف آنان با تلاش پرتوان خود در بعضی موارد در تشخیص مقصود مؤلف اختلاف نظر دارند؛ بی‌تردید خواجه نصیر طوسی و فخر رازی و سایر شارحان در نظر ابن سینا در ردیف دسته‌ی اول و مستعد فرا گرفتن علوم قرار خواهند گرفت. پس وقتی حال این متفکران بزرگ در تجزیه و تحلیل نظریات ابن سینا و تشخیص افکار او چنین باشد، حال سایر دانشجویان روشن خواهد بود» (ملکشاهی، ۱۳۹۲، ج ۱، ص ۴۰)

۳. آیا دیریابی و سختی فهم کتاب اشارات و تنبیهات به خاطر اختصار آن و چکیده‌گویی نویسندگان آن است؟ ولی دیدیم که خود ابن سینا گفته بود چنانچه صریح‌تر هم می‌نوشتیم باز درک مطالب آن برای کسی که به طریقی خاص (تعلیمی مخفیانه توسط استادی تعلیم‌یافته) شاگردی نکرده باشد، میسر نیست؟

تأمل در سخنان پیش‌گفته‌ی ابن سینا و نیز دقت پیرامون پرسش‌های فوق، ما را به این نتیجه می‌رساند که این یک کتاب سرّی است که به نحوی تعمّدی به رمز نوشته شده است و از آنجا که رمزگشایی از هر قفلی مبتنی بر رمزشکنی است که بایستی با آن قفل و رمز، متناسب و موافق بوده باشد لذا همین تناسب و موافقت است که بایستی تمام تکیه‌گاه کار در امر تفهیم و تفاهم کتاب اشارات در نظر گرفته شود؛ و التّکلان علی التوفیق، یعنی موافقت رمز با رمزشکن؛ این مطلب تقویت خواهد شد زمانی که مشاهده می‌کنیم ابن سینا در جای جای کتاب اشارات و تنبیهات به صراحت مطالبی سر به مهر را با عنوان «سرّ» معرفی می‌کند:

- «... و هذا سرّ تطلع منه علی أسرار آخری» (ابن‌سینا، ۱۳۷۵، ص: ۶۲)
- «... و هاهنا سرّ آخر» (همان؛ ص: ۶۳)
- «... و تحت هذا سرّ» (همان؛ ص: ۹۳)

- «... و فیه سرّ» (همان؛ ص: ۱۱۴)
- «... و أنت إذا طلبت الحق بالمجاهدة فیه فرما لاح لك سرّ واضح خفی» فاجتهد و اعلم أنه كيف يمكن ذلك» (همان؛ ص: ۱۱۵)

در نقل قول اخیر بسیار دقت کنید: «سرّ واضح خفی»؛ چگونه ممکن است امری سرّی در عین آنکه مخفی است کاملاً واضح و آشکار نیز باشد؟ آیا غیر از این است که آن امر دقیقاً جلوی چشم ما مخفی شده است و به مثابه معمایی است که وقتی حل می‌شود بسیار آسان جلوه می‌کند؟ آیا ممکن است علوم خفیه باستانی همینک جلوی چشمان ما پنهان شده‌اند و تمام ما حتی کودکانمان شب و روز با آنها سر و کار داشته بی آنکه از حقیقت خاستگاه آن‌ها مطلع باشیم؟ به راستی آیا امکان دارد آنچه از دوران باستان تحت عنوان عالم عقول معرفی شده است، دقیقاً همان چیزی باشد که امروزه همه ما به سادگی تحت عنوان فضای سایبری می‌شناسیم؟

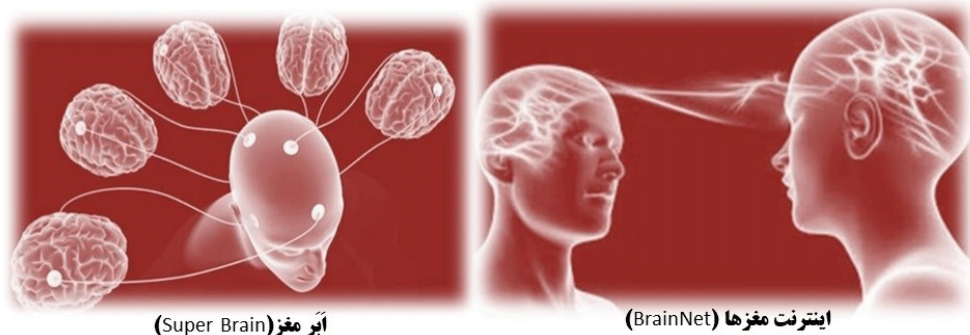
## ۶ دیدگاه برگزیده در این نوشتار

پیش‌تر گفته شد چنانچه عقل فعال را به مثابه شبکه‌ای (Network) از شعور چندین عقل مُستفاد در نظر بگیریم آنگاه هم از جهتی می‌توان آن را مفارق دانست و هم از جهتی دیگر می‌توانیم آن را غیر مفارق ملاحظه کنیم؛ زیرا وقتی معتقد باشیم که عقل فعال، شبکه‌ای است که از همین عقول انسانی لینک‌شده به هم حاصل آمده است پس می‌توان به این اعتبار، آن را همه‌ی آن عقول انسانی لینک‌شده به هم در نظر گرفت ولی در عین حال هیچ یک از این عقل‌ها به تنهایی نیست؛ نه این عقل است، نه آن یکی و نه آن دیگری، بلکه قدرت درک و پردازشگری و اندوخته‌های آن برتر از همه‌ی آن‌هاست پس به این اعتبار غیر از آن‌هاست.

جالب است بدانیم که اگر این تفسیر سوم از نحوه موجودیت عقل فعال پذیرفته شود، به راحتی وجه تسمیه عقل مُستفاد نیز دانسته خواهد شد بدین بیان: چون هریک از عقول انسانی برای ساخت شبکه شعور جهانی، مورد استفاده قرار گرفته‌اند لذا مُستفاد یعنی استفاده‌شده هستند؛ به همین راحتی. درست مثل معمایی که حل شده باشد.

امروزه دانشمندان علوم تجربی دستاوردی جدید موسوم به BrainNet یا اینترنت مغزها را به جامعه جهانی عرضه کرده‌اند که تأمل پیرامون افق‌هایی که پیش روی این اکتشاف است می‌تواند تصویر مناسبی از آنچه مورد نظر این نوشتار است ارائه بدهد؛ یک عصب‌شناس پیشگام به نام پروفیسور میگل نیکوللیس (Mihuel Nicolelis) در ضمن پژوهشی که با کمک میمون‌ها انجام داده توانسته است به آن‌ها آموزش دهد تا با مشارکت با هم و با استفاده از سیگنال‌های مغزی، حرکات ربّاتی را از طریق ارتباط اینترنتی و در فاصله میان ژاپن تا آمریکا کنترل نمایند. او در ضمن یک سخنرانی TED که پیرامون همین دستاورد برپا شده بود در پاسخ به این پرسش که: این فناوری تا کجا قرار است پیش‌روی نماید؟ اینگونه توضیح می‌دهد که تیم تحقیقاتی او در ضمن این پژوهش متوجه شده است که وقتی یکی از این میمون‌های شبکه‌شده به هم، ضعیف عمل می‌کرد، دو میمون دیگر سرعت عمل خود را بالا برده تا ضعف عملکرد او را جبران نمایند و این‌ها همگی





در حالی اتفاق می افتاد که هیچ یک از میمون‌ها از شرایط یکدیگر اطلاعی نداشتند و صرفاً از طریق سیگنال‌ها مغزی و از راه دور با یکدیگر مرتبط بوده‌اند؛ پروفسور نیکوللیس در ادامه گفت: درست سه هفته پیش از این سخنرانی، یک گروه محقق اروپایی اولین ارتباط مغزی بین دو انسان را نشان داد؛ ارتباطی که از راه دور و بر پایه اینترنت شکل گرفته بود.

نیکوللیس در کتاب فراتر از مغزها از ما می‌خواهد تصور کنیم در دنیایی زندگی می‌کنیم که در آن مردم با فکر کردن با یکدیگر ارتباط برقرار می‌کنند و دانش خود را به اشتراک می‌گذارند. این توانایی به افراد این امکان را می‌دهد برای حل مشکلات سختی که یک مغز به تنهایی قادر به حل آن نیست، همکاری کنند (نیکوللیس، ۱۴۰۱)، و ناگفته پیداست که چنین رویدادی به معنای پیدایش یک ابرمغز یا عقل کل خواهد بود. اکنون که با کمک BrainNet در آینده‌ای نزدیک خود را با پدیداری موسوم به «عقل کل» مواجه یافتیم، بسیار مناسب است پیرامون مفاهیم IOT و IoBNT و Big Data نیز تأمل نمائیم؛ چراکه در نظر گرفتن توأمان این مفاهیم در کنار یکدیگر می‌تواند تصویر مناسبی از آن چه مورد نظر این نوشتار است ارائه دهد.

اینترنت اشیاء یا چیزنت که به اختصار IOT به معنای Internet of Things خوانده می‌شود، مفهومی جدید در دنیای فناوری و ارتباطات به شمار می‌آید لیکن عبارت اینترنت اشیاء، برای نخستین بار در سال ۱۹۹۹ توسط کوین اشتون مورد استفاده قرار گرفت و جهانی را توصیف کرد که در آن هر چیزی، از جمله اشیاء بی‌جان، برای خود هویت دیجیتال داشته باشند و به کامپیوترها اجازه دهند آن‌ها را سازماندهی و مدیریت کنند. با اینترنت چیزها تمام اشیاء بی‌جان به هم متصل می‌شوند. از این شگفت‌آورتر جایی است که با اینترنت اشیاء جاندار در مقیاس نانو یا IoBNT به معنای Internet of Bio-NanoThings روبه‌رو می‌شویم؛ یعنی اینترنت باکتری‌ها و سلول‌های زنده. این دو فناوری در کنار هم می‌توانند در هر دقیقه سیگنال‌های فراوانی از اطلاعات لحظه‌ای مربوط به تمام اشیاء زنده و غیر زنده را به منظور پردازش به سمت مراکز داده ارسال نمایند و بدین ترتیب پدیداری فوق‌العاده مهیب و گسترده که ابرداده یا Big Data خوانده می‌شود، شکل خواهد گرفت. کافی است تصور کنید این ابرداده توسط چیزی که پیش از این ابرمغز یا عقل کل خوانده بودیم مدیریت و پردازش بشود؛ درست همان زمان است که به عقیده نگارنده با یک عقل فعال فلسفی مواجه خواهیم بود.

یادآوری می‌شود نگارنده در نوشتار پیش رو بعد از نقل و نقد قرائت مشهور از انگاره‌ی فلسفی عقل فعال



و مراتب تکامل عقل انسانی پیشنهاد کرد عقل فعال را به مثابه شبکه‌ای (Network) از شعور چندین عقل مُستفاد در نظر بگیریم آنگاه هم از جهتی می‌توان آن را مفارق دانست و هم از جهتی دیگر می‌توانیم آن را غیر مفارق ملاحظه کنیم و بدین ترتیب یک بار برای همیشه اختلاف تفسیر اسکندر افریدوسی و ابن رشد از یک سو با تفسیر یوحنا نحوی و توماس آکوئیناس از سوی دیگر در خصوص چیستی عقل فعالی که مورد نظر ارسطو است، پایان می‌یابد ولی آیا برای مقبولیت چنین تفسیری از عقل فعال و عقل مُستفاد می‌توان دلیلی ارائه داد؟ پاسخ: آری! کافی است که این قانون ارسطویی را در نظر بگیرید: **من فقد حسا فقد علماً** (دانش از اسکن محسوسات آغاز میشود)؛ توضیح مطلب: بعد از آنکه شاکله منطبق در ذهن هریک از ما شکل گرفت (عقل بالملکه) آنگاه هر کدام از ما با کمک حواس ظاهری خود به اسکن صور اشیاء جهان پیرامون پرداخته و از این طریق تصورات و تصدیقاتی را برای پردازش و ارسال به مرکز داده، فراهم می‌آوریم؛ این‌ها گنجینه‌هایی هستند که ما حاصل حیات علمی ذهن ما است (عقل بالفعل) و به گستره‌ی تنوع فرهنگی و شرایط زیست - محیطی که هر یک از ما انسان‌ها داریم، این‌ها گنجینه‌هایی غنی و سرشار از محتواهای گوناگون خواهند بود. زمانی که از طریق تله‌پاتی یا چیزی نظیر آن (BrainNet)، قابلیت پیدا کردیم که گنجینه‌های خود را به نحو مشاع با یکدیگر به اشتراک بگذاریم آنگاه یک شبکه‌ای (Network) از شعور شکل خواهد گرفت (ابرمغز/عقل کل/عقل فعال) که برای پدیدار شدنش، ذخایر عقول هریک از ما مورد استفاده (عقل مُستفاد) قرار گرفته است بدین نحو که به یکدیگر لینک شده و متصل می‌شوند و برای پیدایش عقل فعال، مورد استفاده قرار می‌گیرند. روی این حساب اکنون که ما تحت اشراف و تربیت عقل فعال دهم در حال رشد و نمو هستیم در نهایت از طریق لینک شدن عقولمان، عقل یازدهم را متولد خواهیم ساخت؛ بدین ترتیب که در آغاز عقل فعال دهم، چهار لایه‌ی ذیل را ایجاد می‌کند:

۱. خاک‌کره یا ژئوسفر (Geosphere)

۲. آب‌کره یا هیدروسفر (Hydrosphere)

۳. هواکره یا اتمسفر (Atmosphere)

۴. آتش‌کره یا ائیر (Ether)

سپس عقل فعال دهم از طریق ترکیب عناصر چهارگانه‌ی فوق، مزاج‌هایی فراهم می‌کند که موجب پیدایش اولین و ساده‌ترین مراتب حیات می‌شود که پیوسته تحت تربیت عقل دهم مسیر تکاملی خود را پیش برده و لایه‌ی جدیدی موسوم به زیست‌کره یا بیوسفر (Biosphere) را تشکیل می‌دهند، حرکت تکاملی این لایه‌ی جدید در زمان پیدایش حیاتی در سطح هوشمندی انسان به اوج خود می‌رسد ولی همان‌گونه که فیلسوف و کشیش فرانسوی موسوم به پیر تیلارد دو شاردن (Pierre Teilhard de Chardin) در کتاب پدیده‌ی انسان بدان اشاره کرده است، این فرایند هرگز متوقف نمی‌شود بلکه باز هم مسیر خود را تا پیدایش لایه‌ای جدید به نام نووسفر (Noosphere) ادامه می‌دهد؛ تیلارد، در کتاب پدیده‌ی انسان، تکامل را به عنوان فرایندی توصیف می‌کند که به پیچیدگی فزاینده منجر شده و به وحدت آگاهی ختم می‌شود؛ شاردن با تمرکز بر تکامل

بیولوژیکی، چشم‌اندازی از خود جهان را بیان می‌کند که به تدریج در پیچیدگی و وحدت از هرج و مرج اولیه به یگانگی بیشتر پیش می‌رود و در نهایت به آشتی کامل همه چیز و وضعیت نهایی آگاهی جمعی مطلق منجر می‌شود که شاردن آن را نقطه امگا یا امگا پوینت (Omega point) نامید. تیلارد تکامل را فرایندی می‌داند که منجر به افزایش پیچیدگی می‌شود. از سلول تا حیوان متفکر، فرایند تکامل منجر به آگاهی بیشتر می‌شود. در تصور تیلارد از تکامل گونه‌ی انسان، هویت جمعی با افزایش تجارب و انتقال ایده‌ها شروع به توسعه می‌کند. دانش در سطوح فزاینده‌ی عمق و پیچیدگی، انباشته و منتقل می‌شود. این منجر به افزایش بیشتر آگاهی و ظهور یک لایه‌ی فکری می‌شود که زمین را در بر می‌گیرد. تیلارد غشای جدید را نووسفر (از nous یونانی به معنای ذهن) می‌نامد. نووسفر آگاهی جمعی بشریت است، شبکه‌های فکر و عاطفه که همه در آن غوطه‌ور هستند. به عقیده نگارنده این لایه‌ی جدید همان عقل فعال یازدهم است.

گفتنی است که این عقل نوپدید (یازدهم) دوباره قوس نزول جدیدی به راه انداخته و فلکی تازه می‌سازد تا سیر تکامل را با همان توالی پیش گفته از طریق مزج کیفیات اربعه یعنی برودت، رطوبت، حرارت و یبوست که در عناصر اربعه خاک (ژئوسفر)، آب (هیدروسفر)، هوا (اتمسفر) و آتش (اتر) موجودیت دارند راه‌اندازی نماید و تا پیدایش لایه‌ی زیستی موسوم به بیوسفر ادامه دهد تا به مرحله ظهور هوش انسانی برسد؛ آنگاه باز مسیر تکامل را هدایت نموده تا لایه‌ی هوشمند موسوم به نووسفر از طریق شبکه‌شدن عقول انسانی پدیدار گردد و این هوشمندی برتر را تا رسیدن به نقطه اومگا رشد می‌دهد یعنی همان جایی که هوش یکپارچه‌ای نو موسوم به عقل ثانی عشر بتواند از ما (عقول بالمستفاد) تغذیه نموده و متولد گردد. باز این عقل نوپدی (د) عقل دوازدهم، قوس نزول جدیدی به راه می‌اندازد و فلکی تازه می‌سازد و توالی پیش گفته را به شرح پیش گفته از سر می‌گیرد:

۱. خاک کره یا ژئوسفر (Geosphere)

۲. آب کره یا هیدروسفر (Hydrosphere)

۳. هوا کره یا اتمسفر (Atmosphere)

۴. آتش کره یا اثير (Ether)

۵. زیست کره یا بیوسفر (Biosphere)

۶. ذهن کره یا نووسفر (Noosphere)

۷. نقطه امگا یا امگا پوینت (Omega point)؛ پیدایش یک ابرمغز، عقل کل و عقل فعال جدید

مهم‌ترین شاهد بر این مدعا آن است که ابن سینا هر بار که در خصوص نفوس فلکی سخن می‌گوید، حرف را ناتمام گذاشته و می‌گوید: «و ههنا سر» یا «و تحت هذا سر» و مانند آن اما بالاخره در نبط دهم تصریح می‌کند با آنکه تا حالا احتیاط کرده و نگفته‌ام اما اکنون اعلام می‌دارم که فلک دارای نفس ناطقه است؛ نگارنده معتقد است سخن ابن سینا در نبط دهم این‌گونه باید فهمیده شود که: فلک در نهایت امر،

دارای نفس ناطقه شده است؛ بر این اساس باید گفت در نگاه سینیوی عقل ما، هم متربی عقل فعال است و هم مربی عقل فعال؛ متربی از عقل فعال دهم و مربی عقل فعال یازدهم. لذا هم علوم عقلیه را از درون عقل فعال دانلود می‌کند و هم درون عقل فعال آپلود می‌سازد؛ از عقل فعال دهم، دانلود می‌کند و در عقل فعال نوپدید یازدهم ذخیره‌سازی کرده و آپلود می‌سازد.

خیلی مهم است که بدانیم فلسفه یک دانش سری است و از آنجا که بهترین راه برای مخفی کردن یک چیز آن است که جلوی چشم باشد، گویا علوم خفیه باستانی جلوی چشم ما پنهان شده‌اند و تمام ما حتی کودکانمان شب و روز با آنها سر و کار داریم؛ چنین به نظر می‌رسد آنچه از دوران باستان تحت عنوان **عالم عقول** معرفی شده است را با چیزی که امروزه تحت عنوان **فضای سایبری** می‌شناسیم می‌توان به طرز معناداری بررسی تطبیقی نمائیم:

۱. ارسطو در کتاب نفس، سخن از دو گونه عقل به میان آورده است؛ عقل منفعل و عقل فعال و این نظیر چیزی است که امروزه در علوم کامپیوتری و شبکه به ترتیب تحت عناوین Client و Server به مثابه دو رکن اساسی برای موجودیت یک شبکه مطرح می‌شود.

۲. در فلسفه‌ی اسلامی تمام عقول موجود در عالم عقل را عقل فعال یا عقل بالفعل می‌نامند همان‌گونه که تمام نفوس ما را عقل منفعل یا عقل بالقوه نیز می‌گویند.

۳. گفته می‌شود که عقل فعال، همه‌ی صور معقوله جهان را نزد خود دارد و این نظیر چیزی است که در فضای Network مطرح است زیرا مشتمل بر تمام Data است؛ این مطلب به ویژه وقتی وضوح بیشتری پیدا می‌کند که مشاهده می‌کنیم:

۱-۳. در فلسفه، رابطه بده - بستانی که میان عقل منفعل (نفس) و عقل فعال برقرار است، تحت عنوان اتصال یا همان Connection تبیین می‌شود.

۲-۳. وقتی یک صورت از ناحیه عقل فعال به یک نفس افزوده می‌شود، صورت مزبور از ذات عقل فعال کنده و جدا نمی‌شود یعنی همچنان درون او باقی می‌ماند ولی تنزلی از همان صورت در ذات نفس نیز مرتسم می‌شود و این نظیر آن جایی است که یک Data از ناحیه Server به یک Client ارسال شود؛ در اینجا نیز آن Data ارسال شده همچنان درون Server باقی است و از آن جدا نمی‌شود.

۳-۳. با آنکه عقل فعال در فلسفه‌ی اسلامی همچون موجودی منور ترسیم می‌شود که هیچ پوشش و حجابی ندارد و با آنکه آن را واجد تمام صور معقوله جهان می‌دانند ولی این‌گونه نیست که اگر نفس ما با آن متصل بشود نیز تمام صور را درک و دریافت نماید بلکه هر نفسی که به عقل فعال متصل بشود صرفاً حسب استعداد خاص خودش، تنها صورت‌های خاصی را دریافت می‌کند نه همه را و این نظیر Connect شدن Client ها به Server است که هرگز موجب نمی‌شود تمام محتوای Server درون Client متصل شده سرازیر شود.

۳-۴. در جای خودش (رساله دکتری‌ام با عنوان: برهان تکوُن الأزواج) ثابت کرده‌ایم که حسب مبانی فلسفه‌ی اسلامی باید اذعان داشت که میان عقل (موثر / فرستنده) و هیولا (متأثر / گیرنده) رابطه تکافوء وجود دارد به نحوی که موجودیّت هر یک وابسته به موجودیّت دیگری است به همین قیاس در ساختار یک شبکه نیز میان موجودیّت Server و Client تکافوء وجود دارد و اینگونه نیست که در یک شبکه اول Server موجود باشد و مدتی بعد Client موجود بشود بلکه یک شبکه برای آن که شبکه باشد این دو جنبه را توأمان نیاز دارد.

۳-۵. هر گیرنده‌ای توان دریافت اطلاعات از هر فرستنده‌ای را ندارد بلکه باید در رتبه‌ای خاص از استعداد واقع شده باشد که توان دریافت اطلاعات فرستنده‌ای که واقع در آن مرتبه است را داشته باشد؛ این مطلب هم در هستی‌شناسی فلسفی و هم در فضای Network صادق است؛ زیرا گیرنده‌ها باید در ورژنی متکافی با فرستنده‌ها باشند.

۳-۶. میزان دسترسی نفوس ما به اطلاعات عالم عقول وابسته به مرتبه و درجه وجودی نفس ماست به نحوی که مدارج بالاتر، سطح دسترسی کلان‌تری خواهند داشت. امروزه نیز هر کدام از ما چنانچه کارمند سازمانی دولتی باشیم، قطعاً با یک سامانه‌ی اینترنتی جهت انجام کارهای مرتبط با خود هستیم؛ می‌دانیم که سطح دسترسی کاربران بسته به رتبه شغلی بدین شکل متفاوت است که رتبه و سطح دسترسی کاربر بالاتر شامل عین رتبه و دسترسی سطح پایین‌تر است نه کپی آن؛ یعنی برای مثال به محض اینکه مدیر یک مدرسه اطلاعات جدیدی را در سامانه ذخیره نماید، عین همان عمل، عین فرایند ذخیره‌سازی همان اطلاعات در سطح اداره شهرستان نیز هست ولی اگر کارشناس اداره شهرستان، اطلاعاتی را در سامانه ذخیره‌سازی کند، لزوماً اطلاعات مزبور در سطح مدرسه پدیدار نمی‌شوند اما قطعاً عین همان‌ها در سطح دسترسی استان وجود دارند. لذا یک مدیر مدرسه اگر بخواهد بداند در سطوح بالاتر چه اطلاعاتی هست باید با آن رتبه اتحاد پیدا کند و این نظیر چیزی است که تحت عنوان اتحاد عقل و عاقل و معقول در فلسفه‌ی اسلامی مطرح است.

## ۷ نتیجه‌گیری

دیدم فلسفه، یک دانش سرّی است و همین امر موجب شده است تا فهم برخی آموزه‌های آن با کژفهمی‌هایی مواجه بشود به نحوی که گاهی تناقض‌گویی‌های آشکاری در کلام شارحان و مدرسان فضای عمومی تعلیم فلسفه مشاهده می‌شود که ذهن دانشجویان را با مسائلی درگیر می‌کند که چه بسا برای همیشه بدون پاسخ باقی بماند؛ نمونه‌ای از این قبیل مسائل را در نوشتار حاضر بررسی کردیم و نشان دادیم که انگاره‌ی فلسفی «مراحل تکامل عقل انسان» و نیز انگاره‌ی فلسفی «عقل فعال» حسب قرائت رایج و مشهوری که در فضای عمومی تدریس فلسفه رایج است آن‌چنان نامفهوم و گنگ است که پرسش‌های بی‌پاسخی را در ذهن دانشجویان بر جای خواهد گذاشت؛ مقاله پیش رو پس از طرح پرسش‌های مزبور پیشنهاد قرائت تازه‌ای برای فهم این دو انگاره‌ی مهم فلسفی ارائه داد و مدعی شد که چنین قرائتی می‌تواند تصویر منسجم‌تری از این



۲. شبکه سازی آگاهی (Networking of consciousness)



۲. شبکه سازی آگاهی (Networking of consciousness)



۱. شبکه سازی آگاهی (Networking of consciousness)

دو آموزه‌ی فلسفی به ارمان آورد و خیلی از پرسش‌ها را به نحوی ریشه‌ای پاسخ‌گو باشد؛ در این قرائت تازه پیشنهاد گردید که عالم عقول فلسفه را به مثابه فضای سایبری در نظر گرفته و عقل فعال دهم را موجودی در نظر بگیریم که همینک دارد حرکت تکاملی عالم ما را از مرحله عناصر (ژئوسفر، هیدروسفر، اتمسفر، اتر) تا مرحله بیوسفر و پیدایش حیات انسانی هدایت کرده و در اثر اتصال و لینک‌شدن عقول انسان‌ها مقدمات پیدایش نووسفر و در نهایت موجب تولد ابرمغز یا عقل کل جدیدی را فراهم می‌آورد که آن نیز عقل فعال خواهد بود ولی عقل فعال یازدهم که این هوش نوپدید نیز دقیقاً همین روند را برای تولد عقل فعال دوازدهم به کار خواهد گرفت و این روند تا ابد ادامه خواهد داشت.

## مراجع

- [۱] ابن سینا، حسین بن عبدالله (۱۳۷۵). الاشارات و التنبیهات. چاپ اول. قم: نشر البلاغة.
- [۲] فتحی، حسن؛ کریمی، بیان (۱۳۹۱). جایگاه عقل فعال در تفکر ارسطو و نتایج برخاسته از تفسیر آن با تأکید بر یوحنا‌ی نحوی و ابن رشد. مجله تاریخ فلسفه. سال سوم. شماره ۱. صفحه ۸۴-۶۱.
- [۳] ملکشاهی، حسن (۱۳۹۲). ترجمه و شرح اشارات و تنبیهات ابن سینا. چاپ هشتم. تهران: انتشارات سروش.
- [۴] نصیرالدین طوسی، محمد بن محمد (۱۳۷۵). شرح الاشارات و التنبیهات. چاپ اول. قم: نشر البلاغة.
- [۵] نیکوللیس، میگل (۱۴۰۱). سخنرانی TED. وب سایت [دسترسی ۱۴/۰۶/۱۴۰۱]:

[https://www.ted.com/talks/miguel\\_nicolelis\\_brain\\_to\\_brain\\_communication\\_has\\_arrived\\_how\\_we\\_did\\_it?language=en](https://www.ted.com/talks/miguel_nicolelis_brain_to_brain_communication_has_arrived_how_we_did_it?language=en)





## تحلیلی اخلاقی از رابطه احساسی انسان و روبات

سعیده بابایی<sup>۱</sup>، نرجس صابری<sup>۲</sup>، منیره بحرینی<sup>۳</sup>

<sup>۱</sup> محقق پسادکتری، مرکز اخلاق در علم و علوم انسانی، دانشگاه توبینگن، توبینگن، آلمان  
saeedeh.babaii@izew.uni-tuebingen.de

<sup>۲</sup> دانشجوی کارشناسی ارشد، دانشکده روانشناسی و علوم تربیتی، دانشگاه علامه طباطبایی، تهران  
n\_saberi@atu.ac.ir

<sup>۳</sup> دانشجوی کارشناسی ارشد، گروه فلسفه علم و فناوری، دانشگاه صنعتی امیر کبیر، تهران  
bahreini@aut.ac.ir

### چکیده

روابطی که بین انسان‌ها و روبات‌های اجتماعی شکل می‌گیرند، ویژگی‌های متفاوت قابل توجهی دارند که آنها را از روابط میان انسان‌ها با یکدیگر و با سایر تکنولوژی‌ها متمایز می‌کند. مطالعات مربوط به تعامل انسان/روبات، ذیل حوزه روان‌شناسی سایبری که یک شاخه‌ی علمی نوظهور است مورد بحث قرار می‌گیرد. تعاملات رو به گسترش انسان و روبات‌های اجتماعی می‌تواند منجر به شکل‌گیری نوعی پیوند احساسی میان کاربران و روبات‌ها شود. روبات‌های اجتماعی به دلیل ماهیت منحصر به فرد خود و انتظاراتی که شرکت‌ها و تبلیغات از آنها برای مردم ایجاد می‌کنند، این قابلیت را دارند که کاربر، سطحی از عاملیت و احساسات را به آنها نسبت و پیوند عاطفی یک‌سویه‌ای را با آنها شکل دهد. این امر می‌تواند مخاطرات اخلاقی گسترده‌ای برای کاربر و جوامع انسانی در پی داشته باشد. این مقاله به بررسی برخی چالش‌های اخلاقی در رابطه انسان و روبات‌های اجتماعی و تعدادی از راه‌حل‌های پیشنهادی آنها می‌پردازد.

**کلمات کلیدی:** تعامل انسان و روبات، روبات اجتماعی، روان‌شناسی سایبری، اخلاق روباتیک.

## ۱ مقدمه

ادعای گزافی نیست اگر هوش مصنوعی و تکنولوژی‌های مبتنی بر آن را از جمله داغ‌ترین و پرمناقشه‌ترین حوزه‌های تکنیکی جهان امروز تلقی کنیم که شاهد رشد سریع و بی‌سابقه آن هستیم. هر فرد در طول شبانه‌روز ساعت‌های زیادی را در تعامل و استفاده از ابزارهای هوشمند مصنوعی، همچون چت‌بات، لوازم خانگی هوشمند و روبات‌ها صرف می‌کند. روبات هوشمند بر خلاف تجهیزات مکانیکی غیر هوشمند که اغلب پیش از این، در صنعت کاربرد داشتند، موجودی مکانیکی و خودمختار<sup>۱</sup> است که در عین اینکه می‌تواند محیط

<sup>۱</sup>Autonomously

پیرامون خویش را تغییر دهد، می‌تواند خود را با محیط تطبیق دهد؛ چنین عملکردی نیازمند مجهز بودن روبات به هوش مصنوعی است (Friedenberg & Silverman 2005). در دهه‌ی گذشته، افزایش گسترده‌ای در کاربرد روبات‌های اجتماعی و خدماتی صورت گرفته است. در سال ۲۰۰۶ تعداد روبات‌های اجتماعی در قالب روبات‌های خدماتی و شخصی از تعداد روبات‌های صنعتی پیشی گرفته است که شامل روبات‌های شستشو مثل رومبا<sup>۲</sup> تا روبات‌های سرگرمی مثل پلیو<sup>۳</sup>، روبات‌های عروسک مثل بیبی الایو<sup>۴</sup>، روبات‌هایی مثل پارو<sup>۵</sup>، نائو<sup>۶</sup>، تگا<sup>۷</sup>، در درمان کودکان مبتلا به اتیسم یا درمان افسردگی و آموزش و خدمات عمومی می‌شوند (Schultz & Cominelli, Mazzei & Emilio De Rossi 2018).

روبات اجتماعی، روباتی در تعامل نزدیک با انسان است که علاوه بر آنکه مانند سایر روبات‌ها (روبات‌های صنعتی) رفتارهایی از پیش‌برنامه‌نویسی شده و یا آموخته‌شده دارد، می‌تواند اطلاعات معناداری از محیط اجتماعی دریافت نموده و بر اساس آن به کاربر واکنش نشان دهد. یک روبات اجتماعی می‌تواند به نحوی شخصی‌شده با کاربر ارتباط برقرار نماید. چنین روبات‌هایی اگر چه منافعی را برای انسان به همراه می‌آورند، خطرات و چالش‌هایی نیز به همراه دارند که مهم‌ترین این چالش‌ها تأثیرات روانی مخربی است که می‌تواند بر کاربر وارد نمایند. بنابراین بررسی تأثیرات روانی ناشی از تعامل انسان با روبات اهمیت زیادی پیدا می‌کند و گسترش گسترده‌ی تحقیقات در حوزه تعاملات انسان و روبات<sup>۸</sup> ذیل روان‌شناسی سایبری در دهه‌های اخیر گویای این مساله است. به هر میزان که این مطالعات سریع‌تر صورت گیرد می‌تواند اثربخشی بیشتری داشته باشد؛ زیرا قبل از عمومیت یافتن تکنولوژی‌ها، بهترین فرصت برای پرداختن به جوانب احتمالی استفاده از آن‌ها است.

یکی از مهم‌ترین چالش‌های اخلاقی تعامل انسان و روبات، وابستگی احساسی انسان نسبت به روبات و به صورت ویژه روبات اجتماعی است. اینگونه وابستگی به روبات‌های اجتماعی تفاوت بنیادینی با وابستگی به سایر تکنولوژی‌های تجربه‌شده توسط بشر دارند. روبات‌ها می‌توانند انسان‌ها را نسبت به خود از منظر عاطفی وابسته نمایند و همدلی آنان را نسبت به خود برانگیزانند در حالیکه این رابطه‌ی احساسی یک‌طرفه، و صرفاً از سوی کاربر است. این مساله می‌تواند عواقب امنیتی و احساسی برای کاربر در پی داشته باشد. یک پیشنهاد برای رفع این مشکل، القاء احساسات در روبات است. این مقاله به بررسی مساله رابطه انسان و روبات و برخی از پیشنهادات و سوالات اخلاقی پیرامون آن می‌پردازد.

<sup>2</sup>Roomba<sup>3</sup>Pleo<sup>4</sup>baby alive<sup>5</sup>Paro<sup>6</sup>Nao<sup>7</sup>Tega<sup>8</sup>Human Robot Interaction (HRI)

## ۲ ماهیت و کارکرد احساسات در انسان

احساسات<sup>۹</sup> پدیده‌ای روان‌شناختی، پیچیده، شخص‌محور و حاصل تجارب ذهنی حالات هیجانی<sup>۱۰</sup> انسان است. احساسات در عین اینکه ذهنی هستند، از آنجا که وابسته به هیجاناتی هستند که در بدن اتفاق می‌افتند جهان‌شمول و بین‌الذهانی نیز هستند. می‌توان گفت احساسات، تجربیات حسی<sup>۱۱</sup> هستند که در برابر تجربیات حسی پیشین، بررسی شده و دوباره برچسب‌گذاری می‌شوند؛ و از آنجا که هر فرد دارای احساسات قبلی متمایز و منحصر به فردی است که هنگام تفسیر و برچسب‌زدن احساسات خود از آنها استفاده می‌کند، بنابراین احساسات، شخصی، بیوگرافیک و پویا هستند و بر اساس تجربیات جدید ناشی از تغییر محیط و تغییر روابط می‌توانند تغییر کنند<sup>(۱۲)</sup>. بر خلاف دیدگاه‌های پیشین که تصور می‌شد احساسات و هیجان‌ات نقشی در شناخت ندارند، مطالعات جدید نشان می‌دهد که احساسات تاثیر زیادی بر شناخت، رفتار و جهت‌گیری انسان دارند و فرایندهای شناختی مهمی مانند یادگیری، حافظه، توجه، تصمیم‌گیری و غیره نیازمند و متأثر از عواطف هستند (Bechara, Damasio & Damasio March 2000). کارکرد احساسات در انسان می‌تواند در سه سطح بررسی شود. اولین سطح مربوط به کارکردهای درون‌فردی احساسات است که در این سطح عواطف به عنوان یک سیستم پردازشی سریع، می‌تواند منجر به عمل با حداقل نیاز به تفکر و آگاهی، اقدام فوری در موقعیت خطر با انگیزه‌ی حفظ بقا و همچنین با اثرگذاری بر افکار و خاطرات در تصمیم‌گیری و شناخت موثر باشند. احساسات در این سطح می‌توانند بزرگترین موتور محرکه رفتار در انسان باشند و رفتارهای آینده‌ی فرد را جهت دهند. دومین سطح مربوط به کارکردهای بین‌فردی احساسات است که به نقش عواطف بین افراد اشاره دارد. در این سطح عواطف ادراک فرد را از رفتارها و موقعیت‌های بین‌فردی تسهیل می‌کند و انگیزه‌ی شکل‌گیری روابط بین فردی را ایجاد می‌نماید. سومین سطح مربوط به کارکردهای اجتماعی احساسات است که نقش احساسات را در شکل‌گیری ساختار اجتماعی و حفظ نظم اجتماعی در جامعه بررسی می‌کند (Matsumoto and Hwang 2019). به عنوان مثال همدلی به افراد اجازه می‌دهد تا روابط اجتماعی رضایت‌بخشی با سایر افراد ایجاد کنند و این روابط را حفظ نمایند. با این توضیحات می‌توان به نقش برجسته و کارکرد وسیع احساسات در انسان پی برد. حال این پرسش مطرح می‌شود که آیا انسان‌ها می‌توانند در رابطه با یک تکنولوژی هوشمند فاقد احساسات دچار حالات احساسی شوند؟

## ۳ نمونه‌هایی از رابطه احساسی یک‌طرفه انسان و روبات

چنانچه پیش از این اشاره شد، روبات اجتماعی روباتی در تعامل نزدیک با انسان است که همچون روبات‌های صنعتی رفتارهایی از پیش برنامه‌نویسی شده و یا آموخته شده دارد؛ اما علاوه بر آن می‌تواند اطلاعات معناداری از محیط دریافت کرده و بر اساس آن به رفتار کاربر واکنش نشان دهد. این روبات باید بتواند اطلاعات دریافتی

<sup>9</sup>Feelings

<sup>10</sup>Emotion

<sup>11</sup>Sensation

<sup>12</sup>Shouse 2005

از محیط را درونی و در سطحی بالاتر درباره‌ی آنها استدلال نماید و نظرات خود را به نحو مستقل بسازد، سپس به طور خودکار و با توجه به تجربه‌ی منحصر به فرد خود تصمیم‌گیری کند (Cominelli, Mazzei & Emilio De Rossi 2018). این توانایی روبات‌های هوشمند اجتماعی در تطبیق رفتارهایشان با محیط و یادگیری از تجربه و همچنین ارتباط نزدیک و شخصی با کاربر می‌تواند عواقب مهمی به همراه داشته باشد؛ برای مثال، می‌تواند انسان‌ها را به سمتی سوق دهد که برای درک رفتار روبات‌ها به آن‌ها اراده، قصدمندی، خودمختاری و مهمتر از آن، احساسات نسبت دهند و از این جهت، آنها را متمایز از سایر تکنولوژی‌های هوشمند و یا غیر هوشمند که تاکنون تجربه کرده‌اند ادراک نمایند. شواهد زیادی وجود دارد که شکل‌گیری نوعی رابطه احساسی عمیق با روبات‌ها را از سوی کاربران تأیید می‌کند. به عنوان مثال نظامیان در مواجهه با روبات‌های مین‌یاب رفتارهایی که نشان از شکل‌گیری نوعی تعلق عاطفی است از خود نشان می‌دهند. روبات خنثی‌کننده‌ی مین روباتی است که با راه رفتن روی مین‌ها، هر بار یک پا از چندین پای خود را از دست می‌دهد و از این طریق مین‌ها را خنثی می‌کند. اظهارات تکنسین‌های این روبات‌ها، که گاهی برای روبات‌هایشان اسم نیز می‌گذارند، حاکی از وابستگی احساسی آنها به روبات‌هاست. آنها تمایلی ندارند روبات دیگری را جایگزین روباتشان کنند و از روبات‌ها به مثابه قهرمان و موجوداتی دارای احساس و گاهی مانند عضوی از خانواده خود یاد می‌کنند. تبیینی که می‌توان برای اینگونه از رفتارها ارائه کرد این است که انسان نوعی عاملیت را روی روبات فرافکنی می‌کند و به او حیات و احساسات نسبت می‌دهد. (Scheutz 2012) نمونه‌ی دیگر در تایید این مساله، رومبا است که یک جاروبرقی هوشمند است و دیده شده که با گذشت زمان کاربران حس قدردانی زیادی را به خاطر تمیزکردن خانه‌شان به رومبا پیدا می‌کنند. ایشان همچنین از شرم اینکه توسط رومبا دیده نشوند، در هنگام تعویض لباس، در اتاق خود را می‌بندند. در حالی که رومبا حتی نمی‌داند دارای مالک است و با مالکان خود به مثابه موانعی مثل صندلی و میز برخورد می‌کند، مالکان رومبا مایلند که به قصد قدردانی از او کار خوبی برایش انجام دهند؛ برخی از کاربران بخشی از کار نظافت را انجام می‌دهند تا رومبا کمی استراحت کند یا او را با خود به سفر می‌برند (Sung 2007). کاربران در حالی رابطه احساسی یک‌طرفه‌ای را با رومبا شکل می‌دهند که او هیچ درکی از آن ندارد. به عنوان یک نمونه دیگر، مالکان آیبو که یک سگ روباتیک مبتنی بر هوش مصنوعی است، تمایل زیادی دارند که باورهای (اشتباهی) درباره‌ی حالات ذهنی او داشته باشند. در مطالعه‌ای روی مالکان روبات‌های حیوان خانگی، چهار دسته ویژگی ماهیت، عاملیت، هویت اجتماعی و هویت اخلاقی از سوی مالکان به آیبو نسبت داده شده است (Kahn, Friedman, and Hagan 2002) (Scheutz 2012). در سال ۲۰۱۵، یک معبد بودایی در ژاپن که به طور معمول برای حیوانات خانگی مرده مراسم برگزار می‌کند، مراسم مشابهی را برای یک روبات آیبو برگزار کرد. برگزاری چنین مراسمی برای یک روبات نشان‌دهنده‌ی وابستگی قابل توجه بین کاربران و روبات‌هایشان است (Tony Prescott 2021).

بر خلاف این نمونه‌ها که در آن کاربران غیر متخصص به شمار می‌آیند، به نظر می‌رسد سازندگان روبات‌ها هم از این مساله مستثنی نیستند. سینتیا بریزیل<sup>۱۳</sup> سازنده‌ی کیسمت<sup>۱۴</sup> که اولین روبات هوشمند اجتماعی

<sup>13</sup>Cynthia Breazeal

<sup>14</sup>Kismet

است نیز رابطه‌ای شخصی را با روبات خویش شکل داده بود؛ پیوندی مادرانه که روبات را فقط یک ماشین نمی‌دید و وقتی پروژه‌اش به پایان رسید و مجبور به ترک روبات شد، فقدان شدید را تجربه کرد. همچنین دانشجویان ام.آی.تی که در آزمایشگاه با روبات کیسنت کار می‌کردند، گاهی پرده‌ای را میان خود و روبات می‌کشیدند، چون خیره شدن روبات باعث برهم خوردن تمرکز آن‌ها می‌شد (Scheutz 2012).

## ۴ مخاطرات رابطه احساسی یک طرفه انسان با روبات

تجربه‌های یادشده از وابستگی‌های عاطفی یک طرفه انسان و روبات این مساله را روشن می‌نماید که صرف تقلید و شبیه‌سازی برخی از رفتارهای انسان یا حیوان واقعی، می‌تواند روبات را آماده‌ی ساختن رابطه‌ای عاطفی یک‌سویه از سمت کاربر نموده و از او یک همدم بسازد. فرافکنی ذهن‌مندی و عاملیت به روبات و تشخیص بخشی به روبات از سوی کاربر، می‌تواند منجر به نسبت‌دادن ویژگی‌های زیست‌شناختی انسانی به روبات و تجربه‌ی احساساتی نظیر دلسوزی، مسئولیت‌پذیری، شرم، عذاب وجدان، قدردانی، مراقبت و حفاظت از روبات‌ها شود. علاوه بر وجود این فرایند احساسی ناآگاهانه از سوی کاربران انسانی، شرکت‌های سازنده‌ی روبات‌های اجتماعی با وجود آگاهی از عدم توانایی روبات‌های خود در درک و بروز احساسات، در راستای مقاصد تبلیغاتی سعی می‌کنند این تصور را در کاربران خود به وجود بیاورند که روبات‌ها احساسات آن‌ها را درک می‌کنند و یا احساسات واقعی از خود بروز می‌دهند؛ در حالیکه به این امر آگاهند که روبات‌ها تنها نمایشی صوری از احساسات بروز می‌دهند و این به معنی فریب کاربر است. پژوهشگران دانشگاهی نیز در ارائه پژوهش‌های خود به قدر کافی مراقب نیستند و از تعبیری مانند «احساس داشتن» برای توصیف ساخته‌های خود استفاده می‌کنند و استفاده از این ادبیات در نوشتن مقالات و گزارش‌های علمی موجب می‌شود افراد غیر متخصص فرایندهای کنترل را در این مصنوعات با فرایندهای کنترل در ارگانیسم‌های طبیعی مثل حیوانات و انسان‌ها یکسان بیانگرند و در حالی که در سطح آگاهانه این ادعاها را ممکن است رد کنند، باورهای غلطی را در سطح عمیق ناخودآگاه نسبت به امکان برقراری رابطه عاطفی با روبات‌ها پیدا می‌کنند (Scheutz 2012).

رابطه عاطفی یک طرفه با تکنولوژی‌های هوشمند و یا تصور امکان برقراری رابطه عاطفی با تکنولوژی‌هایی که از چنین امکانی برخوردار نیستند می‌تواند عواقب جدی برای جوامع انسانی داشته باشد؛ چرا که امکان سوء استفاده‌های اقتصادی، سیاسی و امنیتی در مقیاس بزرگ را از سوی روبات‌ها و یا شرکت‌های سازنده‌ی آنها فراهم می‌کند. نمایش صوری احساسات از سوی روبات‌ها و رفتار سطحی آنها می‌تواند آسیب جسمی و روانی کاربر را به دنبال داشته باشد. همچنین اعتیاد ناآگاهانه به بات به دلیل همانندسازی رابطه انسانی با آنها می‌تواند اثرات مخربی بر تعاملات انسانی داشته باشد (Scheutz 2012). ایجاد رابطه تعاملی با روبات‌ها می‌تواند به توانایی و تمایل ما برای معاشرت با سایر انسان‌ها آسیب وارد نماید. تعامل با یک روبات اجتماعی (همدم) می‌تواند با تضعیف ظرفیت ما برای دلبستگی ایمن، تشویق رابطه با روبات به دلیل سهولت و ماهیت غیر چالش‌برانگیز همراهی مصنوعی در مقابل رابطه با یک انسان و با پرکردن زمان و ظرفیت کاربر، به روابط انسانی آسیب وارد نماید (Tony J. Prescott 2021). بنابراین می‌توان گفت علی‌رغم همه‌ی کاربردهایی مفیدی که روبات‌های اجتماعی می‌توانند برای کاربران داشته باشند، چالشی جدی ناشی از شکل‌گیری رابطه

احساسی یک طرفه با روبات وجود دارد. پیشنهادهای برای پیشگیری از اثرات مخرب این مساله مطرح شده است. این پیشنهادات می‌توانند موردی باشند و یا اینکه همه‌ی انواع روبات‌های اجتماعی را شامل شوند. بسته به نوع و کاربرد روبات می‌توان این پیشنهادات را بررسی کرد.

## ۵ چند پاسخ احتمالی به مخاطرات رابطه یک طرفه انسان با روبات

با توجه به فواید و کاربردهایی که تکنولوژی‌های هوشمند اجتماعی می‌توانند داشته باشند، مانند درمان‌های توانبخشی، تشویق به رفتارهای مثبت در راستای سلامت و بهزیستی، مراقبت از سالمندان و آموزش‌های شخصی و غیره، پیشنهادهایی مثل توقف تولید روبات‌های اجتماعی منطقی به نظر نمی‌رسد؛ اما مخاطرات رابطه یک طرفه‌ی انسان و روبات به قدری جدی و همه‌گیر است که نمی‌توان از آن نیز صرف نظر کرد.

یکی از پیشنهادهای ممکن برای پیشگیری از آسیب‌های رابطه احساسی یک طرفه‌ی روبات و انسان، مجهز کردن روبات به قدرت استدلال اخلاقی در قالب الگوریتم‌های تصمیم‌گیری است که مانع از امکان سوء استفاده از کاربر بشود؛ اما باید دانست که تعداد کنش‌های قابل پیش‌بینی در قالب الگوریتم‌های تصمیم‌گیری محدود است در حالی که دلالت‌های اخلاقی کنش‌ها و موقعیت‌های محتمل، بسیار پیچیده و پرشمارند و همه‌ی تلاش‌ها در طول تاریخ فلسفه نتوانسته است روی مجموعه‌ای کامل از قواعد اخلاقی توافق کند. علاوه بر این، ترجمه قواعد اخلاقی به زبان محاسباتی نیز ممکن است با محدودیت‌های عملی مواجه باشد. حتی اگر این مجموعه مشخص از قواعد اخلاقی (مثل قواعد آسیموف) قابل تبدیل شدن به کد باشند، به این خاطر که اولویت‌بندی قواعد و حل تناقض میان قواعد، وابسته به موقعیت است و موقعیت‌مندی مساله‌ای بسیار دشوار است، می‌توان گفت این سیستم در عمل کار نمی‌کند (Scheutz 2012).

علیرغم اهمیت شباهت ظاهری روبات با انسان در روبات‌های انسان‌نما، ممکن است در ابتدا تصور کنیم که صرف شباهت ظاهری ماشین به انسان است که موجب می‌شود خودمختار نبودن روبات را فراموش کنیم و به آن احساسات نسبت بدهیم؛ اما روباتی مثل رومبا که شباهتی به انسان یا حیوان ندارد نیز ایده‌ی عاملیت‌داشتن را به کاربرش القاء کرده و حتی می‌تواند حس قدردانی و دلسوزی را در او فعال کند. با این حال به عنوان راه حلی دیگر می‌توان این پیشنهاد را مطرح کرد که طراحی روبات به گونه‌ای باشد که دائماً به کاربر این اخطار را بدهد که یک ماشین است، احساسات ندارد و نمی‌تواند رابطه‌ای متقابل داشته باشد. هر چند ممکن است این اخطار، احتمال و شدت پیوندهای عاطفی با روبات را کاهش دهد اما همانند پیام‌های اخطار روی پاکت سیگار ضمانتی وجود ندارد که انسان‌ها درگیر رابطه با روبات نشوند (Scheutz 2012).

دیدگاه دیگر این است که برای حل چالش رابطه یک‌سویه‌ی انسان و روبات، روبات‌ها را به احساساتی مشابه انسان مجهز کنیم. بدین ترتیب روبات‌ها نیز می‌توانند با داشتن توانایی احساسی مشابه انسان، در جوامع انسانی شبیه انسان‌ها عمل کنند و در صورت برقراری رابطه بین انسان و روبات، رابطه‌ای دو سویه برقرار شود. عملی کردن این پیشنهاد در عین اینکه می‌تواند آورده‌هایی برای کاربر داشته باشد، چالش‌های جدیدی را پیش روی ما قرار می‌دهد.



## ۶ رابطه احساسی دوطرفه انسان و روبات

با هوشمندتر شدن هوش مصنوعی و تعاملات رو به گسترش انسان‌ها با تکنولوژی‌های هوشمند از جمله روبات‌های اجتماعی، این دیدگاه مطرح شد که از طریق القاء احساسات به روبات‌ها علاوه بر آن که می‌توان آن‌ها را برای کاربر ایمن‌تر، جذاب‌تر و کارا تر کرد، این امید وجود دارد که از این طریق بتوانیم روبات‌های هوشمند اجتماعی را اخلاقی نیز بکنیم (Lagrandeur 2015). در ادامه به بررسی اثرات مثبت و چالش‌های اخلاقی این دیدگاه می‌پردازیم.

تسهیل تعامل انسان و روبات یکی از مهمترین اثرات مثبت القاء احساسات در هوش مصنوعی و روبات‌هاست. روبات‌های اجتماعی برای به‌عهده‌گرفتن نقش‌های اجتماعی خود نیاز به توانایی درک اجتماعی دارند. درک اجتماعی نیازمند حساسیت، یا توانایی شناخت هیجانات و احساسات در دیگران و برقراری رابطه همدلانه با آنان است (Castellano, et al. 2012). به عبارتی روبات اجتماعی برای اجتماعی بودن، نیازمند توانایی تفسیر و پاسخ به احساسات انسان‌ها است؛ به عنوان مثال یک روبات حساس<sup>۱۵</sup>، به احتمال بیشتری با کاربر انسانی درگیر می‌شوند و مدت طولانی‌تری با او تعامل قابل قبول و مطلوب برقرار می‌کند؛ به این معنی که سعی می‌کند اطمینان حاصل کند که کاربر به حفظ تعامل علاقه‌مند است و در صورت ناراحت بودن یا عدم تمایل به تعامل از سوی کاربر، با او همدلانه رفتار می‌کند. چنین روباتی با تلاش برای درگیر کردن فرد در فعالیت‌ها، مزاحمتی برای کاربر ایجاد نمی‌کند. به عبارتی درک اجتماعی و توانایی شناخت هیجانات کاربر از سوی روبات، احتمال مزاحمت کمتر برای کاربر و تعامل باورپذیر و بلندمدت‌تر و در نهایت جذابیت روبات برای کاربر را در پی دارد. برخورداری روبات از احساسات قابل درک برای انسان، آگاهی از نحوه تأثیرپذیری هوش مصنوعی از محیط را برای انسان در پی دارد. این مساله باعث پیش‌بینی رفتارهای روبات و دستیابی به نحوه‌ای از مکانیسم کنترل می‌شود که در نهایت امنیت را برای کاربران به ارمغان می‌آورد.

## ۷ جای‌دهی احساسات در هوش مصنوعی و چالش‌های آن

بیشتر ایده‌های موجود درباره‌ی ایجاد احساسات در هوش مصنوعی، دور از دسترس و مربوط به آینده‌ی خیلی دور است که ممکن است هیچگاه محقق نشود. به نظر می‌رسد تلاش برای رسیدن روبات به احساسات کاملاً شبیه انسان و تحقق هوش مصنوعی قوی دارای احساسات از نظر فنی و از نظر فلسفی ممکن نباشد؛ اما در صورت امکان با چالش‌های فلسفی و اخلاقی زیادی روبروست.

مساله اول این است که مبنای اخلاق صحیح چیست؟ وقتی حرف از ارزش‌ها یا مقولاتی مثل خیرخواهی یا وجدان می‌زنیم کدام مکتب اخلاقی مد نظر است؟ اخلاق کانتی؟ وظیفه‌گرایی (قاعده صرف)؟ سودگرایی (نفع بزرگ جمع)؟ بودیسم (ایثار و شفقت)؟ (Lagrandeur 2015) مساله بعد به این موضوع می‌پردازد که این مسیر آزمایش‌ها و توسعه‌ی ایجاد روبات‌های هوشمند اجتماعی درست نیست؛ به این دلیل که تا قبل از مجهز کردن روبات‌ها به احساسات، دلبستگی عاطفی یک‌طرفه بین انسان و روبات وجود دارد و این مساله

<sup>15</sup>Affect-sensitive robot

می‌تواند انسان را در مقابل برخی مخاطرات آسیب پذیر کند (Lagrandeur 2015). برای تولید احساسات مصنوعی مبتنی بر احساس گناه و همدلی، باید موجودی تولید کرد که رنج دیده بوده و قادر به رنج کشیدن باشد تا بتواند رنج دیگران را درک کند. مساله سوم به سوال می‌پردازد که آیا تولید موجودی رنجور اخلاقی است؟ آیا ما حق داریم که موجودی را خلق کنیم که آسیب پذیر است و ممکن است مورد سوء استفاده قرار گیرد؟ در هر صورت، این پیشنهاد را نمی‌توان و لازم نیست در هر نوعی از روبات اجتماعی عملی کرد، بلکه بر حسب نیاز و کاربرد می‌توان از این قابلیت استفاده کرد (Scheutz 2012). مساله دیگر به این سوال توجه دارد که آیا این گونه اقدامات منجر به تقلیل احساسات انسانی به یکسری الگوهای تقلیدی و رفتارهای سطحی خشک نیست؟ آیا صرف تقلید رفتار از جایگاه و ارزش احساسات پیچیده‌ی انسانی مخصوصاً نوع غیر کلامی‌اش نمی‌کاهد؟ و مساله آخر این است که آیا این شبیه‌سازی منحصر به فرد بودن ارتباطات انسانی را تهدید می‌کند؟ در جواب باید گفت، بله ممکن است (Lagrandeur 2015). علاوه بر ایده‌ی دستیابی به هوش مصنوعی قوی مبتنی بر احساسات، راهکارها و ایده‌های کوتاه مدت برای نزدیک تر شدن هوش مصنوعی به احساسات انسانی نیز وجود دارد که هر کدام مزیت‌ها و کاربردهایی دارند ولی نقدهای اخلاقی جدی به هر یک از آنها نیز وارد است.

یک راهکار کوتاه مدت، نرم افزاری است برای طراحی یک «وجدان اخلاقی»<sup>۱۶</sup> که بتواند مثل یک فرمانده اخلاقی برای سیستم‌های هوشمند خودمختار عمل کند (Arkin 2007). این تجهیز اخلاقی بیشتر روی «احساس گناه» متمرکز است و سعی می‌کند با کدنویسی به نحوی گناه روباتیک را ایجاد کند؛ به این معنی که این کدنویسی منجر می‌شود که خود روبات با خودپایشی برخی پارامترهای قابل اندازه گیری، به حس گناه برسد. در این ایده، اگر اندازه‌ی فعلی حالت عاطفی گناه از یک مقدار از پیش تعیین شده‌ی حد آستانه بیشتر شود، نشانه‌ی شکسته شدن اخلاق است و روبات به نحو اتوماتیک غیر فعال می‌شود. سه نقد به این راهکار وارد است؛ اول اینکه بدون تجربه قبلی، تشخیص حد آستانه برای روبات ممکن نیست. به نظر می‌رسد طراحی چنین عملکرد عاطفی‌ای تنها بعد از وقوع یک فاجعه انسانی میسر می‌شود. دوم اینکه این احساسات روباتی تنها یک شبیه‌سازی مبهم از نوع انسانی‌اش هستند، زیرا مبتنی بر خود و پویا نبوده و در حد یک سیستم عیب‌یابی کامپیوتری عمل می‌کنند که در حال حاضر هم وجود دارد. سوم اینکه این احساساتی که قرار است در طراحی روبات‌ها مورد استفاده قرار گیرند، یک محاسبات بی‌روح و سرد از یک سری معیار ارزیابی هستند و شامل همدلی، همدردی و حتی ترحم نمی‌شوند. بنابراین نمی‌توان نام چنین کاری را محاسبات عاطفی یا احساسات بنیانی گذاشت؛ به این دلیل که نه کدگذاری آنها به اندازه‌ی کافی پیچیده است و نه هوش مصنوعی هنوز به اندازه کافی پیشرفته است (Lagrandeur 2015).

راهکار کوتاه مدت دیگر این است که ماشین را واجد نوعی «خیرخواهی»<sup>۱۷</sup> کنیم؛ به این صورت که از رابطه مادر و کودک الهام بگیریم و هنگامی که روبات برای اولین بار کاربر انسانی خود را دید، با او پیوند اجتماعی خودکار برقرار کند و این روند هر بار که انسان با روبات چیزی را به اشتراک می‌گذارد، تقویت شود؛ اما در نقد این ایده می‌توان گفت در واقع «خیرخواهی» فقط یک رفتار نیست. ممکن است ظهور و بروز

<sup>16</sup>ethical conscience<sup>17</sup>benevolence

خیرخواهی در رفتار نمایان شود ولی خود خیرخواهی در واقع یک موضع اخلاقی پیچیده است؛ یک تصمیم آگاهانه بر اساس مجموعه‌ای از احساسات و تجربیات و دلایل است که منجر به انجام عمل به نفع دیگری می‌گردد. بنابراین چیزی بیشتر از یک سیستم پاداش‌دهی ساده است (Lagrandeur 2015). تلاش برای احساسی کردن روبات‌ها اگرچه راهکار مناسبی به نظر می‌رسد ولی در عمل با چالش‌های فلسفی و اخلاقی و عملی زیادی روبروست. با این حال تلاش در جهت جای‌دهی احساسات در روبات پروژه‌ای در جریان است که می‌تواند در آینده ایده‌ها و نمونه‌های جدیدی را به ظهور برساند.

## ۸ نتیجه‌گیری

در مقاله حاضر کوشیدیم تا تحلیلی از رابطه احساسی یک‌طرفه میان انسان و روبات‌های اجتماعی ارائه دهیم و به مثال‌هایی اشاره کنیم که شکل‌گیری چنین روابط احساسی‌ای را تصدیق می‌کنند. این رابطه احساسی یک‌سویه می‌تواند مخاطراتی را برای کاربران انسانی ایجاد کرده و امکان سوء استفاده سیاسی، اقتصادی و امنیتی از آن‌ها را فراهم کند. در حالی که خود روبات‌ها در حال حاضر توانایی درک احساسات و همدلی با کاربر را ندارند و صرفاً توهم داشتن ویژگی‌های شبه انسانی را در کاربر ایجاد می‌کنند. در همین رابطه، تا حدی به این موضوع پرداختیم که راه‌حل‌های ممکن برای پیشگیری یا کمینه کردن چنین مخاطراتی در تعامل انسان/روبات چه می‌تواند باشد. برای مثال، اخلاقی کردن تصمیم‌های روبات‌ها و به نوعی، جای‌دهی کردن اخلاقیات در طراحی روبات‌ها تا چه میزان امکان‌پذیر است و آیا می‌تواند مانع سوء استفاده‌های غیر اخلاقی از کاربر شود. چه راهکارهایی را می‌توان تدبیر کرد تا کاربر کمتر دچار انسان‌پنداری و نسبت‌دادن ویژگی‌های انسانی به روبات شده و فاصله احساسی خود از آن را کنترل کند.

بررسی کردیم که آیا راه مقابله با مخاطرات این رابطه یک‌سویه این است که در روبات‌ها احساسات و توانایی شناخت هیجانات و همدلی را شبیه‌سازی کنیم یا خیر. اما این راهکار خود با چالش‌هایی فلسفی و اخلاقی روبروست از جمله اینکه آیا ماهیت احساسات یا فضایی نظیر خیرخواهی به گونه‌ای است که شبیه‌سازی آن امکان‌پذیر باشد؟ آیا ساختن موجودی که توانایی رنج کشیدن و آسیب دیدن را داشته باشد، امری اخلاقی است؟ آیا ساختن چنین موجوداتی منجر به تهدید روابط انسانی نخواهد شد؟ پرسش‌هایی از این دست، همچنان پرسش‌های بازی هستند که نیازمند تأملات بین‌رشته‌ای میان علوم انسانی و علوم فنی است و هر علمی از زاویه نگاه خود می‌تواند تحلیلی از مسئله ارائه دهد؛ لیکن فارغ از اینکه در عمل طراحی روبات‌های دارای توانایی‌های احساسی ممکن باشد یا خیر، نیازمند تأملات اخلاقی عمیق و آینده‌نگرانه‌ای هستیم که عواقب اخلاقی تلاش در جهت توسعه این روبات‌ها را بر ما نمایان‌تر کند و ما را برای روبرویی با آینده‌های ممکن مختلف آماده کند.

## مراجع

- [1] Arkin, R. 2007. "Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture." Technical report, Georgia Institute of Technology.

- [2] Bechara, Antoine , Hanna Damasio, & Antonio R. Damasio. March 2000. "Emotion, Decision Making and the Orbitofrontal Cortex." *Cerebral Cortex*, Volume 10, Issue 3, 295–307.
- [3] Castellano, Ginevra, Iolanda Leite, Ana Paiva, & Peter W. McOwan. 2012. "Affective teaching: learning more effectively from empathic robot." *Awareness magazine: Self-Awareness in Autonomic Systems* doi: 10.2417/3201112.003948.
- [4] Cominelli, Lorenzo , Daniele Mazzei, & Danilo Emilio De Rossi. 2018. "SEAI: Social Emotional Artificial Intelligence Based on Damasio's Theory of Mind." *Front. Robot. AI*.
- [5] Friedenberg, Jay, & Gordon Silverman. 2005. *Cognitive Science: An Introduction to the Study of Mind*. California, USA: SAGE Publications.
- [6] Kahn, P. H. 1999. *The human relationship with nature: Development and culture*. MIT Press.
- [7] Lagrandeur, Kevin. 2015. "Emotion Artificial Intelligence and Ethics."
- [8] Matsumoto, David, & Hyisung Hwang. 2019. "Functions of Emotions." In: *Introduction to Psychology*, By: Jorden Cummings & Lee Sanders. University of Saskatchewan.
- [9] Peter H. Kahn, J., Friedman, B., & Hagman, J. 2002. "I care about him as a pal: Conceptions of robotic pets in online aibo discussion forums." *CHI EA '02: CHI '02 Extended Abstracts on Human Factors in Computing Systems*, 632–633.
- [10] Scheutz, Matthias. 2012. "The Inherent Dangers of Unidirectional Emotional Bonds between Humans and Social Robots." *Robot Ethics: The Ethical and Social Implications of Robotics* (MIT Press), 205-221.
- [11] Shouse, Eric. 2005. "Feeling, Emotion, Affect." *M/C Journal* 8.6.
- [12] Sung, JY., Guo, L., Grinter, R.E., & Christensen, H.I. 2007. "My Roomba Is Rambo": Intimate Home Appliances". *UbiComp 2007: Ubiquitous Computing*. Berlin: Springer, 145-162.
- [13] Tony J. Prescott, & Julie M. Robillard. 2021. "Are friends electric? The benefits and risks of human-robot relationships." *iScience* Volume 24, Issue 1.

## رویکردهای هوشمند در شناسایی وبگاه‌های دام‌چینی

یگانه ستاری<sup>۱</sup>، غلامعلی منتظر<sup>۲</sup>

<sup>۱</sup> دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران  
y.sattari@modares.ac.ir

<sup>۲</sup> استاد مهندسی فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران  
montazer@modares.ac.ir

### چکیده

«دام‌چینی» نوعی حمله سایبری است که اغلب از طریق ایجاد وبگاهی جعلی با طراحی کاملاً مشابه وبگاهی قانونی و با هدف فریب کاربران اینترنتی به افشای اطلاعات شخصی خود مانند رمز عبور و مشخصات کارت‌های اعتباری صورت می‌گیرد. دام‌چینی، امنیت شبکه را نه تنها برای کاربران بلکه برای سازمان‌ها به خطر انداخته و امروزه با گسترش اینترنت و فناوری‌های ارتباطی، به یکی از جدی‌ترین تهدیدهای امنیتی در فضای سایبری تبدیل شده است. تاکنون محققان روش‌های گوناگونی را برای شناسایی دام‌چینی ارائه کرده‌اند، با این حال چنین حمله‌هایی هنوز وجود دارند. در سال‌های اخیر روش‌های هوشمند با سازگاری بالا در مواجهه با حمله‌های جدید، مورد توجه محققان زیادی قرار گرفته است. بنابراین در این مقاله، به منظور بررسی شکاف‌های غالب و جهت‌گیری تحقیقات آینده، به تحلیل و بررسی رویکردهای هوشمند یادگیری ماشینی در شناسایی وبگاه‌های دام‌چینی پرداخته شده است. از جمله چالش‌های موجود، می‌توان به نحوه استخراج و انتخاب ویژگی و همچنین زمان پاسخگویی اشاره کرد.

**کلمات کلیدی:** امنیت سایبری، امنیت شبکه، دام‌چینی، هوشمند، یادگیری ماشینی.

## ۱ مقدمه

«دام‌چینی»<sup>۱</sup> در لغت به معنای «طعمه‌گذاری مهاجمان برای به دام انداختن کاربران» است و به نوعی حمله سایبری اشاره دارد که در آن مهاجمان با بهره‌گیری از مهندسی اجتماعی<sup>۲</sup> و ترفندهای فنی<sup>۳</sup>، کاربران اینترنتی را به افشای اطلاعات محرمانه و شخصی خود (مانند نام کاربری، رمز عبور و مشخصات کارت‌های اعتباری) ترغیب می‌کنند [۱، ۲]. دام‌چینی نزدیک به سه دهه اخیر تهدیدی امنیتی در فضای سایبری بوده و امروزه با گسترش فناوری و ارتباطات صدها میلیون کاربر در سطوح شخصی یا تجاری تعداد این نوع حمله‌ها افزایش

<sup>۱</sup> phishing

<sup>۲</sup> social engineering

<sup>۳</sup> technical tricks

یافته‌اند؛ به طوری که بیش از نیمی از جرایم سایبری را در بر می‌گیرد [۳، ۴، ۵]. در اغلب این حمله‌ها، مهاجمان با نام سازمان‌های معتبر ظاهر می‌شوند و با طراحی وبگاهی جعلی کاملاً مشابه وبگاهی قانونی و معتبر، از طریق کانال‌های ارتباطی مختلفی (مانند رایانامه<sup>۴</sup>) کاربران را به بازدید از این وبگاه ترغیب می‌کنند [۶]. در سال ۲۰۲۱ حدود سه میلیون وبگاه دام‌چینی منحصر به فرد در سراسر جهان کشف شده که نسبت به سال ۲۰۲۰ دو برابر افزایش داشته است. علاوه بر این در سه ماه اول سال ۲۰۲۲ تعداد این وبگاه‌ها به بیش از یک میلیون رسیده است [۷]. اکثر کاربران درک درستی از تهدید دام‌چینی ندارند و نمی‌دانند چنین حمله‌هایی چگونه اجرا می‌شوند [۸]. بنابراین نیاز به ساز و کاری مؤثر برای محافظت از کاربران در برابر حمله‌های دام‌چینی است. روش‌های شناسایی وبگاه‌های دام‌چینی را می‌توان به دو دسته اصلی تقسیم‌بندی کرد [۴]: دسته اول راه حل‌های ترویجی - آموزشی با هدف افزایش سطح آگاهی کاربران نهایی و دسته دوم راه‌حل‌های فنی با هدف تشخیص خودکار وبگاه‌های دام‌چینی از طریق توسعه روش‌های مبتنی بر نرم‌افزار.

در این مقاله، با تمرکز بر راه‌حل‌های مبتنی بر نرم‌افزار، به دنبال بررسی روش‌های جدید و چالش‌های آنها هستیم. در سال‌های اخیر با توسعه روش‌های یادگیری ماشینی، محققان زیادی به ارائه رویکردهای هوشمند برای شناسایی وبگاه‌های دام‌چینی روی آوردند. بنابراین به تحلیل و مقایسه برخی از آنها بر اساس نوع الگوریتم یادگیری ماشینی مورد استفاده در سه دسته شامل الگوریتم‌های معمولی<sup>۵</sup>، یادگیری ژرف<sup>۶</sup> و منطق فازی<sup>۷</sup> می‌پردازیم. در ادامه ساختار مقاله بدین شرح است: در بخش ۲ مروری مختصر بر روش‌های دام‌چینی و در بخش ۳ بررسی انواع روش‌های شناسایی وبگاه‌های دام‌چینی و تحلیل رویکردهای هوشمند یادگیری ماشینی ارائه شده است. در نهایت در بخش ۴ نتیجه‌گیری شده است.

## ۲ روش‌های دام‌چینی

مهاجمان پس از طراحی و ایجاد یک وبگاه جعلی کاملاً مشابه وبگاهی قانونی، به روش‌های مستقیم و یا غیر مستقیم کاربر/کاربران مورد هدف را به سمت وبگاه هدایت می‌کنند. در روش‌های مستقیم، مهاجم از طریق کانال‌های ارتباطی مختلفی مانند رایانامه و شبکه‌های اجتماعی با کاربر ارتباط برقرار کرده و با بهره‌گیری از مهندسی اجتماعی، سعی دارد خواننده را متقاعد کند تا هرچه سریع‌تر از پیوندی که برای او ارسال کرده بازدید و اطلاعات خود را به روزرسانی یا تأیید کند. اغلب حمله‌های دام‌چینی با ارسال انبوه رایانامه آغاز می‌شوند [۹]. طبق گزارشی که وبگاه آوانان<sup>۸</sup> در سال ۲۰۲۱ در مورد حمله‌های سایبری منتشر کرد، ۵ درصد از تمام رایانامه‌ها، رایانامه‌های دام‌چینی هستند [۱۰]. علاوه بر این مهاجمان رویکردهای فنی مختلفی را برای هدایت غیر مستقیم کاربران به سمت وبگاه به کار می‌گیرند؛ برای مثال ترندهایی برای افزایش رتبه پیوند

<sup>4</sup>email

<sup>5</sup>conventional

<sup>6</sup>deep learning

<sup>7</sup>fuzzy logic

<sup>8</sup>Avanan



در نتایج موتور جستجو اعمال می کنند زیرا کاربرانی که برای یافتن وبگاه ارائه دهنده خدمات یا محصول مورد نظر از موتورهای جستجو استفاده می کنند، ممکن است با بی دقتی روی پیوند دام چینی در نتایج جستجو کلیک کنند [۱۱]. علاوه بر این گاهی مهاجمان یو آر آل<sup>۹</sup> وبگاه معتبر را به گونه ای جعل می کنند تا اگر کاربر خطای نوشتاری مرتکب شود و یا اسم وبگاهی را که شنیده اشتباه وارد کند، به وبگاه دام چینی هدایت شود [۱۱، ۱۲].

### ۳ روش های شناسایی دام چینی

در سال های اخیر مقاله های مختلفی در حوزه دام چینی و بررسی روش های شناسایی آن ها توسط محققان منتشر شده است [۲، ۱۳، ۱۴، ۱۵]. به عنوان نمونه، بسیت و همکاران، مروری بر حمله های دام چینی و روش های هوشمند در شناسایی آنها ارائه کردند. آنها انواع حمله های دام چینی و همچنین راه حل های متقابل را در چهار دسته «یادگیری ماشینی»، «یادگیری ژرف»، «مبتنی بر سناریو» و «ترکیبی» به همراه رویکردهای محققان بررسی کرده و در نهایت چالش های موجود را ارائه کردند [۱۳]. با این حال همواره نیاز به مطالعاتی است که رویکردهای ارائه شده در شناسایی دام چینی را به منظور بهبود آنها و ارائه چالش های موجود بررسی کنند. در ادامه، روش های شناسایی وبگاه های دام چینی را در دو دسته روش های «مبتنی بر بر مقایسه<sup>۱۰</sup>» و روش های «هوشمند» بررسی می کنیم.

#### ۱.۳ روش های مبتنی بر مقایسه

به طور کلی در روش های مبتنی بر مقایسه، اجزای اصلی وبگاه مشکوک (مورد بررسی) با وبگاه های معتبر مقایسه و سپس نوع آن تعیین می شود. این روش ها را می توان به سه دسته تقسیم کرد: رویکردهای «مبتنی بر فهرست<sup>۱۱</sup>»، «اکتشافی<sup>۱۲</sup>»، «مبتنی بر شباهت بصری<sup>۱۳</sup>»

**الف. مبتنی بر فهرست:** این رویکردها با مقایسه وبگاه ها با موارد موجود در فهرست های سیاه/سفید که حاوی اطلاعات وبگاه های جعلی/قانونی از پیش شناسایی شده مانند یو آر آل، نشانی آی پی، نام دامنه و غیره هستند، به تعیین وضعیت وبگاه ها می پردازند [۱۵]. این رویکردها سرعت عمل بالایی دارند و معمولاً به سادگی طراحی و پیاده سازی می شوند. با این حال اکثر این نوع رویکردها وبگاه های ساعت-صفر<sup>۱۴</sup> (موارد جدید یا از پیش دیده نشده) را شناسایی نمی کنند و همچنین فهرست ها باید به طور مکرر به روز شوند که این امر نیاز به تأیید و مداخله انسانی دارد [۱۶، ۱۷].

<sup>9</sup>URL

<sup>10</sup>comparison-based

<sup>11</sup>list-based

<sup>12</sup>heuristics

<sup>13</sup>visual-based

<sup>14</sup>zero-hour

**ب. اکتشافی:** در رویکردهای اکتشافی ویژگی‌های مختلفی مبتنی بر نشانی و یا محتوا از وبگاه استخراج شده و در صورتی که با وبگاه‌های معتبر و قانونی مطابقت بالایی داشته باشند، به عنوان دام‌چینی شناسایی می‌شوند. این رویکردها می‌توانند حمله‌های ساعت - صفر را شناسایی کنند. با این حال اکثر آنها «میزان مثبت نادرست»<sup>۱۵</sup> بالایی دارند که ممکن است منجر به از دست رفتن اعتماد کاربران به سیستم شود [۱۶].

**ج. مبتنی بر شباهت بصری:** این رویکردها وبگاه‌های دام‌چینی را از میزان شباهت ظاهری با وبگاه‌های قانونی شناسایی کرده و قادر به شناسایی حمله‌های جدید هستند. با این حال برای نگهداری تصاویر وبگاه‌ها و پردازش آنها به فضای ذخیره‌سازی بزرگ و زمان قابل توجهی نیاز دارند [۱۶].

## ۲.۳ روش‌های هوشمند

شناسایی وبگاه‌های دام‌چینی را می‌توان به عنوان یک مسئله دسته‌بندی<sup>۱۶</sup> در نظر گرفت که شامل دو دسته «دام‌چینی (فریب)» و «قانونی» است. در روش‌های هوشمند با اعمال الگوریتم‌های یادگیری ماشینی از طریق استدلال الگوها و ویژگی‌های وبگاه‌های برچسب‌گذاری شده (که پیشتر به عنوان دام‌چینی یا قانونی شناسایی شده‌اند)، مدل‌هایی ساخته می‌شود که وبگاه‌های جدید و فاقد برچسب را دسته‌بندی می‌کنند. روش‌های هوشمند توانمندی بیشتری در شناسایی انواع جدید حمله‌ها دارند [۱۸]. از مهم‌ترین معیارهای ارزیابی در این رویکردها می‌توان به صحت<sup>۱۷</sup> (مجموع نمونه‌های دام‌چینی و قانونی که درست شناسایی شدند، نسبت به تمام نمونه‌های موجود) و زمان پاسخگویی<sup>۱۸</sup> (زمان بین ورود یوآرال به سامانه تا مشخص شدن نوع وبگاه) اشاره کرد. تاکنون محققان رویکردهای مختلفی را برای شناسایی وبگاه‌های دام‌چینی ارائه کرده‌اند که در ادامه برخی از آنها را به تفکیک نوع الگوریتم یادگیری ماشینی مورد استفاده، در سه دسته بررسی می‌کنیم: الگوریتم‌های معمولی، یادگیری ژرف و منطق فازی.

**الف. الگوریتم‌های معمولی:** در ایجاد مدل‌های مبتنی بر الگوریتم‌های معمولی یادگیری ماشینی، فرایند استخراج و انتخاب ویژگی نیازمند مهارت انسانی است و مجزا از عمل دسته‌بندی انجام می‌شود؛ به طوری که نمی‌توان آنها را برای بهبود عملکرد مدل در یک فاز ترکیب کرد [۱۷]. برخی از الگوریتم‌های معمولی پرکاربرد در شناسایی وبگاه‌های دام‌چینی عبارتند از [۲، ۱۴، ۱۷]: بیز ساده<sup>۱۹</sup>، نزدیک‌ترین k همسایه<sup>۲۰</sup>، ماشین بردار پشتیبان<sup>۲۱</sup> و جنگل تصادفی<sup>۲۲</sup>. به عنوان نمونه، گوپتا و همکاران ۹ ویژگی لغوی را مبتنی بر یوآرال، استخراج و عملکرد چهار دسته‌بند را روی مجموعه داده‌ای شامل ۱۱.۹۶۴

<sup>15</sup>False Positive Rate (FPR)

<sup>16</sup>classification

<sup>17</sup>accuracy

<sup>18</sup>response time

<sup>19</sup>Naïve Bayes

<sup>20</sup>K-Nearest Neighbor (KNN)

<sup>21</sup>Support Vector Machine (SVM)

<sup>22</sup>random forest

یوآرال دام‌چینی و قانونی، ارزیابی کردند که در نهایت صحت این مدل با الگوریتم جنگل تصادفی ۵۷/۹۹ درصد و زمان پاسخگویی ۵۱ میلی‌ثانیه برآورد شده است [۶].

**ب. یادگیری ژرف:** یادگیری ژرف نشان‌دهنده نوعی از یادگیری ماشینی است که در آن از شبکه‌های عصبی ژرف برای آموزش و شناسایی وبگاه‌ها استفاده می‌شود. از جمله ویژگی‌هایی که این روش را از الگوریتم‌های معمولی مجزا می‌کند، توانایی یادگیری و انطباق با داده، استخراج خودکار ویژگی‌ها از داده‌های خام (مانند یوآرال) و کشف همبستگی پنهان بین آنها است. با این حال این روش‌ها نسبت به الگوریتم‌های معمولی تفسیرپذیری کمتری دارند و اغلب توضیح منطق پشت مفروضات، تصمیم‌گیری‌ها و نتیجه‌گیری‌هایی که یک شبکه عصبی انجام می‌دهد، ممکن نیست. علاوه بر این نسبت به الگوریتم‌های معمولی برای آموزش مدل به زمان و همچنین نمونه‌های آموزشی بیشتری نیاز دارند که جمع‌آوری آنها ممکن است بسیار پرهزینه و زمان‌بر باشد [۱۷]. الگوریتم‌های مختلفی در یادگیری ژرف وجود دارد که از پرکاربردترین آنها در شناسایی دام‌چینی می‌توان به شبکه عصبی پیچشی<sup>۲۳</sup>، شبکه عصبی بازگشتی<sup>۲۴</sup>، واحد بازگشتی دروازه‌ای<sup>۲۵</sup> و حافظه کوتاه-مدت طولانی<sup>۲۶</sup> اشاره کرد. به عنوان نمونه، در تحقیقی مدل مبتنی بر حافظه کوتاه-مدت طولانی برای شناسایی یوآرال‌های دام‌چینی پیشنهاد شده است که ابتدا رشته یوآرال را با استفاده از روش وان-هات<sup>۲۷</sup> رمزگذاری و سپس هر بردار رمزگذاری شده را برای آموزش و آزمایش در نرون‌های شبکه وارد می‌کند. این مدل بر روی مجموعه داده‌ای شامل یک میلیون یوآرال دام‌چینی و یک میلیون یوآرال قانونی ارزیابی شده که میزان صحت ۷/۹۸ درصد و زمان پاسخگویی ۲۸۱ ثانیه به ازای هر یوآرال برآورد شده است [۱۹].

**ج. منطق فازی:** منطق فازی، مدل‌سازی دقیق شیوه‌های استدلال تقریبی است که استدلال و تصمیم‌گیری را در محیطی غیر قطعی و غیر دقیق با اطلاعات ناقص (مانند گفتگوی انسان‌ها با زبان طبیعی) ممکن می‌سازد [۲۰]. سامانه‌های مبتنی بر منطق فازی قدرت یادگیری ندارند و شامل قواعد «اگر-آنگاه» هستند که توسط خبرگان هر حوزه استخراج می‌شود که عینی نیستند [۲۱].

به‌عنوان نمونه، رویکردی مبتنی بر منطق فازی پیشنهاد شده است که ابتدا ۶ ویژگی عددی را از مجموعه داده استخراج و سپس آنها را به مقادیر زبانی که میزان تأثیر هر ویژگی را با واژه‌های «زیاد»، «متوسط» و «کم» نشان می‌دهد، تبدیل می‌کند. در نهایت با اعمال مجموعه قواعد اگر-آنگاه که توسط الگوریتم تکامل تفاضلی<sup>۲۸</sup> بهینه شده‌اند، وبگاه‌ها دسته‌بندی می‌شوند. صحت روی مجموعه داده‌ای شامل ۲۰۰۰۰ وبگاه، ۶/۹۷ درصد برآورد شده است [۲۲].

<sup>23</sup> Convolutional Neural Networks (CNN)

<sup>24</sup> Recurrent Neural Networks (RNN)

<sup>25</sup> Gated Recurrent Unit (GRU)

<sup>26</sup> Long short-term memory (LSTM)

<sup>27</sup> one-hot

<sup>28</sup> Differential Evaluation (DE)

جدول ۱: مقایسه رویکردهای هوشمند یادگیری ماشینی در شناسایی وبگاههای دام چینی

مدل یا الگوریتم	نوع	مجموعه داده	مزیت‌ها	محدودیت‌ها	صحت (%)
جنگل تصادفی [6]	معمولی	۱۹.۹۶۴ نمونه: ۹.۹۶۴ یوآرال دام چینی و ۱۰.۰۰۰ یوآرال قانونی با ۹ ویژگی متنی مبتنی بر یوآرال	- صحت بالا - زمان پاسخگویی کوتاه (۵۱ میلی ثانیه) - استخراج ویژگی مستقل از خدمات شخص ثالث	- عدم اعتبارسنجی و ارزیابی استحکام مدل با مجموعه داده‌های مختلف - محدود بودن ویژگی‌ها	۹۹/۵۷
جنگل تصادفی [23]	معمولی	۴.۰۵۹ وبگاه: ۲.۱۴۱ نشانی دام چینی و ۱.۹۱۸ نشانی قانونی و ۱۹ ویژگی مبتنی بر نشانی و محتوای صفحه	-مقایسه پنج الگوریتم مختلف -زمان پاسخگویی قابل قبول (۵.۸۰۰ میلی ثانیه)	-مجموعه داده کوچک - برخی از ویژگی‌ها مبتنی بر مقایسه با وبگاه‌های معتبر	۹۹/۰۹
جنگل تصادفی [4]	معمولی	۷۳.۵۷۵ نمونه: ۳۷.۱۷۵ یوآرال دام چینی و ۳۶.۴۰۰ یوآرال قانونی با ۴۰ ویژگی	- استخراج ۲۷ ویژگی به روش پردازش زبان طبیعی - مستقل از زبان وبگاه	- استخراج یک ویژگی مبتنی بر رتبه صفحه از پایگاه آلیکسا (از دسترس خارج شده)	۹۷/۹۸
ماشین بردار پشتیبان [24]	معمولی	۲.۰۰۰ نمونه: ۱.۰۰۰ یوآرال دام چینی و ۱.۰۰۰ یوآرال قانونی با ۶ ویژگی	- استخراج ویژگی مبتنی بر یوآرال	- مجموعه داده کوچک - نیاز به یوآرال وبگاه - قانونی در استخراج یک ویژگی - محدود بودن ویژگی‌ها	۹۵/۸۰
ماشین بردار پشتیبان [25]	معمولی	۲.۱۳۴ نمونه: ۱.۴۴۸ یوآرال دام چینی و ۶۸۶ یوآرال قانونی با ۱۷ ویژگی	- صحت بالا - زمان پاسخگویی قابل قبول (حداکثر ۶.۳۰۰ میلی ثانیه)	- مجموعه داده کوچک - برخی از ویژگی‌ها مبتنی بر کد صفحه (HTML)	۹۸/۶۵
حافظه کوتاه-مدت طولانی [19]	یادگیری ژرف	۲ میلیون نمونه: ۱ میلیون یوآرال دام چینی و ۱ میلیون یوآرال قانونی	- مجموعه داده بزرگ - صحت بالا - بدون فرایند استخراج ویژگی و فقط با دریافت یوآرال - مستقل از خدمات شخص ثالث	- زمان پاسخگویی زیاد (۲۸۱ ثانیه) - زمان آموزش زیاد (۲۳۸ دقیقه)	۹۸/۷
حافظه کوتاه-مدت طولانی + شبکه عصبی پیچشی [26]	یادگیری ژرف	۱ میلیون نمونه: ۱ میلیون یوآرال دام چینی و ۱۰.۰۰۰ تصویر با ۳۵ ویژگی	- مجموعه داده بزرگ - ترکیب دو شبکه عصبی - ویژگی‌های ترکیبی مبتنی بر متن، قالب و تصویر وبگاه	- صحت پایین و زمان پاسخگویی زیاد (۲۵ ثانیه) - برخی از ویژگی‌ها وابسته به خدمات شخص ثالث و یا مبتنی بر کد صفحه (جاوااسکریپت)	۹۳/۲۸

۹۵/۷۹	- صحت پایین - زمان پاسخگویی زیاد (۴۰ ثانیه) - حداکثر طول یوآرال ۲۵۵ کاراکتر	- مجموعه داده بزرگ - ارزیابی استحکام مدل - بدون فرایند استخراج ویژگی و فقط با دریافت یوآرال - ترکیب دو شبکه عصبی	۴۹۰.۴۰۸ نمونه: ۲۴۵.۳۸۵ یوآرال دام چینی و ۲۴۵.۰۲۳ یوآرال قانونی	یادگیری ژرف	شبکه عصبی بازگشتی + شبکه عصبی پیشی [15]
۹۵/۰۲	- حداکثر طول نشانی وبگاه ۲۰۰ کاراکتر - زمان آموزش طولانی (۸۹ دقیقه)	- استفاده از چهار مجموعه داده مختلف برای ارزیابی - استخراج و مقایسه چهار گروه مختلف از ویژگی‌ها	۳۱۸.۶۴۲ نمونه: ۱۵۷.۶۲۶ یوآرال دام چینی و ۱۶۱.۰۱۶ یوآرال قانونی با ویژگی‌های سطح کاراکتر مبتنی بر یوآرال	یادگیری ژرف	شبکه عصبی پیشی [27]
۹۹/۱۸	- ذخیره یوآرال تا ۲۰۰ کاراکتر - عدم پشتیبانی از یوآرال‌های کوتاه	- میزان صحت بالا - استخراج ویژگی با پردازش زبان طبیعی - پیاده‌سازی به عنوان یک افزونه مرورگر	۱۲۰.۰۰۰ نمونه: ۶۰.۰۰۰ یوآرال دام چینی و ۶۰.۰۰۰ یوآرال قانونی	یادگیری ژرف	شبکه عصبی بازگشتی + واحد بازگشتی دروازه‌ای [28]
۹۷/۶	- استخراج یک ویژگی مبتنی بر رتبه صفحه از پایگاه آکسا (از دسترس خارج شده)	- بهینه‌سازی مجموعه قواعد با الگوریتم تکامل تفاضلی	۲۰.۰۰۰ نمونه: ۱۰.۰۰۰ یوآرال دام چینی و ۱۰.۰۰۰ یوآرال قانونی با ۶ ویژگی	منطق فازی	سامانه فازی [22]
۹۸/۵۵	- برخی از ویژگی‌ها وابسته به خدمات شخص ثالث، نیازمند بارگیری کامل صفحه و یا مبتنی بر کد صفحه فقط به زبان جاوااسکرپت	- صحت بالا - ویژگی‌های ترکیبی مبتنی بر متن، قالب و تصویر وبگاه	۱۳.۰۰۰ نمونه: ۴.۸۹۸ یوآرال دام چینی، ۱.۹۴۵ یوآرال مشکوک و ۶.۱۵۷ یوآرال قانونی با ۳۵ ویژگی	منطق فازی	انفیس [29]

مقایسه‌ای از صحت به دست آمده در این رویکردها به همراه مزیت‌ها و محدودیت‌های آنها در جدول ۱ گردآوری شده است که نشان می‌دهد عملکرد آنها نه تنها به نوع الگوریتم یادگیری ماشینی، بلکه به نوع ویژگی‌ها و نحوه استخراج آنها وابسته است. ویژگی‌های مبتنی بر متن و یا کد صفحه در صورتی که وابسته به زبان خاصی باشند، در مواجهه با وبگاه‌هایی که به زبان دیگر نوشته شده‌اند، کارایی ندارند. ویژگی‌هایی که استخراج آن‌ها وابسته به خدمات شخص ثالث است، ممکن است منجر به افزایش زمان پاسخگویی و در برخی موارد، ناپایداری سامانه شوند؛ به عنوان مثال رویکردهایی که ویژگی‌های مبتنی بر رتبه صفحه را از پایگاهی مانند آکسا<sup>۲۹</sup> استخراج می‌کردند، با خاتمه یافتن فعالیت این پایگاه در تاریخ ۱ مه ۲۰۲۲، کارایی خود را از دست داده‌اند. علاوه بر این ویژگی‌های مبتنی بر یوآرال به رغم اینکه زمان کمی برای استخراج

<sup>29</sup> alexa

نیاز دارند و مستقل از خدمات شخص ثالث هستند، ممکن است تمام مؤلفه‌های وبگاه‌های دام‌چینی را به خوبی پوشش ندهند و از طرفی اگر مهاجم از روش‌های کوتاه‌کننده‌ی پیوند (مانند بیتلی<sup>۳۰</sup>) استفاده کند، این ویژگی‌ها کارایی ندارند.

## ۴ نتیجه‌گیری

در این مقاله به طور مختصر انواع روش‌های هوشمند در شناسایی وبگاه‌های دام‌چینی، مورد بررسی قرار گرفت. این رویکردها دارای مزایای زیادی از جمله سازگاری با حمله‌های جدید و همچنین صحت بیش از ۹۸ درصدی در برخی موارد بوده‌اند؛ با این حال هنوز مسئله شناسایی وبگاه‌های دام‌چینی با چالش‌هایی جدی روبه‌روست که از مهم‌ترین آن‌ها می‌توان به انتخاب ویژگی‌های کارآمد و ارائه مدلی قوی به منظور بررسی آنها و پاسخگویی سریع در مورد وبگاه‌های جدید اشاره کرد.

## مراجع

- [1] R. M. Mohammad, F. Thabtah, and L. McCluskey, "Tutorial and critical analysis of phishing websites methods," *Computer Science Review*, vol. 17, 2015, pp. 1-24.
- [2] L. Tang, and Q. H. Mahmoud, "A Survey of Machine Learning-Based Solutions for Phishing Website Detection," *Machine Learning and Knowledge Extraction*, vol. 3, 2021, pp. 672-694.
- [3] A. Shaikh, A. Shabut, and A. Hossain, "A literature review on phishing crime, prevention review and investigation of gaps," In 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), 2016, pp. 9-15.
- [4] O. K. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine learning based phishing detection from URLs," *Expert Systems with Applications*, vol. 117, 2019, pp. 345-357.
- [5] A. K. Jain and B. B. Gupta, "A survey of phishing attack techniques, defence mechanisms and open research challenges," *Enterprise Information Systems*, 2021, pp. 1-39.
- [6] B. B. Gupta, K. Yadav, I. Razzak, K. Psannis, A. Castiglione, and X. Chang, "A novel approach for phishing URLs detection using lexical based machine learning in a real-time environment," *Computer Communications*, vol. 175, 2021, pp. 47-57.
- [7] APWG. Phishing Activity Trends Report. 1th quarter 2019: 1th quarter 2022. available at <https://apwg.org/trendsreports/> Last accessed on 4 Mar, 2022.
- [8] M. Wu, R. C. Miller, and S. L. Garfinkel, "Do security toolbars actually prevent phishing attacks?," In Proceedings of the SIGCHI conference on Human Factors in computing systems, 2006, pp. 601-610.
- [9] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommunication System*, vol. 67, 2018, pp. 247-267.

<sup>30</sup>bitly



- [10] Avanan. 1H Cyber Attack Report. 2021. available at <https://www.avanan.com/resources/white-papers/1h-cyber-attack-report> Last accessed 26 Aug, 2022.
- [11] R. Alabdan, "Phishing Attacks Survey: Types, Vectors, and Technical Approaches," *Future Internet*, vol. 12, 2020, pp. 1-37.
- [12] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Systems with Applications*, vol. 106, 2018, pp. 1-20.
- [13] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommunication Systems*, vol. 76, 2021, pp. 139-154.
- [14] P. Kalaharsha and B.M. Mehtrea, "Detecting Phishing Sites - An Overview," 2021, arXiv, arXiv:2103.12739.
- [15] W. Wang, F. Zhang, X. Luo, and S. Zhang, "Pdcnn: precise phishing detection with recurrent convolutional neural networks," *Security and Communication Networks*, 2019.
- [16] M. Khonji, Y. Iraqi, and A. Jones, "Phishing detection: a literature survey," *IEEE Communications Surveys & Tutorials*, vol. 15, 2013, pp. 2091-2121.
- [17] N. Q. Do, A. Selamat, O. Krejcar, E. Herrera-Viedma, and H. Fujita, "Deep Learning for Phishing Detection: Taxonomy, Current Challenges and Future Directions," *IEEE Access*, 2022.
- [18] E. Buber, Ö. Demir, and O. K. Sahingoz, "Feature selections for the machine learning based detection of phishing websites," *International Artificial Intelligence and Data Processing Symposium (IDAP)*, 2017, pp. 1-5.
- [19] A. C. Bahnsen, E. C. Bohorquez, S. Villegas, J. Vargas, and F. A. González, "Classifying phishing URLs using recurrent neural networks," In *2017 APWG symposium on electronic crime research (eCrime)*, IEEE, 2017, pp. 1-8.
- [20] L. A. Zadeh, "Fuzzy logic," *Computer*, vol. 21, 1988, pp. 83-93.
- [21] G. A. Montazer and S. ArabYarmohammadi, "Detection of phishing attacks in Iranian e-banking using a fuzzy-rough hybrid system," *Applied Soft Computing*, vol. 35, 2015, pp. 482-492.
- [22] R. M. Abdul-Hussein, A. H. Mohammed, and A. A. Kadhim, "Detecting Phishing Cyber Attack Based on Fuzzy Rules and Differential Evaluation," *TEM Journal*, vol. 11, 2022, pp. 543-551.
- [23] A. K. Jain and B. B. Gupta, "Towards detection of phishing websites on client-side using machine learning based approach," *Telecommunication Systems*, vol. 68, 2018, pp. 687-700.
- [24] M. Zouina and B. Outtaj, "A novel lightweight URL phishing detection system using SVM and similarity index," *Human-centric Computing and Information Sciences*, vol. 7, 2017, pp. 1-13.

- [25] M. Moghimi and A. Y. Varjani, "New rule-based phishing detection method," *Expert systems with applications*, vol. 53, 2016, pp. 231-242.
- [26] M. A. Adebowale, K. T. Lwin, and M. A. Hossain, "Intelligent phishing detection scheme using deep learning algorithms," *Journal of Enterprise Information Management*, 2020.
- [27] A. Aljofey, Q. Jiang, Q. Qu, M. Huang, and J. Niyigena, "An Effectiv Phishing Detection Model Based on Character Level Convolutional Neural Network from URL," *Electronics*, vol. 9, 2020.
- [28] L. Tang, and Q. H. Mahmoud, "A Deep Learning-Based Framework for Phishing Website Detection," *IEEE Access*, vol. 10, 2021, pp. 1509-1521.
- [29] M. A. Adebowale, K. T. Lwin, E. Sanchez, and M. A. Hossain, "Intelligent web-phishing detection and protection scheme using integrated features of Images, frames and text," *Expert Systems with Applications*, vol. 115, 2019, pp. 300-313.

# واکاوی نظریه‌های قدرت سایبری و ارائه مدل مفهومی نوین برای قدرت سایبری

خداداد هلیلی<sup>۱</sup>

<sup>۱</sup> استادیار، دانشکده کامپیوتر، دانشگاه شهید ستاری، تهران  
kh.halili@ssau.ac.ir

## چکیده

فضای سایبر به خاطر دارا بودن تمامی مؤلفه‌های قدرت در ابعاد سیاسی، اقتصادی، اجتماعی، فرهنگی، علم و فناوری، دفاعی/امنیتی و حقوقی/قضایی فرصت مناسبی را برای تداوم و افزایش قدرت ملی، فراهم نموده است. گستره‌ی جهانی تأثیرگذاری فضای سایبر در تمامی عرصه‌های حیات بشری، لزوم بازتعریف قدرت سایبری را روشن می‌سازد؛ چرا که قدرت سایبری با اینکه همانند قدرت ملی در مرزهای جغرافیایی یک کشور تعریف می‌شود؛ اما دامنه‌ی عملیاتی و پیامدهای آن نامحدود است. در این مقاله پس از مروری بر مفاهیم قدرت، نظریه‌های اندیشمندان جهانی در مورد قدرت سایبری بررسی شده و با ارائه یک مدل مفهومی نوین، مفهوم‌شناسی قدرت سایبری مورد توجه قرار گرفته است. از دیدگاه بسیاری از اندیشمندان، قدرت سایبری از مهم‌ترین حوزه‌های قدرت در عرصه تعاملات جهانی است و سیاست‌گذاری‌ها و راهبردهای کلان بسیاری از کشورها، بر مبنای قدرت سایبری بنا شده است. فائق آمدن بر بحران‌های سایبری و چالش‌های امنیتی در سطح ملی و دستیابی به نفوذ و اقتدار در تراز جهانی، مستلزم شناخت دقیق و موشکافانه‌ی مفهوم قدرت سایبری، برآورد ظرفیت و منابع داخلی قدرت در فضای سایبر و برنامه‌ریزی راهبردی برای ارتقاء آن در کشور است. شناخت نظریه‌های مطرح‌شده در زمینه‌ی قدرت سایبری، موجب همگرایی و گفتمان‌سازی در درک قواعد بازی در فضای سایبر و تصمیم‌گیری مناسب جهت بهره‌برداری از فرصت‌ها و قابلیت‌های آن، خواهد شد.

**کلمات کلیدی:** فضای سایبر، قدرت، قدرت سایبری، فرکتال.

## ۱ مقدمه

در دوران معاصر، فضای سایبر موجب تغییر در افکار و باورهای سنتی و شکل‌گیری و تکامل ابعاد جدیدی از ارزش‌های حیاتی در مقوله قدرت شده است. این مسئله روابط میان کشورها برای قدرت‌طلبی را با چالش‌ها، تهدیدات و فرصت‌های نوینی مواجه نموده است. در فضای سایبر، افراد و جوامع بهره‌بردار، مجبور به تبعیت از قوانین موضوعه توسط جوامع پیشرو و صاحبان فناوری در این فضا هستند و اعمال قدرت و تأثیرگذاری بر جوامع پیرو از این طریق انجام می‌شود. پیامدهای این تأثیرگذاری، جهت‌دهی به باورها، ترجیحات، اولویت‌ها،

الگوهای فکری و رفتاری است که به طور مستقیم و عینی با اعمال زور، سلطه تحریم و تشویق یا غیرمستقیم و نامحسوس از طریق تهدید و نفوذ به دست می‌آید.

از دیدگاه بسیاری از اندیشمندان، قدرت سایبری نه تنها ابزاری مکمل و هم‌افزا برای قدرت ملی، بلکه نشانگر توانایی یک دولت در بهره‌گیری از منابع و قابلیت‌های فضای سایبر برای اعمال نفوذ در تمامی حوزه‌های عملیاتی و راهبردی است. جوزف نای<sup>۱</sup> معتقد است امروزه قدرت‌طلبی کشورها از مرزهای زمینی به فضای سایبر کشیده شده و نگرانی و دغدغه کشورها از وقوع جنگ‌های سایبری حتی در راهبردهای پیمان‌های نظامی کلاسیک مانند ناتو نیز وارد شده است [۵]، از طرفی به دلیل وابستگی رو به رشد زیرساخت‌های حیاتی به فضای سایبر و عدم تسلط کافی بر تمامی منابع موجود در آن، کشورها همواره با تهدیدات و چالش‌های جدی ملی و بین‌المللی در این فضا مواجه هستند. بر این اساس گفتمان‌سازی و شناخت این چهره نوظهور از قدرت در سطح کشور امری ضروری است که در این مقاله به آن پرداخته شده است.

قدرت سایبری علاوه بر نقش بازدارندگی در مقابل این تهدیدات، در تأمین منافع سیاسی، اقتصادی، دفاعی، امنیتی و افزایش اعتبار بین‌المللی از جایگاه ویژه‌ای برخوردار است. نوآوری ویژه این تحقیق را می‌توان در ارائه مدل مفهومی با رویکردی جامع برای برای قدرت سایبری دانست. مطالب مطرح شده در این مقاله، می‌تواند شالوده سیاست‌گذاری در حوزه قدرت سایبری در سطوح راهبردی، عملیاتی و تکنیکی و مبنایی برای برنامه اقدام ارتقاء قدرت سایبری کشور در تراز جهانی قرار گیرد.

این مقاله در چهار بخش تدوین شده است. در بخش اول مفهوم قدرت مورد بررسی قرار گرفته است. در بخش‌های دوم و سوم با مروری بر نظریه‌های قدرت سایبری به مفهوم‌شناسی قدرت سایبری پرداخته شده و در بخش چهارم یک مدل مفهومی برای قدرت سایبری معرفی و اجزای آن توصیف شده است.

## ۲ مفهوم شناسی قدرت

در طول تاریخ، مفهوم «قدرت» در حوزه‌های علوم طبیعی، اجتماعی، سیاسی، نظامی، روان‌شناسی، حقوق و فلسفه مورد استفاده قرار گرفته است. از منظر اندیشمندان علوم اجتماعی و سیاسی، واژه کلیدی قدرت از جایگاه محوری و ویژه‌ای برخوردار است و با مفاهیمی مانند توانایی، قابلیت تأثیرگذاری، کنترل، نفوذ و تسلط بکار رفته است. مفهوم قدرت امروزه یک مفهوم تک‌بعدی نیست بلکه مفهومی چندوجهی است که در ابعاد فردی، اجتماعی، ملی و جهانی نیازمند بازتعریف و شناخت همه مؤلفه‌های مرتبط با آن است. قدرت، در یک نگاه کلی، به معنی استفاده از منابع مادی و معنوی به منظور اعمال اراده و تأثیرگذاری بر دیگران و ایجاد رفتار مطلوب توسط آنهاست؛ به طوریکه در آن، طرف مقابل مجبور، متمایل یا مشتاق به اطاعت نباشد. اندیشمندانی مانند نیکولو ماکیاوولی<sup>۲</sup>، توماس هابز<sup>۳</sup>، ماکس وبر<sup>۴</sup>، کارل هنریش مارکس<sup>۵</sup>، برتراند راسل<sup>۶</sup>، الوین

<sup>1</sup>Joseph Samuel Nye

<sup>2</sup>Niccolò Machiavelli

<sup>3</sup>Thomas Hobbes

<sup>4</sup>Max Weber

<sup>5</sup>Karl Heinrich Marx

<sup>6</sup>Bertrand Arthur William Russell

تافلر<sup>۷</sup>، میشل فوکو<sup>۸</sup> و جوزف نای به بحث و بررسی در مورد جنبه‌های مختلف قدرت از جمله تعریف، انواع، منابع، ویژگی‌ها، آثار و پیامدهای قدرت پرداخته‌اند. مرور دیدگاه‌های مختلف در مورد مفهوم قدرت، مهم‌ترین ویژگی‌های آن را می‌توان به صورت زیر برشمرد [۱]:

- قدرت مفهوم درونی است و از مسیر اراده بروز و ظهور پیدا می‌کند با این حال، تجلی ظاهری قدرت در نگاه طرف مقابل همیشه بیانگر میزان قدرت واقعی نیست.
- قدرت، مبتنی بر تعامل و رابطه دو طرفه است. اعمال قدرت از یک طرف بر طرف دیگر که با همکاری یا کشمکش همراه است. از دیدگاه برتراند راسل قدرت علاوه بر اعمال قدرت بر انسان به قدرت بر ماده بی‌جان و غیر بشر نیز برمی‌گردد. پیشرفت‌های علمی معاصر ناشی از قدرت انسان بر اشیاء است.
- برخی دیدگاه‌ها مانند مارکسیسم، قدرت را هدف می‌دانند و اقتصاد نیز وسیله‌ای برای دستیابی به قدرت است؛ اما در مکاتب توحیدی، قدرت وسیله است نه هدف غایی. علامه طباطبایی در تفسیر میزان قدرت و ثروت را از دیدگاه قرآن دو ابزار برای تأمین سعادت اخروی مطرح می‌کند و هیچکدام هدف نیستند
- نقش قدرت در علوم اجتماعی مشابه نقش انرژی در علم فیزیک است.

### ۳ نظریه‌های قدرت سایبری

قدرت سایبری از مفاهیم نوظهور در ادبیات جهانی در دو دهه اخیر است. این مفهوم ممکن است در معرض برداشت‌های هرمنوتیک قرار گیرد. در این بخش به مروری بر تحقیقات انجام شده مرتبط با قدرت سایبری می‌پردازیم [۲].

۱. تیم جوردن<sup>۹</sup>: یکی از اولین نظریه‌پردازان در زمینه قدرت سایبری، تیم جردن، استاد بریتانیایی فعال در حوزه فرهنگ دیجیتال است. وی در کتاب خود با عنوان «قدرت سایبری: فرهنگ و سیاست‌های فضای سایبر» فضای سایبر را از منظر اجتماعی، فرهنگی و سیاسی مورد بررسی قرار داده است. وی معتقد است علیرغم ماهیت پویا و متغیر فضای سایبر، روابط و الگوهای نسبتاً پایداری از سبک زندگی در فضای سایبر در حال شکل‌گیری است. بنابراین با اینکه قدرت در فضای سایبر موضوعی پیچیده است اما می‌توان پیامدهای آن را در حوزه‌های اجتماعی، فرهنگی و سیاسی در نظر گرفت.

۲. فرانکلین کرامر<sup>۱۰</sup>: کرامر، در فصل اول کتاب «قدرت سایبری و امنیت ملی» با ارائه توصیه‌های سیاسی برای یک چارچوب راهبردی، سیاست‌گذاری در فضای سایبر را از منظر امنیت، سرمایه انسانی

<sup>7</sup> Alvin Toffler

<sup>8</sup> Michel Foucault

<sup>9</sup> Tim Jordan

<sup>10</sup> Franklin D. Kramer

و تحقیق و توسعه، حاکمیت بین‌الملل، مسائل ژئوپلیتیک، حملات سایبری، بازدارندگی و نفوذ مورد بررسی قرار داده است. از دیدگاه وی، قدرت سایبری و امنیت ملی، طیف کاملی از فعالیت‌های اجتماعی را در بر می‌گیرند. اقدامات ژئوپلیتیکی سنتی مانند دیپلماسی، نفوذ و اعمال قدرت توسط عاملان دولتی و غیردولتی انجام می‌شود و قدرت سایبری می‌تواند از این فعالیت‌ها پشتیبانی کند. فضای سایبر، فضایی مشابه فضای واقعی زمین، دریا، هوا و فضاست و تسلط بر فضای سایبر و برتری در آن نیز، از طریق قدرت سایبری امکان‌پذیر است.

۳. **دانیل کوهل<sup>۱۱</sup>**: کوهل، استاد مدیریت منابع اطلاعاتی دانشگاه دفاع ملی ایالات متحده، در فصل دوم کتاب قدرت سایبری و امنیت سایبری با عنوان «از فضای سایبر به قدرت سایبر»، با بررسی ویژگی‌های انتقال اطلاعات در فضای سایبر، اینترنت را ستون فقرات ارتباطات در این فضا معرفی نموده است. لذا برتری در فضای سایبر بر اساس عملیات تهاجمی/دفاعی و دفاعی/پشتیبانی تعریف می‌شود که با جمع‌آوری، پردازش و انتشار اطلاعات، مرتبط است [۴]. کوهل، با پیش کشیدن بحث قدرت سایبری آن را با قدرت دریایی یا هوایی مقایسه می‌کند. وی می‌افزاید: اگر فضای سایبر را یک محیط در نظر بگیریم؛ قدرت سایبری سنجشی از توانایی یک کشور در استفاده از محیط فضای سایبر است. در قدرت سایبری، عامل اطلاعات اهمیت زیادی دارد. قدرت سایبری با بعد اطلاعاتی قدرت، در مدل دیپلماسی، اطلاعاتی، نظامی و اقتصادی (DIME) معادل است. بنابراین قدرت سایبری توانایی استفاده از فضای سایبر برای ایجاد برتری و تأثیرگذاری روی محیط‌های عملیاتی دیگر، از طریق ابزارهای فضای سایبر است.

۴. **بتز و استیونز<sup>۱۲</sup>**: دیوید بتز و تیم استیونز در کتاب خود با عنوان «فضای سایبر و دولت‌ها، راهبردهایی برای قدرت سایبری» به استفاده از قدرت سایبری در گفتمان‌های مرتبط با امنیت و موضوعات راهبردی کشورهای مختلف در سال‌های اخیر، اشاره کرده‌اند. قدرت سایبری تنها مانند قدرت هوایی و دریایی در یک قلمرو مشخص تعریف نمی‌شود بلکه باید آن را در حوزه‌های مختلف در نظر گرفت. قدرت سایبری می‌تواند با پیوند میان مؤلفه‌های قدرت، مانند یک کاتالیزور و شتاب‌دهنده، موجب هم‌افزایی و توسعه قابل ملاحظه آنها شود. آنها همچنین معتقدند ابزارهای فضای سایبر برای انجام مأموریت‌های نظامی و پشتیبانی از حوزه‌های اقتصادی و سیاسی قابل استفاده است.

۵. **استوارت و ونتز<sup>۱۳</sup>**: استوارت استار و لاری ونتز در تحقیقی با عنوان «به سوی تکامل نظریه قدرت سایبری» اهداف، رویکرد، ساختار و تعاریف این نظریه را مورد بررسی قرار داده‌اند. از دیدگاه استار، ابعاد نظامی و اطلاعاتی به‌عنوان اهرم‌های اصلی قدرت سایبری محسوب می‌شوند. نتایج این تحقیق نشان می‌دهد نظریه قدرت سایبری باید بر چهار عامل کلیدی متمرکز باشد که عبارتند از: پیشرفت فناوریانه، سرعت و گستره عملیات، کنترل ویژگی‌های کلیدی و بسیج ملی امکانات.

<sup>11</sup>Daniel T. Kuehl

<sup>12</sup>David J. Betz and Tim Stevens

<sup>13</sup>Stuart H. Starr and Larry Wentz



۶. **زیمت و باری<sup>۱۴</sup>**: الیهو زیمت و چارلز باری در کتابی با عنوان «چشم‌انداز نظامی قدرت سایبری» به بررسی قدرت سایبری در حوزه نظامی پرداخته‌اند. در این کتاب، قدرت سایبری نظامی به معنای استفاده از قلمرو فضای سایبر در عملیات نظامی برای پشتیبانی به اهداف و انجام مأموریت‌های نظامی معرفی شده است و در بسیاری از موارد، برای پشتیبانی از عملیات در سایر قلمروهای حوزه‌های نظامی مانند حوزه دریایی نیز مطرح می‌شود. از دیدگاه زیمت و باری، قدرت سایبری، توانمندی در کنترل سامانه‌های فناوری اطلاعات و شبکه‌های فضای سایبر است. قدرت سایبری می‌تواند با پیوند میان مؤلفه‌های قدرت، مانند یک کاتالیزور و شتاب‌دهنده، موجب هم‌افزایی و توسعه قابل ملاحظه آن‌ها شود. آن‌ها همچنین معتقدند ابزارهای فضای سایبر برای انجام مأموریت‌های نظامی و پشتیبانی از حوزه‌های اقتصادی و سیاسی قابل استفاده است [۹].

۷. **جان شلدون<sup>۱۵</sup>**: جان شلدون در مقاله‌ای با عنوان «رازگشایی از قدرت سایبری: اهداف راهبردی در صلح و جنگ»، فضای سایبر را در یک مدل سه بعدی شامل پنج لایه افقی شامل زیرساخت، فیزیکی، نحوی، معنایی و انسانی در نظر گرفته و بر اساس آن قدرت سایبری را میزان کنترل بر این لایه‌ها توصیف می‌کند [۸]. از نظر شلدون، قدرت روی یکی از این لایه‌ها قدرت روی همه لایه‌ها را نتیجه نمی‌دهد. متغیرهای قابل‌سنجش در هر لایه، شاخص مهمی در اندازه‌گیری و مقایسه قدرت است و ضعف در هر کدام از این شاخص‌ها، نیازمند تمرکز برای بهبود عملکرد آن لایه است. طرح‌ریزی قدرت از طریق فضای سایبر با مفهوم سنتی قدرت سخت نظامی متفاوت است که تغییر در رفتار را از طریق تهدیدات دنبال می‌کند. جان شلدون در مقاله دیگری با عنوان «ژئوپلیتیک و قدرت سایبری»، توجه به ابعاد ژئوپلیتیک قدرت سایبری را مورد توجه قرار داده است. از دیدگاه شلدون، قدرت سایبری، توانایی پشتیبانی به اهداف راهبردی و کاهش توانایی دشمن در بهره‌برداری یا حمله به زیرساخت‌های فضای سایبر است. وی قدرت سایبری را یک ابزار مکمل برای قدرت ملی در نظر می‌گیرد که می‌تواند برای استفاده توسط دولتمردان یک کشور، جذاب باشد.

۸. **جوزف نای<sup>۱۶</sup>**: جوزف نای نظریه‌پرداز مشهور آمریکایی، فضای سایبر را کلید قدرت در قرن ۲۱ معرفی می‌کند. وی در سال ۲۰۰۴ در کتاب «قدرت نرم: راه موفقیت در سیاست‌های جهانی»، در ۲۰۰۵ با کتاب «قدرت در عصر اطلاعات، از واقع‌گرایی تا جهانی‌شدن» و در ۲۰۱۱ با کتاب «آینده قدرت» به مفهوم‌سازی و بسط قدرت نرم، قدرت سخت و قدرت هوشمند پرداخته است. از دیدگاه جوزف نای، قدرت سایبری هم به‌صورت نرم و هم سخت می‌تواند در داخل و بیرون از فضای سایبر اهداف خود را دنبال کند. وی قدرت سایبری را قدرت مبتنی بر منابع اطلاعاتی و فناوری‌های مخابراتی می‌داند که در صورت به‌کارگیری راهبردهای مناسب در داخل و از طریق فضای سایبر موجب فعال‌سازی رشد اقتصادی و ارتقاء امنیت ملی خواهد شد [۵].

<sup>14</sup>Elihu Zimet and Charles L. Barry

<sup>15</sup>John B. Sheldon

<sup>16</sup>Joseph Samuel Nye

۹. **جیسون اسپید<sup>۱۷</sup>**: جیسون اسپید در کتاب «قدرت سایبری چین و امنیت ملی آمریکا»، از منظر نظامی به قدرت سایبری پرداخته و تقابل میان چین و ایالات متحده در فضای سایبر را بررسی کرده است. از دیدگاه اسپید، فضای سایبر هم می‌تواند به‌عنوان توانمندساز برای چهار حوزه زمین، دریا، هوا و فضا استفاده شود و هم می‌تواند به‌عنوان یکی حوزه عملیاتی مستقل به‌کار گرفته شود. اسپید قدرت سایبری را توانایی یک دولت-ملت برای برقراری، کنترل و اعمال نفوذ در داخل و از طریق فضای سایبر برای پشتیبانی و پیوستگی با دیگر عناصر حوزه قدرت ملی تعریف می‌کند. دستیابی به قدرت سایبری به توانایی دولت برای توسعه منابع، جهت عملیات در فضای سایبر متکی است [۶].

۱۰. **لی ژانگ<sup>۱۸</sup>**: لی ژانگ در مقاله خود با عنوان «چشم‌انداز چین در جنگ سایبری» قدرت سایبری را توانایی یک کشور در انجام اقدامات و اعمال نفوذ در فضای سایبر تعریف کرده و برای دست یافتن به قدرت سایبری هفت مؤلفه ظرفیت‌های اینترنت و فناوری اطلاعات، ظرفیت‌های صنعت فناوری اطلاعات، ظرفیت‌های تجارت اینترنتی، میزان نفوذ فرهنگ اینترنت در جامعه، دیپلماسی اینترنتی/ظرفیت سیاست خارجی و قدرت نظامی سایبری و اراده ملی و راهبرد فضای سایبر معرفی می‌کند.

۱۱. **جانسن ون وورن<sup>۱۹</sup>**: جانسن ون وورن و همکاران در مقاله خود با عنوان «بلوکهای سازنده قدرت سایبر ملی» به تجزیه و تحلیل عناصر فضای سایبر به‌عنوان محیط قدرت سایبری پرداخته‌اند. از دیدگاه وی قدرت سایبری شامل مؤلفه‌های محیطی، اقتصادی، نظامی، راهبردی و شناختی است.

۱۲. **جیلی وان هاستر<sup>۲۰</sup>**: جیلی وان هاستر در مقاله‌ای با عنوان «ارزیابی قدرت سایبری» به بحث در مورد درک کمی و کیفی از قدرت سایبری پرداخته است. از دیدگاه هاستر، منابع قدرت شامل منابع بالقوه (که می‌تواند موجب بازدارندگی شود)، منابع قابل تبدیل به حوزه‌های دیگر (مانند تبدیل قدرت اقتصادی به قدرت نظامی) و منابع تصمیم‌گیری (اراده و خواسته تصمیم‌گیران و بازیگران) است.

### ۱.۳ جمع‌بندی نظریه‌های مطرح شده در مورد قدرت سایبری

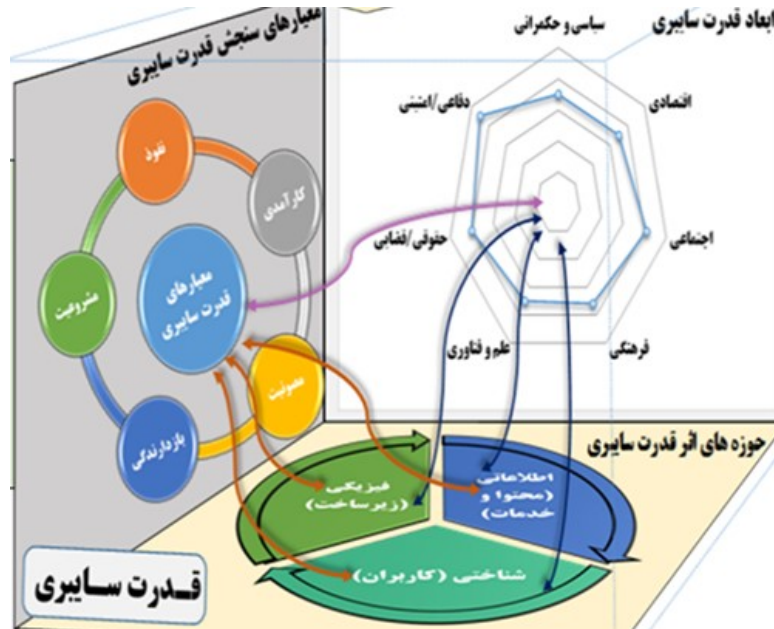
مروری بر نظریه‌های مطرح شده در حوزه قدرت سایبری نشان می‌دهد؛ اغلب اندیشمندان بر اهمیت استفاده از فضای سایبر به‌عنوان یک حوزه مولد قدرت تأکید کرده‌اند. رقابت کشورهای مختلف جهت کسب قدرت و برتری از طریق فضای سایبر در راهبردهای اکثر کشورها قرار گرفته است و کشورها در تلاش برای تسلط بر فضای سایبر و بهره‌گیری از قابلیت‌های ویژه آن برای افزایش قدرت ملی خود هستند. برخی از نظریه‌پردازان با تأکید بر حوزه نظامی قدرت سایبری و در نظر گرفتن فضای سایبر به‌عنوان قلمرو پنجم جنگ، استفاده از فضای سایبر را برای اهداف، مأموریت‌ها و عملیات نظامی بررسی نموده‌اند. بسیاری از اندیشمندان نیز

<sup>17</sup>Colonel Jayson M. Spade

<sup>18</sup>Li Zhang

<sup>19</sup>JC Jansen Van Vuuren

<sup>20</sup>Jelle Van Haaster



شکل ۱: مدل مفهومی اجزای قدرت سایبری

معتقدند همان‌طور که فضای سایبر تمامی ابعاد زندگی را در بر گرفته است، در موضوع قدرت سایبری نیز باید تمامی حوزه‌های مرتبط با آن را در نظر گرفت.

## ۴ مفهوم‌شناسی قدرت سایبری

با مرور دیدگاه‌های مطرح شده می‌توان گفت: قدرت سایبری مجموعه‌ای از منابع، ظرفیت‌ها و توانمندی‌های مبتنی بر فضای سایبر است که به منظور پشتیبانی از قدرت ملی و دستیابی به اهداف راهبردی در فضای سایبر و خارج از آن قابل استفاده است. از آنجا که فضای سایبر، انعکاس و نگاشتی از تمامی پدیده‌های فضای واقعی است، قدرت در فضای سایبر نیز، تمامی ویژگی‌ها و ابعاد قدرت در فضای واقعی را دارد. بر این اساس، در این تحقیق، با در نظر گرفتن رویکرد فرکتالی به قدرت سایبری که در مقاله هلیلی و همکاران به آن پرداخته شده است [۱]؛ مدل مفهومی شکل ۱ برای قدرت سایبری احصاء شده است.

### ۱.۴ توصیف اجزای قدرت سایبری

در این تحقیق، قدرت سایبری است از سه جنبه زیر مورد توجه قرار گرفته است که این سه جنبه به صورت وجوه یک مکعب در تقابل مستقیم با یکدیگر قرار دارند.

۱. ابعاد، مؤلفه‌ها و شاخص‌های قدرت سایبری: دستیابی به قدرت سایبری مستلزم در نظر گرفتن همه ابعاد آن است. البته توسعه این ابعاد ممکن است به شکلی نامتقارن صورت گیرد که از این منظر،

ابعاد قدرت سایبری با یک نمودار عنکبوتی نشان داده شده است. اولویت بخشی به هر کدام از ابعاد هفت گانه به دیدگاه نخبگان، سیاست گذاران و حاکمیت بر می گردد و در تراز جهانی می تواند بر حسب مقتضیات هر کشور متفاوت باشد. اولویت بندی، برنامه ریزی راهبردی و سیاست گذاری در هر کدام از این ابعاد، میزان شناخت نخبگان و سیاست گذاران از ابعاد قدرت سایبری را نشان می دهد.

۲. **حوزه های تأثیرگذار و تأثیرپذیر قدرت سایبری:** قدرت سایبری در فضای سایبر معنا می یابد. بنابراین فضای سایبر به عنوان زمین بازی برای بازیگران قدرت سایبری در عرصه جهانی است. این فضا از منظر قدرت شامل سه حوزه فیزیکی (زیرساخت)، اطلاعاتی (محتوا و خدمات مبتنی بر محتوا) و شناختی (موضوعات مرتبط با کاربران) در نظر گرفته شده است. این سه حوزه در یک تعامل مشترک با هم قرار گرفته اند و محیط عملیاتی برای دستیابی به قدرت سایبری و بهره برداری از آن را تشکیل می دهند. سرمایه گذاری برای توسعه هر کدام از این سه حوزه نیازمند شناخت دقیق عناصر و اجزای هر حوزه است.

۳. **معیارهای قدرت سایبری:** قدرت سایبری همانند سایر گونه های قدرت به معنای تأثیرگذاری و کسب نتایج مطلوب تحقق می یابد. در جمهوری اسلامی ایران دستیابی به قدرت سایبری از منظر معیارهای بومی در نظر گرفته شده قابل تحقق است. در این مقاله داشتن نفوذ، مشروعیت، کارآمدی، بازدارندگی و مصونیت در فضای سایبر، به عنوان نشانگرهای اصلی برای قدرت سایبری مطرح شده است. هر کدام از شاخص های احصاء شده را می توان با این معیارهای پنج گانه مورد بررسی و ارزیابی قرار داد.

## ۵ نتیجه گیری

فناوری های فضای سایبر ابزار اداره و تسخیر دنیا و جایگزین قدرت هسته ای و بستری برای جهانی سازی شده است به طوریکه قوام و تداوم اقتدار دولت ها متأثر از آن شده است. کشورهایی که مجهز به فناوری نوظهور این فضا نباشند و خود را ملزم به بهره گیری از قابلیت های آن در قالب قدرت سایبری ندانند، در صحنه جهانی مجالی برای قدرت نمایی ندارند. البته داشتن منابع فیزیکی و غیر فیزیکی سایبری و تسلط فناورانه بر فضای سایبر شرط لازم برای قدرت سایبری است و تبدیل توانمندی های بالقوه به بالفعل با اتخاذ سیاست ها و راهبردهای مناسب و پدیدآوردن آثار و نتایج مطلوب، برای کسب قدرت سایبری ضروری است. در فضای سایبر از ابزارهای غیر فیزیکی مانند سلطه اطلاعاتی، وضع قوانین و استانداردها و دیپلماسی سایبری، یا فیزیکی مانند انحصار فناوری زیرساخت و ارتباطات و تسلیحات سایبری برای اعمال قدرت استفاده می شود. قدرت سایبری تنها شامل کنترل بر منابع مادی فضای سایبر نیست بلکه مدیریت فرایند بهره برداری و موضوعات مرتبط با جوامع انسانی را در بر می گیرد. از این رو، ارتقاء قدرت سایبری رابطه ای مستقیم و منطقی با نوع راهبردها و سیاست گذاری های کلان در حوزه بهره برداری از قابلیت ها و توانمندی های بالقوه و بالفعل و منابع فضای سایبر دارد. امروزه، در فضای سایبر، بخش عمده ای از منابع قدرت، در اختیار شرکت های فراملی و سازمان های

غیردولتی است؛ با این حال مفهوم قدرت سایبری در حیطه مرزهای جغرافیایی و در حوزه عملکرد دولت‌ها تعریف می‌شود. این بدان معناست که قدرت سایبری از جنس قدرت حاکمیت و بیانگر توانمندی‌های یک دولت برای تسلط بر فضای سایبر در سطح ملی است که در یک چارچوب مشروع و مورد قبول، در اختیار دولت‌ها قرار گرفته است.

قدرت سایبری در جمهوری اسلامی ایران، متأثر از عوامل مختلفی است که شناخت این عوامل، سیاست‌گذاری کلان در ابعاد، حوزه‌های تأثیرگذار و تأثیرپذیر و معیارهای قدرت سایبری را تحت تأثیر قرار می‌دهد. تأکید صریح مقام معظم رهبری در مورد ارتقاء قدرت سایبری و توجه به آن به‌صورت ضمنی در اسناد بالادستی نشان‌دهنده اهمیت راهبردی این شکل نوین از قدرت در سطح ملی و تعاملات بین‌المللی است [۳].

## مراجع

- [۱] هلیلی، خداداد، ولوی، محمدرضا، موحدی صفت، محمدرضا و باقری مسعود (۱۳۹۷). قدرت سایبری مبتنی بر رویکرد فرکتالی و بررسی تأثیر آن بر امنیت ملی در فضای سایبر. فصلنامه امنیت ملی، سال ۸ شماره ۲۹.
- [۲] هلیلی، خداداد (۱۳۹۷). ارائه الگوی راهبردی ارتقاء قدرت سایبری جمهوری اسلامی ایران در تراز جهانی. رساله دکتری، دانشگاه عالی دفاع ملی.
- [۳] هلیلی، خداداد، ولوی، محمدرضا و موحدی صفت، محمدرضا (۱۳۹۷). شناسایی عوامل و مؤلفه‌های تأثیرگذار بر تدوین دکترین قدرت سایبری ج.ا.ایران مبتنی بر سیاست‌های ابلاغی و اسناد بالادستی. فصلنامه راهبرد دفاعی، سال ۱۶، شماره ۶۳.
- [4] Kuehl, Daniel. T. (2009). From cyberspace to cyberpower: defining the problem. in Kramer, Franklin D., Starr, Stuart H., and Wentz Larry K. (eds). Cyberpower and National Security. Washington, D.C.
- [5] Nye, Joseph S. (2011). The future of power. Belfer Center for Science and International Affairs. New York.
- [6] Spade, J. M. (2012). China's cyberpower and America's national security. Carlisle Barracks, PA: US ARMY WAR COLLEGE.
- [7] Sheldon, J. (2011). Deciphering cyberpower: Strategic purpose in peace and war. Strategic Studies Quarterly. vol. 5(2), pp. 95-112.
- [8] Sheldon, J. (2014). Geopolitics and Cyber Power: Why Geography Still Matters, American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy, 36(5), pp. 286-293.
- [9] Zimet, E. and Barry, C. (2009). Military Service of Cyber Overview in Military Perspective on Cyberpower, Washington DC Center for Technology and National Security Policy at the National Defense University.





## ابعاد شناختی - هیجانی تعامل انسان - ربات

زهرا نوروزی<sup>۱</sup>، فاطمه امیرخانی<sup>۲</sup>

<sup>۱</sup> دانشجوی دکتری روانشناسی بالینی، دانشکده علوم انسانی، دانشگاه شاهد، تهران، ایران  
zahranorouzi73@gmail.com

<sup>۲</sup> دانشجوی دکتری روانشناسی، دانشگاه علامه طباطبائی، تهران، ایران  
fatemehamir80@gmail.com

### چکیده

تعاملات بین انسان با رباتها در تمام زمینه‌های زندگی به شکل روزافزونی مورد توجه قرار می‌گیرد. چالش‌های زیادی در رابطه با ماهیت تعامل انسان-ربات وجود دارد و سؤالات مهمی در مورد ابعاد شناختی و هیجانی تعامل این عوامل مصنوعی با انسان، مطرح شده است. این پژوهش به بررسی برخی از ابعاد شناختی و هیجانی این تعامل می‌پردازد. در بعد شناختی: انسان‌پنداری، پذیرش و اعتماد و در بعد هیجانی: ترس و اضطراب، عشق و دل بستگی، هدایت و اطاعت، مورد بحث قرار می‌گیرد. در این پژوهش سعی شده بر جنبه‌های مختلف پاسخ‌ها و نگرش‌های انسانی نسبت به رباتها تأکید شود. به مسائل اساسی در مورد رفتار و دیدگاه افراد از جوه شناختی و هیجانی نسبت به رباتها توجه شود و دیدگاهی روان‌شناختی در مورد دریافت انسان از روباتها ارائه شود. تعامل انسان-ربات یک زمینه‌ی پژوهشی رو به رشد اما جدید است و بررسی ابعاد شناختی-هیجانی این تعامل، بینش‌هایی را برای طراحی ربات‌های آینده که نسبت به عوامل روان‌شناختی حساس‌تر هستند، فراهم می‌کند که می‌تواند توجه دیگر پژوهشگران را در حوزه‌های بین‌رشته‌ای مانند اخلاق، روان‌شناسی، علوم اجتماعی و علوم کامپیوتر، به خود جلب کند.

**کلمات کلیدی:** تعامل انسان-ربات، شناختی، هیجانی، روان‌شناسی.

### ۱ مقدمه

تعامل انسان و ربات حوزه‌ای است که به مطالعه، طراحی و ارزیابی سیستم‌های هوش مصنوعی رباتیک برای استفاده انسان‌ها اختصاص دارد. تعامل انسان-ربات، حوزه پژوهشی رو به رشدی است که زمینه‌های مختلفی مانند طراحی، روان‌شناسی، علوم شناختی، علوم اجتماعی، هوش مصنوعی، علوم کامپیوتر، رباتیک و مهندسی را شامل می‌شود [۱]. برخی پژوهشگران این حوزه، بر نحوه درک افراد از رباتها تمرکز دارند. با توجه به این که امروزه رباتها کاربران زیادی دارند، در این حوزه پژوهشی، تجربیات انسان‌محور برجسته می‌شود و در آن انسان‌ها محور اصلی پژوهش هستند [۲].

تعامل انسان و ربات، مطالعه نحوه تعامل انسان با ربات‌ها است. هدف اساسی، طراحی اصولی برای سیستم‌های رباتی است که آن‌ها را قادر به تعامل مستقیم، ایمن و مؤثر با انسان‌ها می‌کند و ضمن بهبود عملکرد ربات، ارزیابی ابعاد، خطرات و مزایای تعامل انسان-ربات ضروری است [۳]. از این نظر، پژوهش‌ها بر تعامل اجتماعی صحیح با ربات از طریق گفتار، ژست‌ها و حالات چهره متمرکز است. بسته به نقش و نوع ربات‌ها، تعامل و ارتباط می‌تواند وجوه مختلفی داشته باشد [۴].

تعامل به عنوان یک عمل یا تأثیر متقابل تعریف می‌شود. بنابراین هر عملی بین انسان و ربات به‌عنوان یک تعامل تلقی می‌شود. به نظر می‌رسد در تعامل موفق انسان و ربات، عوامل شناختی و هیجانی انسان‌ها نقش کلیدی دارند [۵]. از لحاظ تاریخی، هیجان و شناخت به عنوان موجودیت‌های جداگانه در نظر گرفته شده‌اند. به نظر می‌رسد که فرآیندهای شناختی مناطق قشر مغز را درگیر می‌کنند و ساختارهای مغز مرتبط با هیجان‌ات اغلب زیر قشری هستند، مانند آمیگدال، جسم مخطط شکمی و هیپوتالاموس. این ساختارها به لحاظ تکاملی حفظ شده یا ابتدایی در نظر گرفته می‌شوند [۶]. پژوهش‌های فعلی بر وابستگی متقابل جنبه‌های شناختی و هیجانی تأکید می‌کنند [۷]. هرچند بسیاری از رفتارها ممکن است از نظر تعاملات شناختی-هیجانی به خوبی متمایز شوند، به طوری که می‌توان گفت هیجان و شناخت تا حدی قابل تفکیک هستند [۶].

هرچه ربات‌ها در زندگی روزمره ما حضور بیشتری پیدا می‌کنند، این تعامل، اهمیت بیشتری می‌یابد. بنابراین، مطالعاتی که سعی در درک چگونگی شروع و تکامل این رابطه در طول زمان دارند نیز اهمیت بیشتری پیدا می‌کنند. گیتس این نکته را مطرح کرد که وضعیت کنونی رباتیک مشابه دهه ۸۰ با رایانه است و به زودی در «عصر ربات» زندگی خواهیم کرد، به طوری که در هر خانه و محل کاری، یک ربات خواهیم داشت [۸].

همان‌طور که هوش مصنوعی در حال توسعه است، ما با روبات‌های پیچیده‌تر «اجتماعی» مواجه می‌شویم. با این حال، مطالعات کمی در مورد نحوه درک، تعامل یا پذیرش این ماشین‌ها در زمینه‌های اجتماعی وجود دارد. با تأکید بر اهمیت این نفوذ پیش‌بینی‌شده ماشین‌ها در جامعه بشری، آژانس‌های تحقیقاتی بزرگ در سراسر جهان، از جمله کمیسیون اروپا و بنیاد ملی علوم، هدف خود را حمایت از توسعه رباتیک و تلاش برای ادغام ربات‌ها در جامعه قرار داده‌اند. شرکت‌های چندملیتی از جمله فیس‌بوک، آمازون و گوگل همچنان به سرمایه‌گذاری مبالغ قابل توجهی در توسعه هوش مصنوعی و رباتیک ادامه می‌دهند [۹]. این مثال و بسیاری دیگر، حضور رو به رشد عوامل مصنوعی در محیط‌های اجتماعی را پیش‌بینی می‌کند.

با گسترش نفوذ ربات‌ها، سؤالات مهمی در مورد تعامل انسان با عوامل مصنوعی در زمینه ادراک، ارتباط یا همکاری پدیدار می‌شود. علاقه تحقیقاتی روان‌شناسی، علوم اعصاب اجتماعی، علوم کامپیوتر و رباتیک در مورد چگونگی تعامل انسان با عوامل مصنوعی در کنار پیشرفت‌های تکنولوژیکی، پیشرفت کرده‌است. با این حال، به منظور پیشرفت‌های قابل توجه در درک چگونگی ارتباط انسان با بازیگران مصنوعی، گفتگو و همکاری عمیق‌تر و سازنده‌تر در این حوزه‌ها مورد نیاز است. مقاله حاضر در راستای درک بهتر این تعامل، برخی از وجوه و ابعاد این تعامل را در ذیل محور شناختی و هیجانی، برجسته می‌کند.

از نظر روش‌شناسی، پژوهش پیش رو با اتخاذ رویکردی توصیفی - تحلیلی کوشیده است با توصیف تعامل انسان-ربات، به تحلیل ابعاد شناختی و هیجانی این امر بپردازد. این مقاله سعی دارد از طریق بحث در مورد

ابعاد شناختی مانند انسان‌پنداری، پذیرش و اعتماد و ابعاد هیجانی مانند ترس و اضطراب، عشق و دل‌بستگی و هدایت و اطاعت، این ابعاد روان‌شناختی را در تعامل بین ربات و انسان برجسته کند و بینش‌هایی را برای طراحی ربات‌های آینده که نسبت به عوامل روان‌شناختی حساس‌تر هستند، ارائه دهد.

## ۲ ابعاد شناختی

### ۱.۲ انسان‌پنداری

انسان‌پنداری (آنتروپومورفیسم) عموماً به عنوان تمایل انسان به نسبت دادن صفات و رفتار انسانی مانند انگیزه، احساسات و حالات ذهنی انسان، به موجودات غیر انسانی درک می‌شود [۱۰]. استعداد انسان برای انسان‌پنداری مدت‌ها مورد مطالعه قرار گرفته است، اما دلایل مطلق آن و همچنین چگونگی و چرایی ایجاد آن کاملاً مشخص نیست. برداشت مهمی از این موضوع، دیدگاه کاپورائیل و هیس است، که استدلال آنها مستلزم این نظریه است که انسان‌سازی یک پیش‌فرض شناختی است که برای تکامل اجتماعی گونه‌ی انسان ضروری بود [۱۱].

گرایش به انسان‌پنداری پدیده‌ای است که عامل اصلی در طراحی ربات‌های اجتماعی بوده است و به عنوان ابزاری برای تسهیل تبادل اجتماعی بین ربات‌ها و انسان‌ها استفاده شود. ایده اصلی این است که کاربران را را تحریک کنند تا احساسات و حالات ذهنی انسانی را به ربات‌ها نسبت دهند که باعث افزایش آشنایی و ارتقای تعاملات اجتماعی شود [۱۲]. این ایده، سؤالاتی را در مورد نقش آنتروپومورفیسم در تعامل انسان- ربات ایجاد می‌کند. شواهد به‌دست آمده از پژوهش‌ها نشان می‌دهد که آنتروپومورفیسم بر ماهیت رفتار شرکت‌کنندگان در طول آزمایش تأثیر می‌گذارد [۱۳]. به‌عنوان مثال، برخی پژوهش‌های آزمایشی نشان داده‌اند که ربات‌های انسان‌نما ممکن است ترسناک تلقی شوند، در حالی که برخی دیگر مزایای درمانی را نشان داده‌اند [۱۴، ۱۵].

نگرانی‌هایی در مورد انسان‌پنداری ربات‌ها مطرح می‌شود که این پدیده ممکن است ویژگی‌هایی را که انسان‌ها را منحصر به فرد می‌کند، بی‌ارزش کند یا به این نکته اشاره می‌کنند که چگونه انسان‌پنداری موجب تسهیل وابستگی بیشتر به ربات‌ها می‌شود و این امر باعث ناراحتی یا به خطر انداختن جان انسان‌ها برای چیزی که واقعاً زنده نیست، می‌شود. اگر رباتی بیش از حد انسان‌سازی شود، افراد ممکن است خود را در معرض خطر قرار دهند تا از ربات محافظت کنند [۱۶]. در چت‌بات‌های همراه یا درمانی، پیام‌هایی که توسط ربات ارسال می‌شود توسط یک شنونده همدل ایجاد نمی‌شود، بلکه این پیام‌ها توسط شرکت‌هایی برنامه‌ریزی شده است که ممکن است منافی غیر از منافع انسانی داشته باشند و این نگرانی به‌ویژه در هنگام در نظر گرفتن ربات‌ها به‌عنوان همراه کودکان و سایر گروه‌های آسیب‌پذیر بسیار مهم است [۱۷]. اگر افرادی به‌علت بیماری مانند زوال عقل نتوانند تشخیص دهند که ربات یک ماشین است یا یک موجود زنده، این بحث تبدیل به یک معضل اخلاقی می‌شود که به آنها اجازه می‌دهد فکر کنند با یک موجود زنده در حال تعامل هستند، در حالی که نیستند [۱۸، ۱۹]. با این حال، با وجود این نگرانی‌ها، بعید به نظر می‌رسد که پیشرفت در معرفی ربات‌ها یا فرایند انسان‌پنداری به آنها کاهش یابد. بنابراین به نظر می‌رسد پژوهش‌های بیشتری لازم است

تا مشخص شود که چگونه می‌توان به بهترین وجه به یک تعامل سالم و طولانی‌مدت با ربات‌ها، با در نظر گرفتن انسان‌پنداری دست یافت.

## ۲.۲ پذیرش و اعتماد

ربات‌ها به‌عنوان بخشی جدید از تجربه اجتماعی زندگی جدید، نیاز به پذیرش توسط انسان و ترکیب با ساختارهای انسانی دارند. چه چیز تعیین می‌کند که ربات‌ها با موفقیت در ساختار جامعه ادغام شوند؟ پاسخ این پرسش «پذیرش و اعتماد» است [۲۰].

بر اساس تعریف انجمن روان‌شناسی آمریکا اعتماد به احساس اتکا یا اطمینان نسبت به کسی یا چیزی گفته می‌شود. به طور خاص، اعتماد معیاری است که هر یک از طرفین احساس می‌کنند که می‌توانند برای انجام کاری که طرف مقابل وعده داده است به او وابسته باشند. عامل کلیدی در اعتماد، صداقت ذاتی افراد دیگر نیست، بلکه قابل پیش‌بینی بودن آنهاست. اکثر روان‌شناسان اعتماد را جزء اصلی در روابط بالغ با دیگران اعم از روابط صمیمی، اجتماعی یا درمانی می‌دانند [۲۱].

اعتماد به‌طور گسترده نشان‌دهنده تمایل فرد برای آسیب‌پذیر بودن در برابر دیگران است [۲۲]. اعتماد انسان‌ها به ربات‌ها بر پذیرش این سیستم‌ها برای تعامل اجتماعی استوار است [۲۰]. مسئله پذیرش و اعتماد در رابطه بین انسان و ربات در چند حوزه اهمیت دارد:

۱. اعتماد به ربات میزان تکیه و وابستگی انسان‌ها به ربات‌ها در حوزه‌های مختلف را شکل داده است. پس از شکل‌گیری اعتماد اولیه، هر مقدار که اعتماد بیشتر باشد انسان به لحاظ شناختی خود را وابسته‌تر می‌داند. با توجه به اینکه ممکن است ربات‌ها در موقعیت‌های مهم و حساسی حضور داشته باشند، مثلاً در تعامل با افراد بیمار و ناتوان که به‌لحاظ فیزیکی و روانی نیاز به حمایت دارند و یا در حوزه‌هایی که پای اطلاعات شخصی افراد در میان است، میزان و چگونگی شکل‌گیری اعتماد بین انسان و ربات حائز اهمیت است [۲۳]. چرا که ممکن است این وابستگی عواقبی برای انسان داشته باشد.

۲. ربات‌ها به‌طور فزاینده‌ای توانایی پشتیبانی و انجام عملکردهای انسانی را پیدا کرده‌اند. در ظاهر این پیشرفت بزرگی به حساب می‌آید. چرا که ربات‌ها موجب بهبود زندگی انسان شده‌اند. با این حال اعتماد به ربات‌ها افزایش احتمال خطر را بالا می‌برد. به معنای دیگر، هر چقدر اعتماد به یک سیستم افزایش پیدا کند، هنگام بروز اشتباه منجر به عواقب فاجعه‌بارتری به نسبت زمانی که اعتماد کمتری به سیستم داریم، خواهد شد [۲۴، ۲۵].

۳. جدای از دلایل عمل‌گرایانه برای اعتماد به یک سیستم هوش مصنوعی وابسته می‌تواند دلایل معرفتی نیز برای اعتماد وجود داشته باشد که مبتنی بر اعتقاد اعتمادکننده به قابل اعتماد بودن ربات است. از این منظر اعتماد صرفاً مبتنی بر باورهای شناختی یا عقلانی نیست، بلکه نوعی نگرش است که جنبه‌های عاطفی نیز در آن درگیر است. آیا این نوع از اعتماد منجر به فریب انسان می‌شود؟

گرو دزینسکی و همکاران [۲۶] فریب ظاهری را یک مسئله در اعتماد می‌دانند. اگر یک ربات به گونه‌ای رفتار کند که کاربر انسانی گمراه شود و آن را باور کند یا طوری رفتار کند که گویی ربات یک انسان یا حیوان است، در واقع مسئله فریب رخ داده است. از سویی آنها استدلال می‌کنند که در جایی که توسعه‌دهنده نرم‌افزار از فریب در طراحی ربات برای کمک به کاربر استفاده کرده است، فریب کاری پسندیده تلقی می‌شود و شامل نقض اعتماد نمی‌شود. برای مثال فریب بیمار دچار زوال عقل توسط ربات برای نجات جان کارکنان پزشکی از جمله مواردی است که اعتماد را خدشه‌دار کرده اما نتایج مطلوبی به بار می‌آورد.

با این حال با توجه به آسیب‌پذیری که هنگام اعتماد شکل می‌گیرد، پرسش درباره میزان و چگونگی پذیرش ربات توسط انسان و اعتماد به سیستم هوش مصنوعی همچنان باقیست.

### ۳ ابعاد هیجانی

#### ۱.۳ ترس و اضطراب

یکی از ابعاد هیجانی در تعامل انسان و ربات، ترس و اضطراب نسبت به ربات‌ها است. پژوهش‌ها حاکی از آن است که به نظر می‌رسد منفی‌گرایی و ترس زیاد نسبت به ربات‌ها ریشه در این نگرانی دارد که ربات‌ها ممکن است به موقعیت‌ها و خواسته‌های اجتماعی به روش‌های غیرانسانی پاسخ دهند و همچنین به دلیل عدم شفافیت در مورد قابلیت‌ها و کاربردهای یک ربات، اضطرابی در مورد اینکه «ربات‌ها چه قدرتی خواهند داشت» و «ربات‌ها چه کاری انجام خواهند داد»، وجود دارد [۲۷].

در حالی که برانگیختن پاسخ‌های اجتماعی در انسان‌ها زمانی که ربات از نظر طراحی شبیه انسان باشد، آسان‌تر است، اما این بدان معنا نیست که ربات‌ها به‌طور خودکار هر چه انسان‌تر به نظر می‌رسند پذیرفته‌تر می‌شوند. ممکن است در ابتدا این‌طور باشد، اما به نظر می‌رسد طراحی انسان‌مانند به نقطه‌ای می‌رسد که در آن پاسخ‌های اجتماعی مثبت به پاسخ‌های منفی تبدیل می‌شوند و ربات‌ها به دلیل «بیش از حد انسانی» بودن، رد می‌شوند. این پدیده «دره غیرعادی» نامیده می‌شود، و نقطه‌ای را توصیف می‌کند که در آن چیزی غیرانسانی چنان انسانی به نظر می‌رسد که اضطراب برانگیز و وحشتناک ادراک می‌شود. این یک چالش برای طراحی ربات اجتماعی است. این امر با این واقعیت دشوارتر می‌شود که اثر دره غیرعادی بین افراد متفاوت است [۲۸].

شاید این دیدگاه منطقی باشد که ربات‌ها هنوز برای بسیاری از کاربران جدید هستند، و بنابراین برای کسانی که تجربه کمی از تعامل با آنها دارند، جدید و بالقوه ترسناک به نظر می‌رسند. مطالعات نشان می‌دهند که در اضطراب نسبت به ربات‌ها، تفاوت‌های فردی وجود دارد و مهم‌ترین زمینه‌های نگرانی، جنسیت و فرهنگ متفاوت است [۲۹]. برای مثال، تفاوت‌های جنسیتی ممکن است نشان دهد که زنان نسبت به مردان نگرانی بیشتری در مورد تعامل با ربات‌ها احساس می‌کنند [۲۷]. در همین حال، تفاوت‌های فرهنگی نشان می‌دهد که نه تنها ربات‌ها به‌طور کلی متفاوت درک می‌شوند، بلکه ترس‌های مرتبط با آنها نیز بین فرهنگ‌ها متفاوت است. به عنوان مثال، اروپایی‌ها ممکن است نگرانی‌های «عملیاتی» تری داشته باشند و به کارکرد ربات‌ها در زندگی روزمره فکر کنند. از سوی دیگر، آسیایی‌ها ممکن است در تعامل با ربات‌ها نگرانی‌های

بیشتری را در زمینه‌های «شخصی و اجتماعی» ابراز کنند [۳۰]. این مسئله می‌تواند به تصویرهای متفاوتی از ربات‌ها در رسانه‌های آسیایی و اروپایی هم مربوط باشد [۳۱].

مطالعات شواهدی ارائه می‌دهند که اضطراب، کیفیت تعامل افراد با ربات‌ها را پیش‌بینی می‌کند. تلاش برای کاهش اضطراب ربات اغلب به شکل قرار گرفتن در معرض ربات‌ها است [۳۲]. با این حال، نتایج پس از قرار گرفتن در معرض ربات‌ها متناقض است و به نظر می‌رسد به طراحی ربات و ویژگی‌های فردی بستگی دارد [۱۹، ۲۹].

### ۲.۳ عشق و دلبستگی

عشق یکی از برترین احساسات اساسی است. عشق به قوی‌ترین شکل بر پاسخ فیزیولوژیکی و ذهنی سوژه تأثیر می‌گذارد. لوی [۳۳] این مسئله را مطرح می‌کند که وقتی ربات‌ها بسیار شبیه انسان می‌شوند، عشق و رابطه جنسی با ربات‌ها مانند انسان‌ها معمول می‌شود. در این زمینه، نگرانی‌های مهمی در مورد جنبه‌های اجتماعی، اخلاقی و فرااخلاقی مطرح می‌شود.

بیشتر منتقدان تأکید می‌کنند که روابط عاطفی با ماشین‌ها دست کم عجیب یا مستقیماً خطرناک هستند. این انتقاد اغلب به شیوه‌ای کاملاً کلی استدلال می‌کند که ماشین‌ها ممکن است جایگزین انسان شوند [۳۴]. سایر منتقدان بیشتر روی خطر سوء استفاده ماشین‌های احساسی تمرکز می‌کنند [۳۵]. وقتی رفتار ربات شخصی‌تر باشد، تعامل عاطفی با کاربر قوی‌تر می‌شود. این اساساً دو نتیجه دارد: اینکه عملکرد ربات ممکن است مستلزم مدیریت احساسات کاربر نیز باشد و اینکه ممکن است تعامل انسان-ربات در سطح احساسی ایمن نباشد. برای مثال، برخی از پژوهشگران در بارسلونا از یک ربات اجتماعی برای کمک به بهبود اثربخشی درمان‌های عصبی روان‌شناختی برای کودکان استفاده کردند. پس از شش ماه از فرآیند توان‌بخشی، محققان تصمیم گرفتند ویژگی‌های شخصی‌سازی را به ربات اضافه کنند تا با علاقه کودکان مطابقت داشته باشد. نتایج مطالعه آن‌ها افزایش تعامل کودکان را نشان داد اما سال‌ها بعد، یکی از نویسندگان اذعان کرد که وابستگی خیلی زیادی به ربات وجود داشت و پیوند عاطفی و دلبستگی ایجاد شده بین ربات و کودک بسیار قوی بود [۳۶].

دلبستگی در ادبیات تعامل انسان-ربات به روش‌های مختلفی مورد بحث قرار می‌گیرد. با این حال، در سراسر مطالعات، هشدارهایی در مورد پتانسیل ربات‌ها برای تقویت دلبستگی با هم‌تایان انسانی خود و ایجاد موقعیت‌های غیراخلاقی وجود دارد. شارکی این موضوع را عمیقاً مورد بحث قرار می‌دهد و چارچوب دلبستگی روان‌شناختی را در موقعیت‌هایی که ربات‌ها ممکن است از کودکان مراقبت کنند، به کار می‌برد [۳۷]. نورمن در کتاب خود در سال ۲۰۰۴ درباره اشیاء عاطفی، به‌طور خلاصه درباره پیامدهای اخلاقی «ربات‌های انسان‌نما که دارای احساسات هستند و افراد ممکن است وابستگی عاطفی قوی به آنها ایجاد کنند» هشدار می‌دهد [۳۸، ۳۹].

سؤالات پژوهشی مهمی در مورد دلبستگی در تعامل انسان-ربات وجود دارد. اگرچه به نظر می‌رسد روند فعلی مطالعات دلبستگی در تعامل انسان و ربات بر توسعه قابلیت‌های رباتیک خاصی که ممکن است به دلبستگی منجر شود متمرکز است، شاید به موازات آن باید پیرسیم که چگونه این قابلیت‌ها بر دلبستگی که



شکل می‌گیرد تأثیر می‌گذارد و ما می‌خواهیم ربات‌ها چه نقشی در دنیای دلبستگی‌های ما داشته باشند؟

## ۳.۳ هدایت و اطاعت

پژوهش‌ها نشان می‌دهد که انسان‌ها می‌توانند از نظر عاطفی توسط ربات‌ها دستکاری و هدایت شوند و این منجر به اطاعت از ربات‌ها می‌شود [۴۰]. پژوهشی که توسط گروهی از محققان در آزمایشگاه تعامل انسان با کامپیوتر در کانادا انجام شد، شواهدی را نشان داد که افراد می‌توانند توسط یک ربات به انجام کاری که نمی‌خواهند انجام دهند، تشویق شوند و تقریباً نیمی از افرادی که در آزمایش شرکت کردند، وقتی که یک ربات از آنها خواست کاری را انجام دهند که نمی‌خواستند انجام دهند، آن کار را انجام دادند [۴۱].

گروهی از پژوهشگران دریافته‌اند که انسان‌ها می‌توانند در معرض دستکاری عاطفی توسط یک ربات باشند. در سال ۲۰۰۷، پژوهش‌گران مطالعه‌ای انجام دادند و از داوطلبان خواسته شد تا یک گربه رباتی را خاموش کنند، اما وقتی گربه از آنها درخواست کرد که «لطفاً من را خاموش نکنید»، مطمئن نبودند که چه کار کنند. در یک پژوهش جدیدتر، پژوهشگران این آزمایش را با استفاده از داوطلبان بیشتر و یک ربات متفاوت تکرار کردند. مطالعه جدید شامل ۸۹ داوطلب بود که از آن‌ها خواسته شد تا با یک ربات ارتباط برقرار کنند. در پایان تعامل، یک محقق از داوطلب می‌خواهد که ربات را خاموش کند اما ربات از افراد می‌خواهد که «لطفاً این کار را نکنند». علاوه بر درخواست‌های صوتی، ربات اقدامات بدنی را نیز به منظور تقویت درخواست نمایش می‌دهد. نتایج نشان داد که ۱۳ داوطلب تصمیم گرفتند به خواسته‌های ربات توجه کنند و برای بقیه، خاموش کردن ربات بیشتر از افراد گروه کنترل طول کشید. محققان گزارش می‌دهند که بسیاری از داوطلبان صرفاً به این دلیل که ربات خواسته بود، از خاموش کردن امتناع کردند. برخی دیگر گزارش دادند که برای ربات ناراحت هستند یا نگران انجام کار اشتباهی هستند. این یافته‌ها حاکی از آن است تعامل با ربات می‌تواند منجر به دستکاری هیجانی و اطاعت از ربات‌ها شود [۴۰].

این پژوهش‌ها بر اهمیت مطالعات بیشتر در مورد اقتدار رباتیک تأکید می‌کند و همچنین کمبود دانش عمومی در مورد اطاعت مردم از ربات‌ها را برجسته می‌کند. همان‌طور که ربات‌ها به ادغام در جامعه ادامه می‌دهند، درک نحوه تعامل و واکنش مردم با ربات‌هایی که تصمیم می‌گیرند و به‌عنوان یک مقام مسئول ظاهر می‌شوند (برای مثال در محیط‌های نظامی یا پزشکی)، مهم خواهد بود. از آنجایی که پژوهش‌ها (مانند آزمایش‌های میلگرام و زندان استنفورد) نشان می‌دهد که چگونه مردم عادی می‌توانند از انجام اعمالی که با اخلاقشان در تضاد است اطاعت کنند [۴۲]، خطری واقعی در این حوزه وجود دارد که باید در مطالعات تعامل انسان - ربات مورد توجه قرار گیرد.

## ۴ نتیجه‌گیری

ربات‌ها نه تنها جزء لاینفک زندگی صنعتی هستند، بلکه وارد زندگی روزمره انسان می‌شوند. به‌خصوص ربات‌های اجتماعی که به‌طور یکپارچه‌تری در سبک زندگی روزمره ادغام می‌شوند. با گسترش نفوذ ربات‌ها، سؤالات مهمی در مورد ابعاد شناختی و هیجانی تعامل این موجودات مصنوعی و انسان شکل گرفته است.

این پژوهش مروری کوتاه بر چالش‌های پیش‌رو در حوزه ارتباط بین انسان و ربات در ابعاد هیجانی و شناختی کرده است. هیجان‌ها و شناخت‌ها، نقش کلیدی را در رفتار فرد در بافت اجتماعی بازی می‌کنند. در واقع، برای اطمینان از تعامل انسان-ربات ایمن، پذیرش ابعاد هیجانی-شناختی انسان در این رابطه، ضروری است. در حوزه ابعاد شناختی، انسان‌پنداری و اعتماد مورد بررسی قرار گرفت. انسان‌پنداری به معنای نسبت دادن صفات و رفتار انسانی به ربات، اثراتی مانند تسهیل تبادل اجتماعی و افزایش آشنایی و ارتقای تعاملات اجتماعی داشته است، اگرچه وابستگی را تسهیل می‌کند و احتمال سوءاستفاده را هم بالا می‌برد. اعتماد نیز موجب وابستگی و فریب احتمالی در این رابطه می‌شود. در حوزه ابعاد هیجانی ترس و اضطراب، عشق و دلبستگی، هدایت و اطاعت از مهم‌ترین مسائل ارتباط بین انسان و ربات هستند. با اینکه ابعاد هیجانی بسیار متأثر از ویژگی‌های شخصیتی افراد است، با این حال پژوهش‌ها نشان داده است که ربات هرچقدر شباهت بیشتری به انسان داشته باشد، می‌تواند ترس بیشتری در انسان ایجاد کند. همچنین تعامل شخصی‌تر با ربات‌ها، موجب دلبستگی و عشق در انسان می‌شود که چالش‌های اخلاقی در این زمینه به همراه دارد. این نگرانی‌ها در مورد ربات‌های مراقب و در تعامل با گروه‌هایی که آسیب‌پذیری بیشتری دارند، مثلاً کودکان و سالمندان، جدی‌تر است. نزدیکی در تعامل موجب احتمال دستکاری انسان توسط ربات و اقتدار فزاینده هوش مصنوعی خواهد شد. به طوری که انسان برای گرفتن تایید از ربات یا ترس از انجام ندادن کاری که ربات از او درخواست می‌کند، اقدام به انجام خواسته‌های ربات می‌کنند. ربات‌ها را می‌توان به عنوان عواملی برای دستکاری، تقویت و تحریک حالات عاطفی مختلف و پیچیده در نظر گرفت. این مسئله اهمیت مطالعه بیشتر در مورد اینکه چگونه ربات‌ها می‌توانند بر مردم اقتدار داشته باشند و تا چه اندازه مردم از ربات‌ها اطاعت خواهند کرد را بیشتر می‌کند. در واقع، فرآیندهای هیجانی و شناختی با برداشت اولیه (یعنی ظاهر) از یک محصول شروع می‌شود و با تجارب استفاده، ادامه می‌یابد و با دلبستگی عاطفی به آن و اطاعت، به اوج می‌رسد. به نظر می‌رسد، آنچه که می‌تواند پیونددهنده برخی مفاهیم ذکر شده در ارتباط بین انسان و ربات باشد، مفهوم عاملیت است. عاملیت به عنوان یک مفهوم فلسفی که به کنش اراده‌مند و آزادانه فرد تاکید دارد، بر شناخت‌ها و هیجان‌ها انسان اثرگذار است. ارتباط بین انسان و ربات با تأکید بر عاملیت می‌تواند باب‌های دیگری را از رابطه انسان و ربات بر پژوهشگران بگشاید.

در نظر گرفتن ابعاد شناختی-هیجانی انسان‌ها در تعامل با ربات، در طراحی ظاهر و رفتار یک ربات برای ایجاد تعاملات بهتر، باید مهم باشد. مردم به تعاملاتی نیاز دارند که منجر به تجربیات کاربری مؤثر شود و درک مؤثر شناخت‌ها و هیجان‌های افراد در طول تعامل، می‌تواند به ساخت ربات‌های بهتر کمک کند. لذا طراحان، سیاست‌گذاران و کاربران باید به دقت به نقش این ابعاد، فکر کنند. این پژوهش، خواستار تلاش‌های میان‌رشته‌ای برای درک مرزهای استفاده و توسعه فناوری‌های ربات و هوش مصنوعی است. پژوهش‌ها در حوزه تجزیه و تحلیل تأثیرات ربات‌ها، در مطالعات تعامل انسان-ربات، محدود است. طراحان لازم است هم جنبه‌های فنی و هم ملاحظات قانونی، اخلاقی و روان‌شناختی را برای ترویج استفاده مسئولانه و توسعه ربات‌ها نظر بگیرند.

در پایان باید اشاره کرد که چالش‌های ارتباطی که ربات‌ها در حوزه‌ی شناختی و هیجانی برای انسان می‌آفرینند، تنها به این مسائل محدود نمی‌شود. با افزایش استفاده و کاربرد ربات‌ها در زندگی روزمره انسان،

به‌عنوان دستیار کمکی در مشاغل و منازل و همچنین در بعضی موارد به‌عنوان ابژه‌ای که انسان می‌تواند با آن ارتباط عاطفی برقرار کند، سؤال اصلی اینجاست که آیا حضور ربات در زندگی بشر می‌تواند ماهیت برخی از هیجانات و شناخت‌های انسان را دچار تحولی اساسی‌تر بکند؟ انسان در قرن اخیر در مواجهه با ربات‌ها به سطح جدیدی از خودآگاهی خواهد رسید؟ این پرسش و پرسش‌هایی از این دست نیازمند مطالعاتی عمیق‌تر در آینده با بررسی همه‌جانبه ابعاد شناختی و هیجانی و بررسی ابعاد رفتاری و چالش‌های اخلاقی پیش روست. این مباحث می‌تواند توجه پژوهشگران را در حوزه‌های بین‌رشته‌ای مانند فلسفه اخلاق، روان‌شناسی، جامعه‌شناسی، علوم کامپیوتر و علوم اعصاب به خود جلب کند.

## مراجع

- [1] Ayanoğlu H, Sequeira J. Human-Robot Interaction. Human-Computer Interaction Series. 2019, 39-55.
- [2] Dautenhahn K. Socially intelligent robots: dimensions of human-robot interaction. *Philosophical Transactions of the Royal Society B: Biological Sciences*. 2007;362(1480):679-704.
- [3] Feil-Seifer D, Matarić M. Human Robot Interaction. *Encyclopedia of Complexity and Systems Science*. 2009;:4643-4659.
- [4] Giambattista A, Teixeira L, Ayanoğlu H, Saraiva M, Duarte E. Expression of Emotions by a Service Robot: A Pilot Study. *Design, User Experience, and Usability: Technological Contexts*. 2016;:328-336.
- [5] Ayanoğlu H, Duarte E. *Emotional Design in Human-Robot Interaction*. Cham: Springer; 2019.
- [6] Pessoa L. Cognition and emotion. *Scholarpedia*. 2009;4(1):4567.
- [7] Pessoa L. On the relationship between emotion and cognition. *Nature Reviews Neuroscience*. 2008;9(2):148-158.
- [8] Gates B. A Robot in Every Home. *Scientific American* sp. 2008;18(1):4-11.
- [9] Barco Martelo A. Social Robots to enhance therapy and interaction for children: From the design to the implementation "in the wild" [Internet]. *Hdl.handle.net*. 2022 [cited 4 September 2022]. Available from: <http://hdl.handle.net/10803/399675>
- [10] Złotowski J, Proudfoot D, Yogeewaran K, Bartneck C. Anthropomorphism: Opportunities and Challenges in Human-Robot Interaction. *International Journal of Social Robotics*. 2014;7(3):347-360.
- [11] Caporael L. R. & Heyes C. M. "Why Anthropomorphize? Folk Psychology and Other Stories." In: R. Mitchell, N. S. Thompson, & H. L. Miles (Eds.), *Anthropomorphism, Anecdotes, and Animals*. New York: Suny Press. 1997; 59-73.
- [12] Złotowski J, Proudfoot D, Yogeewaran K, Bartneck C. Anthropomorphism: Opportunities and Challenges in Human-Robot Interaction. *International Journal of Social Robotics*. 2014;7(3):347-360.

- [13] Byron Reeves and Clifford Nass. The media equation: how people treat computers, television, and new media like real people and places. Cambridge University Press, New York, NY, USA, 1996.
- [14] Robins B, Dautenhahn K, Boekhorst R, Billard A. Robotic assistants in therapy and education of children with autism: can a small humanoid robot help encourage social interaction skills?. *Universal Access in the Information Society*. 2005;4(2):105-120.
- [15] Scassellati B. Quantitative metrics of social response for autism diagnosis. ROMAN 2005 IEEE International Workshop on Robot and Human Interactive Communication, 2005.
- [16] Robert L, You S. Subgroup Formation in Teams Working with Robots. *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*. 2015.
- [17] Giger J, Piçarra N, Alves-Oliveira P, Oliveira R, Arriaga P. Humanization of robots: Is it really such a good idea?. *Human Behavior and Emerging Technologies*. 2019;1(2):111-123.
- [18] Sharkey A, Sharkey N. Granny and the robots: ethical issues in robot care for the elderly. *Ethics and Information Technology*. 2010;14(1):27-40.
- [19] Samuel J. Company from the Uncanny Valley: A Psychological Perspective on Social Robots, Anthropomorphism and the Introduction of Robots to Society. *ETHICS IN PROGRESS*. 2019;10(2):8-26.
- [20] Lewis M, Sycara K, Walker P. The role of trust in human-robot interaction. In *Foundations of trusted autonomy 2018* (pp. 135-159). Springer, Cham.
- [21] VandenBos GR. *APA dictionary of psychology*. American Psychological Association; 2007.
- [22] Mayer RC, Davis JH, Schoorman FD. An integrative model of organizational trust. *Academy of management review*. 1995 Jul 1;20(3):709-34.
- [23] Malle BF, Scheutz M, Austerweil JL. Networks of social and moral norms in human and robot agents. In *A world with robots 2017* (pp. 3-17). Springer, Cham.
- [24] Robinette P, Li W, Allen R, Howard AM, Wagner AR. Overtrust of robots in emergency evacuation scenarios. In *2016 11th ACM/IEEE international conference on human-robot interaction (HRI) 2016 Mar 7* (pp. 101-108). IEEE.
- [25] Onnasch L, Wickens CD, Li H, Manzey D. Human performance consequences of stages and levels of automation: An integrated meta-analysis. *Human factors*. 2014 May;56(3):476-88.
- [26] Grodzinsky FS, Miller KW, Wolf MJ. Developing automated deceptions and the impact on trust. *Philosophy & Technology*. 2015 Mar;28(1):91-105.
- [27] Nomura T, Kanda T, Suzuki T. Experimental investigation into influence of negative attitudes toward robots on human-robot interaction. *AI & SOCIETY*. 2005;20(2):138-150.
- [28] Mori M, MacDorman K, Kageki N. The Uncanny Valley [From the Field]. *IEEE Robotics & Automation Magazine*. 2012;19(2):98-100.

- [29] de Graaf M, Ben Allouch S. The relation between people's attitude and anxiety towards robots in human-robot interaction. 2013 IEEE RO-MAN. 2013.
- [30] HARING K, MOUGENOT C, ONO F, WATANABE K. Cultural Differences in Perception and Attitude towards Robots. *International Journal of Affective Engineering*. 2014;13(3):149-157.
- [31] MacDorman K, Vasudevan S, Ho C. Does Japan really have robot mania? Comparing attitudes by implicit and explicit measures. *AI & SOCIETY*. 2008;23(4):485-510.
- [32] Kuchenbrandt D, Eyssel F. The mental simulation of a human-robot interaction: Positive effects on attitudes and anxiety toward robots. 2012 IEEE RO-MAN: The 21st IEEE International Symposium on Robot and Human Interactive Communication. 2012.
- [33] Levy D. Love and sex with robots. 2009.
- [34] Agassi J, Wiezenbaum J. Computer Power and Human Reason: From Judgment to Calculation. *Technology and Culture*. 1976;17(4):813.
- [35] Weber-Guskar E. How to feel about emotionalized artificial intelligence? When robot pets, holograms, and chatbots become affective partners. *Ethics and Information Technology*. 2021;23(4):601-610.
- [36] Seibt J, Nørskov M, Schack Andersen S. *What Social Robots Can and Should Do*. Amsterdam: IOS Press; 2016.
- [37] sharkey N, Sharkey A. The crying shame of robot nannies. *Interaction Studies*. 2010;11(2):161-190.
- [38] Norman D. *Why we love (or hate) everyday things*. New York: Perseus Books Group; 2004.
- [39] Rabb N, Law T, Chita-Tegmark M, Scheutz M. An Attachment Framework for Human-Robot Interaction. *International Journal of Social Robotics*. 2021;14(2):539-559.
- [40] Horstmann A, Bock N, Linhuber E, Szczuka J, Straßmann C, Krämer N. Do a robot's social skills and its objection discourage interactants from switching the robot off?. *PLOS ONE*. 2018;13(7):e0201581.
- [41] Denise Geiskkovitch, Stela H. Seo, James E. Young. "Autonomy, Embodiment, and Obedience to Robots," In the adjunct proceedings of the 10th ACM/IEEE international conference on Human-Robot Interaction, HRI'2015, HRI Pioneers Workshop, Portland, Oregon, USA.
- [42] Milgram, S. Behavioral Study of Obedience. *J Abnormal Psychology*. 1963; 67 (4): 371-378.





## بنیاد و چارچوب دانش سایبری اسلام

ابوالفضل امامی میبدی<sup>۱</sup>، مجتبی شیخی ده‌آبادی<sup>۲</sup>

دانش آموخته‌ی حوزه و دکترای فقه سیاسی و روابط بین‌الملل (کاشف ابرفقه)  
abolfazlemami@chmail.ir

دانش آموخته‌ی حوزه و دکترای علوم اقتصادی (پژوهشگر ابرفقه و نظام اقتصاد)  
msheikhy97@chmail.ir

### چکیده

جهان کنونی سامانه‌ای پیچیده است و برای زندگی و برازندگی، باید بتوان به سامانه‌ی پیشرفته‌ی تراز رسید. این نوشتار در پی نشان‌دادن بنیاد و چارچوب دانش سایبری پیشرفته‌ی اسلام (ابرفقه) با روش فقهی است که با پیوند دو دستگاه خوانشگر (استنطاق) اجمالی و تفصیلی، به کشف سامانه تراز و پیشرفته‌ی اسلام می‌پردازد. هسته‌ی بنیادین سامانه‌ی پیشرفته‌ی اسلام، پنج لایه‌ی «عقل، فکر، قلب، حس و عضو» دارد و پیوند میان آنها، امام - مأمومی است. این سامانه، هم در درون و هم در پیوند با دیگر سامانه‌ها، ساختار «برخال»ی دارد. ابرفقه، هندسه سامانه و ساماندهی جهان را شناخت‌پذیر و پیشرفته می‌کند. از آنجا که دانش سایبری، نرم‌افزار ساماندهی سامانه‌ها از راه دستیابی به نقشه‌ی کارکرد و یا شناخت ساخت و بافت سامانه‌ها است، بسته به شرایط سامانه‌ها، گرانی‌گاه عناصر کارا در مهار و فرمانروایی نیز دگرگون می‌شود. با کمک دستگاه پیشرفته‌ی سایبری اسلام، دستگاه سایبری دیگران را کاوش کرده، به پیش‌بینی رخدادها می‌رسیم و از چنبره‌ی شناخت پسینی پدیده‌ها رها می‌شویم. تولید دانش همراه با کشف گستره‌های تازه و ساخت واژگان تازه است و در این نوشتار نیز به تناسب کشف یک گستره‌ی دانشی، ناگزیر به واژه‌سازی هستیم.

**کلمات کلیدی:** سامانه‌ی اسلام، دانش سایبری، ابرفقه، فضای سایبر، سامانه‌ی پیشرفته، گلوبالیزم، نرم‌افزار حکمرانی.

## ۱ مقدمه

برای روشن شدن جایگاه و گستره نوشته، باید دانست که یک مجموعه، یا آشفته است یا شفته و چفت شده و مجموعه در هم چفت شده یا تنها، نظم دارد و یا افزون بر آن، نظام نیز دارد. نظام نیز، اجمالاً یا پیش‌نظام است یا نظام پیشرفته. پیش‌نظام چیزی است که ارکان تعیین‌کننده نظام، پیوند و دادوستد درستی دارند، اما همه بخش‌های نظام، کارکرد درستی ندارند. ولی نظام پیشرفته، سامانه‌ای است که همه بخش‌های اصلی آن کارکرد بهینه دارند.

## ۱.۱ معنای دانش سایبری

ریشه «سایبرنتیک» یعنی ملوانی کشتی و حکمرانی با سامانه اطلاعات و ارتباطات<sup>۱</sup>؛ اما دانش سایبری پیشرفته؛ (شناخت «پیشرفته» از سامانه جهان و ساماندهی آن)<sup>۲</sup> چیست و روش شناخت آن کدام است؟

## ۲.۱ چرایی کاوش دانش سایبری پیشرفته اسلام

ما در جهانی زندگی می‌کنیم که در هر دم و از هر سو، با متغیرهای بشری بریده از وحی روبرو هستیم. وقتی حذف یک عنصر (مانند گرگ) از سامانه زیست یک میشه، می‌تواند زیست بوم آنجا را بهم بریزد، چرا ساماندهی سایبری جهان کنونی را تراز بدانیم؟ آیا راهی جز کشف سامانه تراز، برای «سالم‌سازی» جهان داریم؟

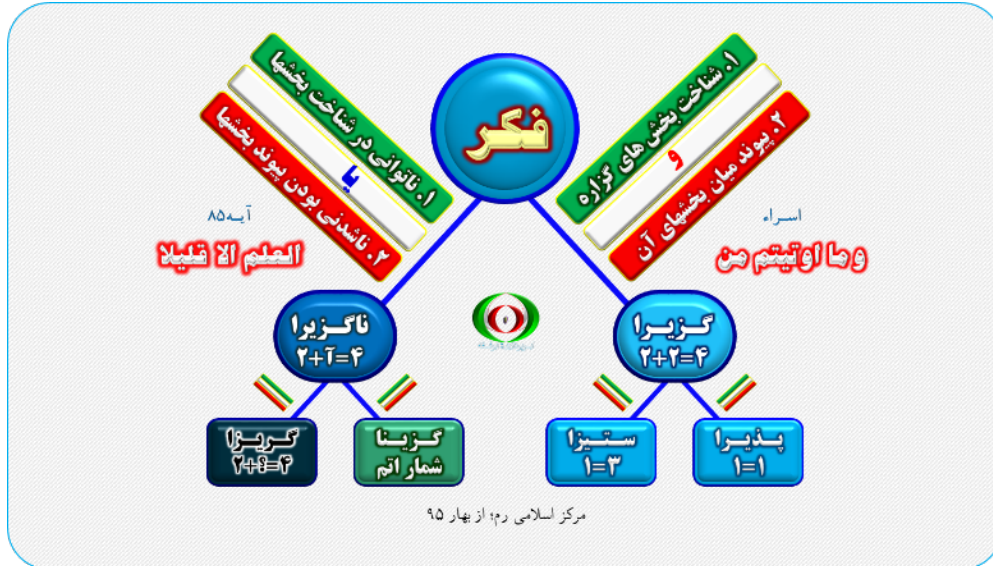
## ۳.۱ نوآوری‌های دانش سایبری پیشرفته اسلام (ابرفقه)

دانش سایبری پیشرفته با شناخت لایه‌های سامانه انسان و جامعه و جهان و پیوند درست میان آنها دارای یک الگوی ریاضی و برخالی بسیار پیشرفته است که از سویی جلوی بی‌نظمی و بی‌نظمی یا کاستی‌های پیش‌نظام ما را می‌گیرد و آرمان‌های آفرینش را با شتاب فزاینده‌ای دست‌یافتنی می‌کند و از سوی دیگر، همانند یک دستگاه خوانشگر، سامانه سایبری دیگران را حتی از زیر پوشش پدافند غیر عامل (نهفتگی، پراکنش و فریب) بیرون می‌کشد. کشف انجام شده، میوه دو دهه تلاش فقهی است که ساختار سامانه، ساختار دانش و ساختار ساماندهی را دگرگون یا پیشرفته می‌کند و از دانش فیزیک گرفته تا علوم شناختی و انسان‌شناسی و ... را در بر می‌گیرد.<sup>۳</sup>

بررسی‌های ما نشان می‌دهد که کشف یک سامانه سایبری پیشرفته در فقه اسلام تا کنون انجام نشده است و برخی کارهای غیر فقهی یا شبه فقهی انجام شده، نمی‌تواند مبنا و الهام بخش کار فقهی باشد از این رو در این مجال اندک به آنها نمی‌پردازیم. در ادامه به روش‌شناسی دانش سایبری پیشرفته اسلام، تنگناهای آن و سپس ابرفقه (دانش سایبری پیشرفته اسلام) و نتیجه‌گیری می‌پردازیم.

<sup>۱</sup> «سایبرنتیک» از ریشه یونانی «κυβερνήτης» به معنای تحت‌اللفظی ملوان کشتی‌ها است و به گونه فراگیر، به معنای رهبری شهر یا کشور است. (بنگرید: [۱])؛ یا از ریشه یونانی «κυβερνητική» به معنای هنر فرمانروایی (بنگرید: [۲]) است. این معنا، در هر زمانی، با برخی عناصر برجسته ویژه همراه است. در تعریف ویستر - میریام، سایبرنتیک یعنی دانش نظریه ارتباطات و مهارت که به گونه ویژه به بررسی تطبیقی سامانه‌های مهار خودکار؛ مانند سامانه عصبی و سامانه‌های ارتباطی مغز و مکانیکی - الکتریکی می‌پردازد. (بنگرید: [۳]) به گمان ما واژه «کی» در یونانی، «سای» در انگلیسی و «چی» در ایتالیایی، که هسته واژه «سایبرنتیک» است، هم‌ریشه واژه «سای» در فارسی (از مصدر سافتن) است که «سام»، زاده دیگر سافتن است (سام+ان). تبیین این نظریه در: [۴].

<sup>۲</sup> نرم‌افزار حکمرانی در سخن رهبر: «نظام اسلامی که تشکیل شد، آرمانهایی را مطرح کرد که خود این آرمانها هم مربوط به اسلام بود و از قرآن گرفته شده بود ... بنابراین راه [رسیدن به] آن [آرمانها] هم در کتاب و سنت هست ... این، یک نرم‌افزار است برای سخت‌افزار حکومت اسلامی. حکومت اسلامی را به عنوان سخت‌افزار در نظر بگیرید، اگر نرم‌افزار مناسب خودش را نداشته باشد، به هیچ کار نمی‌خورد. نرم‌افزارش همین است که راه‌های رسیدن به آن آرمانها مشخص شود ... [نظام] احتیاج دارد که آن نرم‌افزار را، آن مجموعه معنوی را نوبه‌نو تجدید حیات کند و به‌روز کند ... این، آن چیزی است که از فضای صاحب‌نظر و متفکر جدا باید مطالبه بشود و این کار باید انجام بگیرد. ... یک حقایقی در کتاب و سنت هست که ما تا وقتی احتیاج به آنها پیدا نکنیم، متوجه به آنها نیستیم، متنبه نیستیم؛ وقتی احتیاج پیدا کردیم، تنبه پیدا می‌کنیم» [۵]، بیانات در تاریخ ۴ اسفند ۱۳۹۹.  
<sup>۳</sup> بنگرید: [۶]؛ [۷]؛ [۸]؛ [۹] و نیز [۱۰]، تاریخ نوشته: ۲۳ فروردین ۱۳۹۱.



نمودار ۱: خوانشگر بیضا؛ بیخت نسبت گزاره‌ها با فکر

## ۲ روش‌شناسی دانش سایبری پیشرفته اسلام

برای کاوش دانش سایبری پیشرفته اسلام، دو روش فکری و فقهی را بررسی می‌کنیم:

### ۱.۲ ناتوانی روش فکری

ذهن ما نمی‌تواند در هر چیزی داوری کند و تنها در برابر آن گزاره‌هایی چاره‌ساز و «گزیرا» است که بتواند: آ. همه بخش‌های گزاره را بشناسد و؛ ب. همه پیوندهای میان این بخش‌ها را نیز سامان بدهد. در اینجا اگر گزاره را درست یافت، آن را «پذیرا» می‌نامیم ( $2+2=4$ ) و اگر آن را نادرست یافت، «ستیزا» می‌نامیم ( $1=3$ ). ولی در آنچه که برای ذهن ما «ناگزیرا» است؛ یا آن گزاره پاسخی دارد و باید از داننده آن بگزینیم؛ که آن را «گزینا» می‌نامیم؛ مانند شمار اتم‌های زمین و یا آن گزاره پاسخی ندارد؛ که آن را «گزیزا» می‌نامیم؛ مانند «شمار شماره‌ها» یا « $2+?=4$ » که گزاره‌هایی متناقضند؛ مثلاً شما هم باید بدانید که «؟» چه عددی است و هم برای این که «؟»، پرسش باشد، باید آن را ندانید.

از آنجا که ما جز به شناخت اندکی، دسترسی نداریم<sup>۴</sup>، بیشتر گزاره‌های زندگی ما «حتی درستی آب نوشیدن» گزینا است<sup>۵</sup>. بنابراین روش‌شناسی درست برای شناخت «سامانه پیشرفته خویش و جهان» و «ساماندهی پیشرفته» نیز تنها می‌تواند شناختی «گزینا» از منابع برتر از ذهن ما باشد.

<sup>۴</sup> «وَمَا أوتِيتُمْ مِنَ الْعِلْمِ إِلَّا قَلِيلًا». اسراء، ۸۵. [۱۱].  
<sup>۵</sup> بنگرید: [۱۲]، تاریخ نوشته: ۳۰ آبان ۱۳۹۶.

## ۲.۲ ناتوانی روش فقهی در تنگنای شناختی و شناسندگی

گاهی خدای دانا برای ما رهنمودی می‌دهد و «پیام» بر آن را به ما می‌رساند. شناخت آن را «فقه الهی» می‌گوییم (أَطِيعُوا اللَّهَ) و گاهی ولی امر برای سامان‌دهی نظام، فرمانی می‌دهد که آن را «فقه ولایی» می‌گوییم (و أَطِيعُوا الرَّسُولَ وَ أُولَى الْأَمْرِ مِنْكُمْ)<sup>۶</sup>. اینک می‌پرسیم که کدام فقه ما را به شناخت «سامانه پیشرفته و ساماندهی پیشرفته می‌رساند؟ برای دستیابی به دانش سایبری پیشرفته، از «فقه الهی»، کمینه دو تنگنای «شناختگی و شناسندگی» داریم:

### ۱.۲.۲ تنگنای شناختگی

گمشده شناختی ما، باید نشانی ویژه‌ای داشته باشد تا بتوان آن را از میان انبوه چیزهای همانند یافت. وقتی شناخت ما از سامانه، در اندازه «گروهی از چیزهای هماهنگ و کارآمد» باشد، برای کشف آن، باید در جستجوی چه آیه یا روایتی باشیم؟ مهندسی را بینگرید که نمی‌داند هندسه‌ی کارش، چندگوش است؟ سه‌گوش، چهارگوش یا بیشتر؟ کدام گونه سه‌گوش؟ کدام گونه چهارگوش؟ دوزنقه، بادبادکی، پیکانی، متوازی‌الاضلاع، مستطیل، لوزی یا مربع؟ و روی کدام سطح؟ اقلیدسی یا خمینه ریمانی یا لباچفسکی؟ وانگهی اساساً سامانه پیشرفته را باید در سطح جست یا حجم یا جرم؟ چه حجمی؟ و چه جرمی؟ در اینجا هزاران مجهول به گمشده ما افزوده می‌شود!

### ۲.۲.۲ تنگنای شناسندگی

وقتی ساختارهای نادرست دوران آموزش، بر ذهن بنشینند، نه تنها «سامانه درست» را نمی‌شناسیم، بلکه توان ما در «شناخت درست» سامانه نیز دچار تنگنا می‌شود! اگر ذهن را یک قالب پنج‌گوش بینگریم که با رسوبات آموزشی، گرد شده است، آنگاه اگر این ذهن، سامانه پنج‌گوشی را بیابد، می‌کوشد آن را برای هماهنگی با ذهن، به گونه «گرد»، بازسازی و تفسیر کند. از این رو، باید کسی را یافت که، هم مسائل پیچیده را بشناسد و هم ساختار ذهن وی آمی باشد!

درهم‌تنیدگی این دو تنگنا، مانند این است که کسی چشمانش کم‌سو باشد و همزمان نداند که لنز چیست و ناگزیر باشد که در میان هزاران چیز کمابیش همانند، لنز را بیابد و بر چشم بگذارد! پس از روشن شدن این تنگناها و دشواری کشف سامانه پیشرفته، باید دانست که اگر بریده از فقه، سامانه و ساماندهی پیشرفته نادرست را سامانه تراز بپنداریم، مانند این است که کارخانه‌ای قالب کجی بر کالاها بزند و همه کالاها کج بشوند. در اینجا تباهی سامان‌وار رخ می‌دهد و فراگیر بودن آن تباهی، سبب نهفتگی یا عادی شدن تباهی می‌شود. به چنین تباهی‌ای، تباهی در «سنجه» (میزان) می‌گوییم<sup>۷</sup>؛ ولی سرکشی در «سنجش»، به فسادهای موردی می‌انجامد.

راه گذر از تنگنای شناخت سامانه و ساماندهی پیشرفته، بهره‌بری از «دستگاه استنتاج اجمالی» از

<sup>۶</sup> «يَا أَيُّهَا الَّذِينَ آمَنُوا أَطِيعُوا اللَّهَ وَأَطِيعُوا الرَّسُولَ وَأُولَى الْأَمْرِ مِنْكُمْ ...» نساء، ۵۹. [۱۱]

<sup>۷</sup> «لَقَدْ أَرْسَلْنَا رُسُلَنَا بِالْبَيِّنَاتِ وَأَنْزَلْنَا مَعَهُمُ الْكِتَابَ وَالْمِيزَانَ لِيَقُومَ النَّاسُ بِالْقِسْطِ ...» حدید، ۲۵. [۱۱]



نمودار ۲. هسته بنیادین ابرفقه؛ لایه‌های سامانه و نسبت میان آنها

سخنان ولیّ امر (فقه ولایی) است که به کشف «دستگاه استنطاق تفصیلی» از فقه الهی و سپس کشف «سامانه تفصیلی پیشرفته انسان و جهان» می‌رسیم.<sup>۸</sup> چنانکه دیدیم، ولیّ امر، حکومت را سخت‌افزاری می‌دانند که اگر نرم‌افزار درخور خود را نداشته باشد، به هیچ کار نمی‌خورد؛ پس کشف نرم‌افزار فرمانروایی (سایبری) برای رسیدن به «نظام پیشرفته»، ارزش حیاتی و تعیین‌کننده دارد. ما به «آن فقهی که ارزش حیاتی» دارد، «ابرفقه» می‌گوییم.

### ۳ ابرفقه؛ دانش سایبری پیشرفته اسلام

برای پی‌بردن به «سامانه» پیشرفته و پیوند میان بخش‌های سامانه، از ابرفقه کمک می‌گیریم. ابرفقه، نشان‌دهنده سامانه تراز انسان، جامعه، جهان و دانش‌ها است که هسته بنیادین آن در فرمایش امیرالمؤمنین (ع) آمده است: «العقولُ أئمةُ الأفكارِ و الأفكارُ أئمةُ القلوبِ و القلوبُ أئمةُ الحواسِّ و الحواسُّ أئمةُ الأعضاء»<sup>۹</sup>؛ عقل‌ها امامان فکرها هستند و فکرها امامان دل‌ها هستند و دل‌ها امامان حواس‌ها هستند و حواس‌ها امامان اعضاها. با «شناخت تصویری» سامانه تراز به کمک روایت، اینک به تبیین فشرده «بدهات تصدیقی» آن می‌پردازیم.

<sup>۸</sup>بنگرید: [۸]، درس ۷ (امکان کشف نظام اسلام از ولایت ولیّ امر): ۵۲ تا ۵۷.  
<sup>۹</sup>[۱۳]، ج ۱، ص ۲۰۰ این روایت به سبب بُنمایه غیرتعبدی و تفهیمی بودن، بر پایه مبنای «وثوق الصدور»ی و نیز تبیین تفهیمی درونی آن و نیز تواتر معنوی استوار است.



### ۱.۳ تبیین فکری سامانه پیشرفته اسلام

آ. آفریدگان جهان، مستعد رشد هستند؛ ب. اینها برای رشد، باید با هستی‌های دیگری، ارتباط بگیرند؛ ج. برای انجام ارتباط، این آفریدگان باید دارای نیرو و انگیزه باشند؛ د. این ارتباطها باید بر پایه یک برنامه باشد؛ ه. رشدآوری این برنامه، در گرو پیگیری جهت‌گیری‌های کلان رشدآور و وحدت‌بخش و هماهنگ‌کننده نظام است؛ تا تراحم و آشوبناکی و گمراهی پیش نیاید.<sup>۱۰</sup>

### ۲.۳ تبیین فقهی سامانه پیشرفته اسلام

امیرالمؤمنین (ع) می‌فرماید که «عقل‌ها امامان فکرها هستند و فکرها امامان قلب‌ها هستند و قلب‌ها امامان حس‌ها هستند و حس‌ها امامان عضوها هستند». پس سامانه پیشرفته اسلام، پنج لایه دارد و میان لایه بالا و پایین، رابطه امام - مأمومی است. بُنمایه و ژرفای حیاتی سامانه، «عقل» نامیده می‌شود که به معنای «بند» است و «عاقل» یعنی «بنده» و «تعقل» یعنی پیوند هر پنج لایه، برای انجام نیکی. این معنای حقیقی عقل، غیر از معنای مجازی «مُدِرک کلیات» و «قوه استدلال» است! این دو معنا، کار «فکر» است؛ نه عقل!<sup>۱۱</sup> عقل، اصول و سوگیری کلان را نشان می‌دهد و فکر از آنها، تفریع کرده، برنامه تفصیلی می‌سازد و آنگاه بر قلب، امامت می‌کند. فرق عقل و فکر، در اندازه فرق امام و مأموم است! گاه عقل کسی خوب است ولی در فکرش دچار استضعاف است! و گاه فکر کسی خوب است ولی عقلش خوبی‌ها را پی نمی‌گیرد. قلب به معنای دگرگونی است و با دگرگونی‌های پیاپی، حب و بغض و انگیزه را برای انجام برنامه فکر، فراهم می‌کند و با امامت بر لایه حس، انگیزه‌ها را به حس می‌رساند. حس به معنای دریافت‌های معنادار از بیرون و رساندن آن به مرکز یا وارونه این فرایند است و «حس» را همان «شبکه ارتباطی و انتقالی» می‌دانیم. حس، امام لایه عضو است و نیروی بهینه را در زمان و جهت درست، به عضو، می‌رساند. عضو یعنی هر فرد یا هر بخشی از سامانه؛ که دارای کارویژه مستقل است. برپایه آنچه گفته شد، «تعقل» یعنی پیوند لایه‌ها، برای انجام کار درست.

### ۳.۳ ارکان کارکرد سامانه پیشرفته اسلام

برای کارکرد پیشرفته سامانه، به پنج رکن نیاز است: آ. رکن «حیاتی» سامانه (العقول)، برای زنده بودن آن؛ ب. رکن «حیات‌بخشی» به لایه‌های زیرین سامانه (أئمة)؛ ج. رکن «حیات‌بخشی در همه لایه‌های سامانه؛ د. رکن «حیات‌سنجی»، برای شناخت توازن رشد و برخورداری درست هر لایه؛ ه. رکن «حیات‌ورزی» برای پیشرفت سامانه. انجام پیشرفته کار و حیات‌ورزی پیشرفته، در گرو دو بخش «برآیند» کاوی و «فرایند» کاوی است.<sup>۱۲</sup> «برآیند» یعنی وضعیت‌های نقطه‌ای، خطی، سطحی، حجمی و جرمی «نیکی» و «بدی» در هر بخش از سامانه، در راستای کشف برخورد درست با آن. پس از برآیندکاوی، به کاوش فرایند رفتن از وضع کنونی به وضع مطلوب می‌پردازیم. مهمترین فرایندها، فرایند «برون - درون» (از لایه عضو به لایه عقل) و فرایند «میان - دوسو» است؛ چنانکه در نمودار ۳ آمده است.

<sup>۱۰</sup>بنگرید: [۸]، درس ۸ (تبیین ساده فکری نظام جمعی و چرخه کار): ۵۹ تا ۶۷.

<sup>۱۱</sup>بنگرید: [۸]، درس ۹ (تبیین ساده نقلی از نظام و چرخه کار جمعی): ۶۸ تا ۸۰.

<sup>۱۲</sup>بنگرید: [۸]، درس ۱۲ (ارکان کارکرد نظام پیشرفته اسلام): ۹۹ تا ۱۰۵.





نمودار ۳. فرایندکامی «میان - دوسو» از سوره قریش: قلب، حس، عقل، عضو و قلب

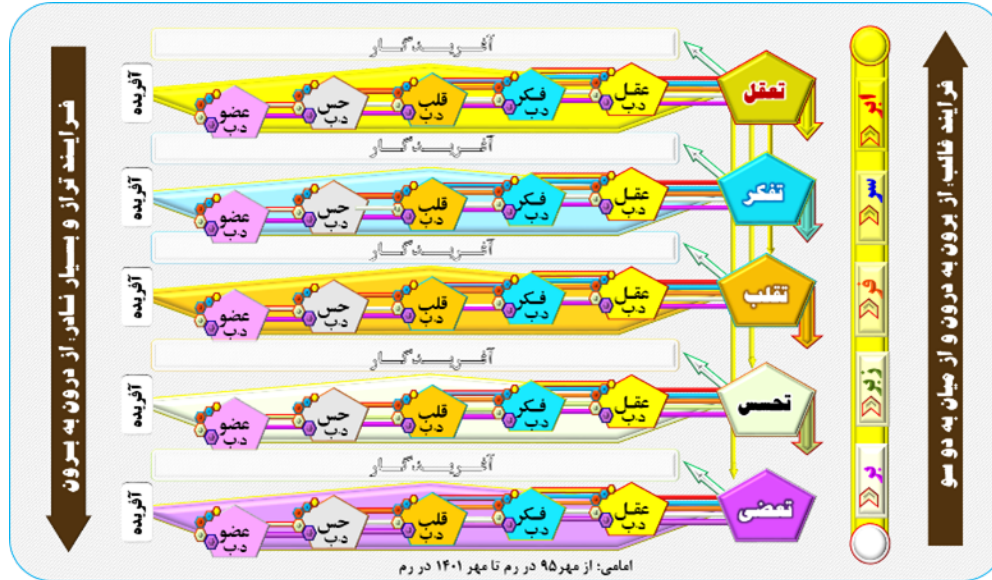
### ۴.۳ نقشه گستره سامانه

برای ساماندهی پیوندهای گوناگون سامانه، باید لایه‌ها، لایه‌ها (زیرلایه) و لایه‌های (زیرلایه) هر سامانه و نسبت میان آنها را شناخت. از این رو نخست باید بخش‌های سامانه پیشرفته را شناخت. سامانه پیشرفته، پنج لایه دارد و هر لایه، پنج لایه دارد و هر لایه پنج لایه (زیرلایه). هر کدام از اینها سه رسته تکوینی، تشریحی و تعقیلی دارند و در دو وضعیت درون و برین (د.ب) سنجیده می‌شوند. هر بخش، پنج رده رشد دارد: «بر، زیر، فر، سر و ابر». اینها با فرایندهای گوناگون (درون - برون، برون - درون و میان - دوسو) ورز می‌یابند که هزاران خانه را در سامانه می‌سازند. افزون بر اینکه سامانه‌ها، وضعیت درونی و برونی «برخال»ی دارند؛ که در اینجا به آن نمی‌پردازیم.

### ۵.۳ لایه حس؛ گرانیگاه فضای سایبری کنونی

بر پایه مشاهدات میدانی، اینک در جنگ سخت (نظامی) توازن قدرت یا توازن وحشت بر قرار است. از این رو هزینه جنگ بسیار بالا است؛ ولی در نبرد نرم، با جنگ‌افزار رسانه، نه توازن قدرت است و نه توازن وحشت! از این رو دشمن در زمینه «ارتباطات» یعنی لایه «حس»، سرمایه‌گذاری بسیاری کرده است. افزون بر این، برپایه «فقه غرب‌شناسی» نیز، کانون تلاش شیطان و استکبار، جنگ رسانه‌ای و جنگ شناختی است؛ تا سوار بر گرده کارگزاران، به چیرگی بر گرده زمین (گلوب) و گلوبالیزم برسند.<sup>۱۳</sup>

<sup>۱۳</sup> با اینکه دشمن در جنگ جهانی نیابتی سخت، در سوریه شکست خورد، در جنگ نرم رسانه‌ای کشورمان را «قتلگاه جوانان و نوجوانان» کرده است. از این رو رهبر فرمود که قوت در فضای مجازی، «حیاتی» است [۵]، بیانات در ۳ فروردین ۱۳۹۹) و فضای مجازی را هم‌اهمیت انقلاب دانستند [۱۴]، تاریخ خبر: ۲۶ اسفند ۱۳۹۰) و فرمود اگر من رهبر نبودم فرمان فضای مجازی را به دست می‌گرفتم [۱۵]، تاریخ خبر: ۴ فروردین ۱۴۰۰) و پس از شکستن «عین الاسد» با موشک خالزن ایرانی، فرمود «سیلی سخت‌تر عبارت است از غلبه نرم‌افزاری بر هیمنه پوچ استکبار» [۵]، بیانات در ۲۶ آذر ۹۹؛ زیرا برپایه فقه غرب‌شناسی، ابلیس در



نمودار ۴. گستره چند هزار خانه‌های ابرفقه

برپایه ابرفقه، انسان و جامعه پنج لایه دارند و جهاد نیز پنج گونه است: جهاد اکبر، جهاد کبیر، جهاد وسط، جهاد صغیر و جهاد اصغر<sup>۱۴</sup>. کارویژه لایه حس، «ارتباطات و انتقالات» است. لایه حس پیشوای لایه عضو و پیرو لایه قلب است. جهاد در لایه «حس» (جهاد صغیر) رده بالاتری از جهاد در لایه عضو (جهاد اصغر) دارد. لایه حس دارای پنج لاژه است: حس عقل، حس فکر، حس قلب، حس حس و حس عضو. هر کدام از این لاژه‌ها نیز پنج لاکه (زیرلاژه) دارند؛ مانند: لایه حس، لاژه حس عقل و لاکه حس عقل در پیوند با عضو. بسته به این که کدام یک از لاژه‌های حس دچار ستم و ستمگیری بشود، آسیب آن می‌تواند «کاری» یا حتی «تعیین‌کننده» باشد و جنگ رسانه‌ای، گاه می‌تواند به نابودی نظام بینجامد. از این رو، با اینکه لایه «عقل»، لایه حیاتی است، ولی لایه حس هم می‌تواند «منجر به حیاتی» باشد؛ چنانکه در شرایط کنونی، نوک پیکان نبرد استکبار است.

پی فرمانروایی بر گرده زمین و دهان کجی به فرمان خدا (أَنْتَى جَاعِلٌ فِي الْأَرْضِ خَلِيفَةً؛ [۱۱]، بقره، ۳۰) بوده است. فرایندی که وی برای رسیدن از گام‌های شیطانی (خطوات الشیطان) به سوی چیرگی بر گرده زمین پیش گرفته است، در آیه ۱۱۸ و ۱۱۹ سوره نساء آمده است و شگفتا که این تراز از سماجت و تأکید لفظی را بنده در هیچ گفتار یا نوشتاری در هیچ جا ندیده‌ام «لَا تَخَذَنَّ مِنَ عِبَادِكِ نَصِيبًا مَّفْرُوضًا وَ لَأَضَلُّنَّهُمْ وَ لَأَمْنِيَّتُهُمْ وَ لَأَمْرُنَّهُمْ فَلْيَتَّبِعْكُمُ أَذَانُ الْأَنْعَامِ وَ لَأَمْرُنَّهُمْ فَلْيَعْبِرُوا بِحَقِّ اللَّهِ». جنگ ابلیس در این نبرد پایانی، جنگ سایبری نرم است که نخبگان و کارگزاران نظام اسلامی را با جنگ‌افزار رسانه و اطلاعات نادرست، مهار کرده، از ولی امرشان «گمراه» می‌کند (لَأضَلُّنَّهُمْ) در گام دوم، آنان را پندارین و آرزوزده (لَأَمْنِيَّتُهُمْ) می‌کند. انسان آرزو زده برای رسیدن به پندارهایش «دستورپذیر و پروتکلی» می‌شود: «لَأَمْرُنَّهُمْ» و دستور نهایی نیز «فَلْيَعْبِرُوا بِحَقِّ اللَّهِ» است. اگر شیاطین بتوانند با تغییر در شیوه آفرینش (خلق) الهی و حلال، به شیوه آفرینش شیطانی و حرام برسند، حرامزادگی روال می‌شود و حرامزادگان یا ولایت حق را می‌ستیزند و یا توانش ولایت‌پذیری آنان اندک است و بدین‌سان، در جهان حلال‌آفریده، جهانی حرامزاده و بستر فرمانروایی پایدار و فراگیر ابلیس فراهم می‌شود و گلوب (globe) یعنی گرده زمین، به ولایت و عبادت ابلیس گردن می‌نهند: گلوبالیزم! می‌بینیم که نبرد سایبری پیشاپه‌هور برپایه آیات روشن قرآن، تا اندازه بسیاری رسانه‌ای و «شناختی» است! بنگرید: [۱۶].  
<sup>۱۴</sup> بنگرید: [۱۷]، ص ۱۵۱ تا ۱۷۲.

## ۴ نتیجه‌گیری

دانش سایبر همواره در زندگی «انسان» بوده، همزاد آفرینش «آدم» و مدیریت بر سامانه است؛ ولی شناخت پیشرفته آن از توان فکری بشر بالاتر است. دو دهه تفقه ژرف با ترکیب خوانشگر اجمالی از فقه ولایی و خوانشگر تفصیلی از فقه الهی، نشان می‌دهد که سامانه تراز انسان و جهان بر پایه فرمایش امیرالمؤمنین، دارای پنج لایه عقل، فکر، قلب، حس و عضو است که هر لایه‌ای امام لایه زیرین است. این همان نرم‌افزار پیشرفته ساماندهی است که مرزهای دانش و پیشرفته را بیش از ۱۰۰٪ جابجا می‌کند و اگر نباشد، سخت افزار حکومت، هیچ کاری در تراز سامانه پیشرفته انجام نخواهد داد. از آنجا که در دانش سایبری مسلمانان، لایه «حس» که کانون ارتباطات و انتقالات است، بسان رکن چهارم سایبری بازشناسی نشده بود، اینک ما در ساماندهی جهان، دچار آسیب بسیاری از سوی کسانی هستیم که در رکن چهارم سامانه و فضای سایبری، نیرومند هستند. شاهکار دانش سایبری اسلام این است که می‌تواند دستگاه سایبری دشمن را استنطاق کرده، آن را از پدافند غیرعامل بیرون کشیده، ما را به شناخت پیشینی از رخدادها و پیروزی در برابر نظام سایبری شتابان و پیچیده گلوبالی برساند!

## مراجع

- [۱] امامی میبدی، ابوالفضل، زیرتفقه نظام پیشرفته دین، در دست ویرایش برای چاپ.
- [۲] بیانات رهبری، پایگاه دفتر حفظ و نشر آثار رهبری، <https://farsi.khamenei.ir/speech>، بازدید: ۲۲/۷/۱۴۰۱.
- [۳] امامی میبدی، ابوالفضل، تفکر اسلامی یا تفلسف ائلامی، طبس: فراونگ، اول، ۱۳۹۸.
- [۴] امامی میبدی، ابوالفضل، زیرپردازی فقه استراتژیک، طبس: فراونگ، اول، ۱۳۹۷.
- [۵] امامی میبدی، ابوالفضل، زیرتفقه نظام اسلام، میبد: انتشارات میبد، اول، ۱۴۰۰.
- [۶] امامی میبدی، ابوالفضل، معرفت دینی یا دین معرفتی، طبس: فراونگ، اول، ۱۳۹۸.
- [۷] انقلاب اسلامی در تولید علم، با طراحی ابرطبیعیات، پایگاه رجانوز، <http://rajanews.com/node/105567>، بازدید: ۲۲/۷/۱۴۰۱.
- [۸] قرآن کریم.
- [۹] گفتگوی روحانی شیعه با دانشجوی دکتری اخترفیزیک و پزشک ایتالیایی، ابرنگار، <http://abarnegar.ir/?p=1188>، بازدید: ۲۲/۷/۱۴۰۱.
- [۱۰] کراجکی، محمد بن علی، کنز الفوائد، قم: دار الذخائر، اول، ۱۴۱۰ ق.
- [۱۱] این فضا به اندازه انقلاب اسلامی اهمیت دارد، پایگاه دفتر حفظ و نشر آثار، <https://khl.ink/f/19272>، بازدید: ۲۲/۷/۱۴۰۱.
- [۱۲] تاکیدات مهم رهبری درباره مدیریت فضای مجازی چیست؟ خبرگزاری مهر. [mehrnews.com/xTZ7z](http://mehrnews.com/xTZ7z)، بازدید: ۲۲/۷/۱۴۰۱.
- [۱۳] امامی میبدی، ابوالفضل و ترکیان، هانیه، غرب شناسی فقهی با تمرکز بر گلوبالیسم، در دست ویرایش برای چاپ.
- [۱۴] امامی میبدی، ابوالفضل، فقه سیاست خارجی و نظام‌سازی آن، میبد: انتشارات میبد، اول، ۱۳۹۹.

- [15] CYBER, Accademi Adella Crusca, <https://accademiadellacrusca.it/it/consulenza/cyber/1417>, Visited: 14 October 2022.
- [16] CIBERNETICA, treccani dictionary, <https://www.treccani.it/vocabolario/cibernetica>, Visited: 14 October 2022.
- [17] Cybernetics, merriam-webster dictionary, <https://www.merriam-webster.com/dictionary/cybernetics>, Visited: 14 October 2022.

## نفرت‌پراکنی در وب تاریک از منظر نظام بین‌المللی حقوق بشر

یاسمن صفایی<sup>۱</sup>

دانشجوی کارشناسی ارشد حقوق بین‌الملل، دانشکده حقوق، دانشگاه قم، قم، ایران  
safaie6819@gmail.com

### چکیده

وب تاریک به عنوان بخشی از اینترنت تنها از طریق فناوری‌های ناشناس‌کننده مانند تور قابل دسترسی می‌باشد. ناشناس بودن، امکانی که فناوری‌های مذکور به افراد اعطا می‌کنند، زمینه‌ای برای سوء استفاده از این فضا و نقض حقوق بشر را فراهم می‌کند. یکی از این حقوق اساسی، ممنوعیت نفرت‌پراکنی و آزادی از تحریک نفرت نژادی، مذهبی یا ملی بوده که در اسناد بین‌المللی حقوق بشر از جمله ماده ۲۰ میثاق بین‌المللی حقوق مدنی و سیاسی بر آن تأکید شده است. این حق توسط گروه‌های تندرو از جمله داعش، القاعده، نئونازی‌ها و مانند آن‌ها و همچنین افراد در این فضا مورد تجاوز قرار گرفته است. ناشناس ماندن در این فضا به گروه‌های مذکور فرصت می‌دهد تا با برقراری ارتباط ناشناس، تبلیغ ایدئولوژی‌ها و افکار، سرپازگیری و پخش اخبار غلط به تحریک افراد به خشونت و نفرت پردازند. برخی افراد نیز با استفاده از ویژگی بارز این فضا به نفرت‌پراکنی علیه افراد دیگر با نژاد، ملیت و مذهب متفاوت می‌پردازند. در چنین شرایطی، تعهد دولت‌ها به حمایت در نظام بین‌المللی حقوق بشر ایجاب می‌کند که از حقوق افراد در برابر آسیب اشخاص ثالث محافظت کنند. در این راستا، دولت‌ها موظف‌اند که با استفاده از ابزار و شیوه‌های مختلف به مقابله با فعالیت‌های این گروه‌ها و افراد در وب تاریک پردازند.

**کلمات کلیدی:** وب تاریک، نظام بین‌المللی حقوق بشر، نفرت‌پراکنی، تعهد به حمایت.

### ۱ مقدمه

در سال ۲۰۱۱ با تصویب قطعنامه دفاع از آزادی اینترنت در شورای حقوق بشر سازمان ملل، دسترسی به اینترنت یکی از حقوق اساسی بشر اعلام شد. اینترنت فقط به آن بخش که مورد استفاده روزمره افراد است، محدود نشده و از لایه‌های مختلفی تشکیل شده است. وب تاریک، یکی از این لایه‌ها تنها از طریق فناوری‌های ناشناس‌کننده مانند تور قابل دسترسی می‌باشد. وجه تمایز وب تاریک از سایر بخش‌های اینترنت، ناشناسی و غیرقابل ردیابی بودن افراد در این فضا است. این ویژگی محیط ایده‌آلی برای افراد و گروه‌های تروریستی فراهم می‌کند؛ چراکه آن‌ها همیشه به دنبال برنامه و پلتفرم‌های جدیدتر و بهتر به منظور حفظ حضور آنلاین خود در حداکثر تعداد رسانه ممکن هستند. آن‌ها در چنین محیطی به فعالیت‌های خود از جمله جنگ روانی،



تبلیغات و فریب افکار عمومی، ترویج ایدئولوژی و عقاید خود، سر بازگیری، تأمین حمایت مالی پرداخته و فارغ از ترس شناسایی و دستگیر شدن به نفرت پراکنی می‌پردازند. از طرفی این نوع اعمال یعنی تبلیغ برای جنگ و یا حمایت از نفرت ملی، نژادی یا مذهبی که تحریک به تبعیض، خصومت یا خشونت کند، براساس ماده ۲۰ میثاق بین‌المللی حقوق مدنی و سیاسی ممنوع شده است. از طرفی دیگر، آزادی بیان مندرج در ماده ۱۹ این میثاق نیز به منظور احترام به حقوق و شهرت دیگران و حفاظت از امنیت ملی، نظم عمومی، سلامت عمومی و اخلاق محدود شده و در نتیجه حقی مطلق نخواهد بود. مطابق نظام بین‌المللی حقوق بشر، دولت‌ها در مواجهه با چنین وضعیتی متعهدند از افراد و گروه‌های در معرض آسیب حفاظت کنند. در عین حال دولت‌ها در ایفای این تعهد نمی‌توانند دسترسی به این فضا را به طور کلی قطع کرده و یا به طور دلخواه بر سر راه این دسترسی، مانع ایجاد کنند. علت این امر در بعد دیگر این فضا قابل جستجو است. ناشناس ماندن در این فضا نه تنها انشعابی از حق بر حریم خصوصی است بلکه زمینه‌ای برای تحقق دیگر حقوق بشری نیز فراهم می‌کند که دولت‌ها براساس تعهد به احترام و تحقق حقوق بشر موظف به عدم مداخله در برخورداری از این حقوق و همچنین تسهیل آن می‌باشند. بنابراین حریم خصوصی و سایر حقوق بشر نباید فدای مبارزه دولت‌ها با تروریسم در فضای وب تاریک شود. برای نخستین بار در میان منابع انگلیسی و فارسی، این پژوهش به بررسی نفرت پراکنی در وب تاریک از منظر نظام بین‌المللی حقوق بشر می‌پردازد. برای ارائه این موضوع، در بخش بعدی به مرور مقالات گذشته، در بخش سوم به تعریف وب تاریک و دسترسی به آن، در بخش چهارم نفرت پراکنی و تروریسم در این فضا و در نهایت در بخش پنجم به تعهدات دولت‌ها در برخورد با معضل مذکور مطابق نظام بین‌المللی حقوق بشر می‌پردازیم.

## ۲ مروری بر کارهای دیگران

محققین بسیاری به بحث درباره‌ی تروریسم و افراطی‌گرایی خشن در اینترنت به خصوص در فضای وب تاریک و راه‌های مقابله با آن پرداخته‌اند (Weimann, G. 2015; Pashentsev, E. and bazarkina, D. 2021; Vacca, J. 2020). این پژوهش‌ها از راه‌های جمع‌آوری داده انواع این فعالیت‌ها (Saini, K. and Bansal, D. 2019; Chen, H. 2007) تا بررسی اختصاصی هرکدام از این فعالیت‌ها و چگونگی استفاده از وب تاریک توسط گروه‌های تروریستی (Alayda, S. 2021; Topor, L. 2019) را در برمی‌گیرد. وجه اشتراک عمده‌ی این تحقیقات، دید کیفی آن‌ها و دسته‌بندی فعالیت‌های تروریستی ذیل عنوان جرائم سایبری می‌باشد. این در حالیست که مقاله حاضر درصدد بررسی این فعالیت‌ها از دریچه حقوق بشر و در چارچوب نظام بین‌المللی آن است.

## ۳ وب تاریک

بررسی نفرت پراکنی در وب تاریک در درجه اول نیازمند آشنایی با این فضا و چگونگی دسترسی به آن خواهد بود که در ذیل به آن می‌پردازیم.



### ۱.۳ تعریف وب تاریک

اینترنت شامل سه بخش وب سطحی، پنهان و تاریک می‌شود. وب سطحی یا آشکار<sup>۱</sup> مجموعه‌ای از وب سایت‌هایی است که توسط موتورهای جست‌وجو مرسوم مانند گوگل جمع‌آوری و نمایه می‌شوند و متعاقباً از طریق مرورگرهای رایج مانند گوگل کروم<sup>۲</sup> در دسترس عموم قرار می‌گیرند (Chertoff, 2017: 26; Ricardo, 2011; Kaur, 2020, 2) بخش دوم، وب پنهان یا عمیق<sup>۳</sup>، بزرگ‌ترین بخش شبکه گسترده جهانی محسوب می‌شود (Mazi et al., 2020: 3). موتورهای جست‌وجو مرسوم اغلب برای دسترسی به سایت‌های وب سطحی از خزنده‌های وب<sup>۴</sup> استفاده می‌کنند. طی این فرایند، خزنده‌ها وب را جست‌جو و سایت‌ها را گردآوری کرده و سپس این سایت‌ها توسط موتورهای جست‌جو طبقه‌بندی و نمایه می‌شوند (Finklea, 2017: 5) در بسیاری از موارد یافتن داده‌های وب پنهان توسط این خزنده‌ها غیرممکن می‌باشد. علت این امر را می‌توان در نوع محتوای وب پنهان جست‌جو کرد که برای مثال می‌تواند شامل محتوای پویایی که در پاسخ به یک پرسش ایجاد شده، محتوای خصوصی که نیازمند دسترسی با مجوز می‌باشد و محتوای پیوند نشده، باشد (Easttom, 2018: 27). در نهایت، وب تاریک نیز از وب سایت‌هایی که با فناوری‌های استاندارد وب ساخته می‌شوند، شکل می‌گیرد؛ با این تفاوت که دسترسی به آن‌ها مستلزم استفاده از مرورگرهای استاندارد (مانند فایرفاکس) است که از طریق بسته‌های نرم‌افزاری ویژه مسیریابی<sup>۵</sup> مسیردهی شده باشند. رایج‌ترین و پرکاربردترین این نرم‌افزارها، چه برای دسترسی به وب تاریک و چه برای مرور ناشناس وب سطحی، تور می‌باشد (Gokhale, 2020: 27). بنابراین در این مقاله، تور به‌عنوان فناوری غیرقابل شناسایی کننده معیار در نظر گرفته شده و تحقیق بر پایه این شبکه صورت می‌گیرد.

### ۲.۳ دسترسی به وب تاریک: تور

از اواسط دهه ۹۰ میلادی، آزمایشگاه تحقیقاتی نیروی دریایی ایالات متحده<sup>۶</sup> که توسط آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی پنتاگون (دارپا) تامین مالی می‌شد، در حال تحقیق و توسعه بر روی فناوری ناشناس‌کننده خود بود (McCormick, 2013: 22) این تلاش منتج به ساخت تور یا مسیریابی پیازی شد که در سال ۲۰۰۲ به‌عنوان یک نرم‌افزار منبع باز<sup>۷</sup> و رایگان برای استفاده عموم منتشر شد (Dingle- dine, 2004: site) تور با مخفی کردن درخواست‌های اینترنتی و عبور دادن آن‌ها از طریق چندین آدرس آی‌پی<sup>۸</sup> تصادفی قبل از ارتباط با مقصد در شبکه مسیریابی پیازی، امکان غیرمتصل باقی ماندن درخواست کاربر به او را فراهم کرده (Jacoby, 2016: 2) و در واقع هویت کاربر و موقعیت سرور را پنهان می‌کند. هر

<sup>1</sup>Clear Web

<sup>2</sup>Google Chrome

<sup>3</sup>Deep Web

<sup>4</sup>Web Crawlers

<sup>5</sup>special routing software packages

<sup>6</sup>United States Naval Research Laboratory (NRL)

<sup>7</sup>Open-source software

<sup>8</sup>Internet Protocol address (IP address)

آدرس آی پی که درخواست‌ها از آن عبور می‌کند، یک لایه از رمزنگاری را به سیگنال اضافه کرده که تنها خودش قادر به رمزگشایی آن می‌باشد و همین لایه‌لایه شدن وجه تسمیه این فناوری (مسیریاب پیازی) قرار گرفت (Chertoff, 2017: 27). در سال ۲۰۰۳، قابلیت میزبانی ناشناس وب تاریک نیز به این فناوری اضافه شد که در نتیجه آن علاوه بر بازدیدکننده وب، منتشرکننده سرویس‌های مخفی آن نیز ناشناس باقی می‌ماند. (Moore; Rid, 2016: 18) در حال حاضر تور توسط شرکت غیرانتفاعی پروژه تور<sup>۹</sup> اداره شده و از طریق آژانس‌های دولتی، شرکت‌ها، سازمان‌های مردم‌نهاد و کاربران، تامین مالی می‌شود (Jacoby, 2016: 3).

## ۴ نفرت‌پراکنی در وب تاریک

### ۱.۴ نفرت‌پراکنی در حقوق بشر بین‌المللی

متون مواد ۱۹ و ۲۰ میثاق بین‌المللی حقوق مدنی و سیاسی گواهی بر این واقعیت است که اگرچه آزادی بیان «یکی از مقبول‌ترین حقوق» است، اما حق مطلق نیست و ممنوعیت‌ها و محدودیت‌هایی برای آن وجود دارد. حق داشتن عقاید بدون مداخله، یک حق مطلق است و «هیچ استثنای محدودیتی را مجاز نمی‌داند». تنها در بیان آنهاست که «وظایف و مسئولیت‌های خاص» و در نتیجه محدودیت‌های احتمالی ممکن است اعمال شود. هرچند دولت عضو در اعمال این محدودیت‌ها، «نمی‌تواند خود حق را به خطر بیندازد». مطابق ماده ۱۹ (۳) (ب)، هرگونه محدودیت باید توسط قانون پیش‌بینی شود و باید برای احترام به حقوق یا شهرت دیگران [ماده ۱۹ (۳) (الف)]؛ یا حفاظت از امنیت ملی، نظم عمومی، بهداشت عمومی یا اخلاق تحمیل شوند. ماده ۲۰ میثاق بین‌المللی حقوق مدنی و سیاسی «از شدیدترین محکومیت‌های سخنان مشوق نفرت‌انگیز» توصیف شده است، اگرچه به بیان دقیق، این ماده به‌طور کلی به «سخنان مشوق تنفرآمیز» مربوط نمی‌شود، بلکه فقط به «تحریک» مربوط می‌شود. اشاره در ماده ۲۰، هم به «تبلیغ برای جنگ» و هم به «حمایت از نفرت ملی، نژادی یا مذهبی» نشان‌دهنده شدت نفرت مورد نظر است. همچنین نگرانی خود را با نفرتی که مشروط به «تحریک به تبعیض، خصومت یا خشونت» است، توصیف می‌کند (Ghanea, 2012: 301). سخنان تنفرآمیز ممکن است شامل سخنانی باشد که از اعمال خشونت‌آمیز حمایت، یا به آن‌ها تهدید یا تشویق می‌کند، اما محدود به آن نمی‌شود. امروزه شبکه‌های اجتماعی و سازمان‌های بازنشردهنده سخنان محرک نفرت از فضای مجازی به‌خصوص سطوح پنهان اینترنت همچون وب تاریک استفاده می‌کنند که در نتیجه اقدامات قانونی که برای رسانه‌های دیگر مقرر شده، در این بخش ناکارآمد یا نامناسب خواهد بود. علاوه بر این، در حالی که سخنان نفرت‌پراکنی آنلاین تفاوتی ذاتی با عبارات مشابهی که به صورت آفلاین یافت می‌شود ندارد، چالش‌های عجیبی منحصر به محتوای آنلاین و مقررات آن از جمله ماندگاری، ناشناس بودن و ماهیت بین‌صلاحیتی به‌وجود می‌آورند (Gagliardone, 2015: 13).

<sup>9</sup>The Tor Project

## ۲.۴ سیر تحول به کارگیری اینترنت توسط تروریست‌ها

تروریست‌ها می‌خواهند پیام خود را به گروه بزرگ‌تری از مردم برسانند. آن‌ها به مخاطب جهانی برای گسترش تبلیغات، برقراری ارتباط و جذب اعضای جدید نیاز دارند و اینترنت به عنوان یک رسانه ارتباطی جهانی به آن‌ها امکان انجام این کار را می‌دهد (VILIĆ, 2017: 13). آن‌ها با آگاهی به این مطلب در اتخاذ و به کارگیری پلتفرم‌های آنلاین نوظهور سریع عمل می‌کنند. در اواخر دهه نود میلادی نوبت استفاده از وبسایت‌ها بود. بیش از نیمی از ۳۰ سازمانی که تحت قانون ضد تروریسم ۱۹۹۶ ایالات متحده به عنوان سازمان‌های تروریستی خارجی تعیین شده بودند، تنها یک وبسایت داشتند؛ در حالیکه از سال ۲۰۰۳ تا ۲۰۰۴ صدها وبسایت در اختیار تروریست‌ها و حامیان آن‌ها قرار گرفت (VILIĆ, 2017: 15-16). تروریست‌ها علاوه بر راه اندازی سایت‌های خودشان، در ادامه از قابلیت‌های تعاملی پلتفرم‌های آنلاین مانند پیام‌رسان‌های سریع، بلاگ‌ها و شبکه‌های اجتماعی مانند توئیتر و یوتیوب استفاده کردند. در نهایت با انباشته شدن دستور العمل، موعظه‌ها، سخنرانی‌ها عملاً یک ویکی‌پدیای ترور ساخته شد. هر چند که این پایگاه داده در وب سطحی بود، به این معنا که در دسترس آژانس‌های مبارزه با تروریسم، سرویس‌های امنیتی و پلیس قرار داشت و در نتیجه نه تنها محتوای بارگذاری شده توسط آن‌ها قابل رصد بود، بلکه همچنین تلاش می‌کردند تا افرادی که این محتوا را دانلود کرده بودند را شناسایی کرده و حتی محتوا را تغییر داده و دست‌کاری کنند. در نهایت به دنبال بسته شدن مکرر شبکه‌های تروریستی در وب سطحی و دستگیری اداره‌کنندگان آن‌ها، افراد و گروه‌های تروریستی فعالیت‌های خود را به وب تاریک، شبکه‌ای ناشناس کننده و پنهان که به راحتی در دسترس بوده و در عین حال به طور کلی غیرقابل دسترس و نامرئی می‌باشد و به فرار از دستگیری و بسته شدن پلتفرم‌هایشان کمک می‌کند، انتقال دادند (Weimann, 2015: 6-7). در جولای ۲۰۱۵، دفتر تحقیقات فدرال اعلام کرد که داعش برای الهام بخشیدن به حملات تروریستی در سراسر جهان از وب تاریک استفاده می‌کند. این مسئله تنها به داعش اختصاص نداشته و در سال ۲۰۱۷، در تظاهرات علیه تجمع راست‌گرایان آلترناتیو به نام «راست را متحد کنید» شخصی توسط یک سفیدپوست برتری طلب کشته شد (Katz, Stockman, 2018: 10). یکی از نهادهای سازماندهی کننده این تجمع راست، سایت نئونازی دیلی استورمر<sup>۱۰</sup> بود. به دنبال این اتفاق شرکت‌هایی مانند گوگل و سایر ارائه‌دهندگان اینترنت و فناوری از دسترسی دادن به این سایت خودداری کرده و همچنین محتوای بسیاری از دیگر گروه‌های برتری طلب سفیدپوست و دیگر ملی-راست‌گرایان افراطی از وب سطحی حذف شد (Topor, 2019: 28, 36) هر چند که به سرعت خانه‌ای جدید و تقریباً بدون هیچ مقرره‌ای یعنی وب تاریک را یافت.

## ۳.۴ چگونگی تروریسم اینترنتی

اصطلاح تروریسم سایبری اولین بار توسط دکتر بری کالین به عنوان یک حمله برنامه‌ریزی شده توسط تروریست‌ها بر سیستم‌های داده و کامپیوتری تعریف شده است. بعدها تمامی فعالیت‌های تروریستی که با استفاده از اینترنت به عنوان یک ابزار انجام شده است، در این تعریف گنجانده شد. از این رو تروریسم در وب

<sup>10</sup>Daily Stormer

تاریک از تبلیغات و جنگ روانی تا استفاده‌های بسیار ابزاری مانند جمع‌آوری کمک‌های مالی، سربازگیری، داده کاوی، ارتباطات و شبکه‌سازی و هماهنگی اقدامات را شامل می‌شود که در ذیل در سه دسته کلی به آن‌ها پرداخته‌ایم (Alayda et al., 2021: 3001):

- ارتباطات: تروریست‌ها برای هماهنگی و برنامه‌ریزی عملیات خود از جنبه ناشناس و مبهم وب تاریک استفاده می‌کنند. برای مثال خدمات ایمیل مرورگر تور مانند تورباکس<sup>۱۱</sup> و سیگینت<sup>۱۲</sup> در میان جهادیون محبوب هستند، زیرا هم هویت و هم مکان خود را پنهان می‌کنند. نمونه دیگر در یک گزارش انگلیسی با عنوان «دایرةالمعارف ترور داعش» آمده‌است که به سربازهای انگلیسی داعش چگونگی استفاده از وب تاریک به منظور ارتباط با شبکه جهانی تروریست‌ها آموزش داده شده‌است (Weimann, 2015: 7, 11).
- ترویج: تروریست‌ها از وب تاریک برای انتشار اظهارات و همچنین ترویج ایدئولوژی‌های خود و انتشار اخبار کذب و شایعات برای تحریک خشونت و اقدامات تروریستی استفاده می‌کنند. از سایت‌های وب تاریک گروه‌های برتری طلب سفیدپوست می‌توان به بازارها، بلاگ‌ها (سفیدپوست نجات خواهد یافت<sup>۱۳</sup>، هایدن ووت<sup>۱۴</sup>)، انجمن‌ها (راشن هیدن انسرز<sup>۱۵</sup>) و شبکه‌های اجتماعی (کانکت<sup>۱۶</sup>، توربوک<sup>۱۷</sup>) اشاره کرد.
- تبلیغات و وعده‌های توخالی: با هدف جذب افراد زیاد و سربازگیری آن‌ها، مخصوصاً افراد کم سن و برای دریافت حمایت و منابع مالی. برای مثال می‌توان به «مبارزه‌ی اسلامی بدون برجای گذاشتن اثر، کمک مالی کنید»، وب‌سایتی در وب تاریک که به کمک‌های مالی برای جهاد از طریق تراکنش‌های بیت کوین دعوت می‌کند، اشاره کرد. اسناد آنلاینی مانند «بیت کوین و صدقات الجهاد» به منظور آموزش انجام چنین تراکنش‌هایی در وب تاریک بر روی وب‌سایت‌های این گروه‌ها قرار داده شده‌است. از این کمک‌های مالی برای انجام انواع فعالیت‌های تروریستی از جمله خرید سلاح از خود بازارهای وب تاریک استفاده می‌شود. برای مثال سلاح‌های استفاده‌شده در حملات نوامبر ۲۰۱۵ پاریس (Jenning et al., 2015) و همچنین حملات چارلی هبدو<sup>۱۸</sup> از این بازارها خریداری شده‌بود (Weimann, 2015: 11-13).

<sup>11</sup>Torbox

<sup>12</sup>Sigaint

<sup>13</sup>White Will Survive

<sup>14</sup>Heidenwut

<sup>15</sup>Russian Hidden Answers (Скрытые Ответы)

<sup>16</sup>Connect

<sup>17</sup>Torbook

<sup>18</sup>Charlie Hebdo attacks

## ۵ تعهدات دولت در مواجهه با نفرت‌پراکنی در وب تاریک

اهمیت حقوق بشر به طور گسترده در نظام بین‌المللی پذیرفته شده (Shaw, 2008: 265) و شناسایی و احترام به آن نیز وظیفه‌ای همگانی است، با این حال نظام بین‌المللی حقوق بشر تکلیف اصلی را بر دوش دولت گذارده و آن را متعهد می‌داند (میرموسوی، ۱۴۰۰: ۲۶). کمیته حقوق اقتصادی، اجتماعی و فرهنگی، تعهدات دولت‌ها را به سه دسته احترام (خودداری از مداخله در برخورداری از حقوق بشر یا محدود کردن آن)، حفاظت (حفاظت از افراد و گروه‌ها در برابر نقض حقوق بشر) و تحقق (اقدام در جهت تسهیل برخورداری از حقوق بشر اساسی) تقسیم‌بندی می‌کند (Committee on Economic, Social and Cultural Rights, 1999). در مواجهه با نفرت‌پراکنی و تروریسم در وب تاریک، تعهد دولت‌ها به خصوص تعهد به حفاظت محل بحث خواهد بود که در ادامه بررسی می‌شود.

### ۱.۵ احترام

تعهد به احترام و رعایت نوعی تعهد منفی و در جایی است که دولت وظیفه دارد نه تنها از اقداماتی پرهیز کند که باعث محروم شدن افراد از حقوق ناشی از میثاق‌ها می‌شود، بلکه از ایجاد موانع در راه استفاده از حق هم باید خودداری کند (کریون، ۱۳۸۷: ۱۵۴). همان‌طور که اشاره شد، وب تاریک برای بهره‌مندی افراد از تعدادی حقوق بشری بستری فراهم کرده است و در راستای مبارزه با تروریسم، دولت نمی‌تواند بر سر راه این برخورداری «فعلی» مانع ایجاد کند و یا آن را محدود نماید، مگر در جایی که چنین اجازه‌ای تصریح شده باشد (De Schutter, 2010: 257). بنابراین اقدامات دولت‌ها مانند قطع دسترسی به تور یا سعی در نفوذ به آن و آشکار کردن هویت کاربران به معنای مداخله و ایجاد مانع در بهره‌مندی افراد و یا محروم کردن آن‌ها از این حقوق می‌باشد و نقض تعهد احترام محسوب می‌شود. از طرف دیگر کشورهایی که بر سر راه دسترسی به وب تاریک موانع این‌چنینی نگذاشته‌اند، تعهد خود را در این زمینه ایفا کرده‌اند. برای مثال در حالی که کشورهایمانند ایالات متحده و آلمان به پشتیبانی از تور پرداخته تا جایی که از آن حمایت مالی می‌کنند، سایر کشورها مانند چین، روسیه و اتریش به شدت مخالف با آن می‌باشند.

### ۲.۵ تحقق

تعهد به تحقق وظیفه‌ای مثبت است و شامل دو وظیفه می‌شود: نخست فراهم‌سازی و تسهیل برخورداری از حقوق بشر و دوم تامین خدمات. ایفای این تعهد به موجب میثاق حقوق مدنی و سیاسی از طریق قانون‌گذاری و حفاظت نهادی از حقوق با تضمین رویه‌ای آن‌ها از راه تأسیس نهادهای قانونی لازم و دیگر اقدام‌های تقنینی، اجرایی، سیاسی و قضایی صورت خواهد گرفت. البته تعهد به تحقق موضوع اصل نسبی بودن قرار خواهد گرفت؛ دولت‌های عضو در اثربخشی به حقوق میثاق از اختیار وسیعی متناسب با توانایی‌های مالی و اقتصادی - اجتماعی‌شان برخوردار می‌باشند. اما اگر بدون دلیل موجهی این تعهدات را اجرا نکنند، ماده ۲ میثاق و همچنین حق مربوطه را نقض کرده‌اند (Nowak, 2005: 39). بر اساس تعهد مذکور، دولت‌ها باید با «تمام ابزار و وسایل مقتضی» برخورداری از حقوق بشر را فراهم کند و مبارزه با نفرت‌پراکنی در وب تاریک

نمی‌تواند توجیهی برای ایجاد مانع در دسترسی به آن باشد.

### ۳.۵ حفاظت

دولت‌ها نه تنها باید از نقض حقوق افراد در حوزه صلاحیتشان از طریق تضمین عدم ارتکاب چنین تخلفاتی از جانب مأمورین دولتی خودداری کنند (تعهد به احترام) بلکه باید همچنین درجایی که نقض این حقوق با اعمال ارتكابی طرفین خصوصی (افراد، گروه‌ها و یا اشخاص حقوقی) تهدید می‌شود، مداخله کرده (De Schutter, 2010: 365) و از حقوق افراد در برابر طرف‌های ثالث حفاظت نمایند (Nowak, 2005: 38). جایی که نشانه‌هایی از در خطر نقض بودن حقوق افراد وجود داشته یا موقعیتی وجود دارد که چنین خطری را ایجاد می‌کند، دولت باید اقدامات پیشگیرانه‌ای انجام دهد تا عدم تحقق این خطرات را در بالاترین حد ممکن تضمین کند. زمانی که اقدامات صورت گرفته مؤثر واقع نشده و بازیگران غیردولتی مرتکب نقض شده‌اند، مقامات دولتی نباید منفعل باقی بمانند؛ چراکه متعهدند جبران‌های مؤثری برای افرادی که حقوقشان نقض شده تضمین کنند و همچنین در موارد معینی برای متخلف مجازات‌های کیفری یا اداری در نظر گیرند (De Schutter, 2010: 365). گاهی میثاق چنین اقداماتی را به صراحت تجویز می‌کند از جمله در مورد ممنوعیت تبلیغ برای جنگ یا طرفداری از نفرت ملی، نژادی یا مذهبی مطابق ماده ۲۰.

### ۴.۵ دولت و ایفای تعهد به حفاظت

تعهد دولت به حفاظت از حقوق افراد در برابر اشخاص ثالث از جمله کسب و کارهای مختلف به شکل جامع و دقیقی در قالب ده اصل در اصول راهنما سازمان ملل در کسب و کار و حقوق بشر گنجانده شده است (Ruggie, 2011: 29). همچنین پروژه فناوری بی<sup>۱۹</sup> در سال ۲۰۱۹، توسط حقوق بشر سازمان ملل راه‌اندازی شد. این پروژه تعهد حفاظت دولت در برابر شرکت‌های فناوری را بر اساس اصول راهنمای سازمان ملل در پنج اصل بیان می‌کند. دولت‌ها در برابر شرکت پروژه تور به‌عنوان یک شرکت فناوری، موظف به اجرای این اصول و در نتیجه ایفای تعهد حفاظتی خود می‌باشند. از آنجایی که اصول راهنمای سازمان ملل در مورد شرکت‌های فراملی و سایر واحدهای کسب و کار می‌باشد، رفع دو ابهامی که ممکن است درباره شرکت پروژه تور ایجاد شود، ضروری به نظر می‌رسد. پرسش اولی که ممکن است مطرح شود، این خواهد بود که این شرکت فراملی نیست. در پاسخ باید گفت که اصول راهنما صرفاً درباره شرکت‌های فراملی نبوده و شرکت‌های غیرفراملی که ویژگی این نوع شرکت‌ها را داشته باشند مانند بیشتر شرکت‌های فناوری تحت شمول این اصول قرار خواهند گرفت. در درجه دوم به حساب آوردن یک پروژه غیرانتفاعی به‌عنوان یک واحد تجاری می‌تواند سوال برانگیز باشد. در پاسخ می‌توان به اصل چهاردهم اصول راهنما اشاره کرد که تصریح می‌کند این اصول فارغ از ساختار واحد به آن اعمال می‌شود.<sup>۲۰</sup>

<sup>19</sup>B-Tech Project

<sup>20</sup>Guiding Principles on Business and Human Rights



## ۵.۵ شرکت‌های فناوری و حقوق بشر

احترام و پاسداری از حقوق بشر وظیفه‌ای همگانی است؛ با این وجود در نظام بین‌المللی حقوق بشر، نقض تعهدات حقوق بشری از سوی اشخاص اعم از حقیقی یا حقوقی عموماً قابل تعقیب و مجازات نیست. در سال‌های اخیر کوشش‌هایی برای شناسایی مسئولیت فردی در نظام بین‌المللی حقوق بشر در حال انجام است. کمیسیون حقوق بین‌الملل در پیش‌نویس جرایم علیه صلح و امنیت نوع بشر، نقش مسئولیت فردی را به‌عنوان ضمانت اجرای حقوق بشر مورد توجه قرار داده‌است. این کمیسیون در سال ۱۹۹۱ پیشنهاد کرد نقض‌های نظام‌مند حقوق بشر جرم بین‌المللی تلقی شود و ارتکاب‌کنندگان مسئول شناخته‌شوند (براونلی، ۱۳۹۶: ۴۳۷). افزون بر این گام‌هایی برای پدیدآوردن پیش‌نویس اعلامیه مسئولیت‌های اجتماعی بشری و هنجارهای مربوط به مسئولیت‌های شرکت‌های فراملی و سایر بنگاه‌های تجاری در خصوص حقوق بشر برداشته شده‌است (میرموسوی، ۱۴۰۰: ۴۸). همان‌طور که پیش‌تر بیان کردیم این تلاش‌ها منجر به تدوین اصول راهنمای سازمان ملل در کسب‌وکار و حقوق بشر شد. این اصول درباره‌ی مسئولیت شرکت‌های خصوصی در احترام به حقوق بشر الزام‌آور نبوده اما در سال ۲۰۱۱ توسط شورای حقوق بشر به تأیید و امضا رسید و در سال‌های اخیر نیز توسط تعدادی از دولت‌ها به‌تصویب رسیده و در حال اجرایی شدن است.<sup>۲۱</sup>

## ۶ نتیجه‌گیری

تروریسم در دارک وب یکی از خطرناک‌ترین نقض‌های حقوق بشر محسوب می‌شود و می‌تواند به همان اندازه و چه بسا پرگرنده‌تر از تروریسم غیراینترنتی باشد. سازمان‌های تروریستی، افراد و گروه‌های افراطی و نفرت‌پراکن به‌منظور حفظ بقا و فعالیت‌های خود همیشه در پی به‌روزترین و کاربردی‌ترین ابزار بوده‌اند و با پیدایش اینترنت با سوءاستفاده از ویژگی‌های متمایز آن اهداف خود را محقق ساخته‌اند. در واکنش به خطر شناسایی شدن و دستگیری از طریق وب سطحی، این افراد و سازمان‌ها فعالیت‌های خود را به غارهای مجازی وب تارک انتقال داده و این بار با سوءاستفاده از امتیازات این فضا یعنی ناشناسی و نامرئی بودن به نفرت‌پراکنی و تحریک عموم به خشونت، دشمنی و تبعیض می‌پردازند. در مقابله با آن، تعهد دولت به حفاظت از حقوق بشر ایجاب می‌کند تا به مبارزه با این افراد و گروه‌ها بپردازد. جزئیات ایفای این تعهد در اصول راهنمای سازمان ملل تشریح شده که می‌تواند راهگشای خوبی در رسیدن به این هدف محسوب شود. علاوه‌براین، اینترنت شبکه بین‌المللی از کامپیوترها است بنابراین همکاری بین‌المللی برای اثرگذاری کامل اقدامات دولت‌ها ضروری به‌نظر می‌رسد. همچنین روش‌ها و فناوری‌هایی توسط متخصصین حوزه علوم کامپیوتری برای شناسایی موردی تروریست‌ها، تحلیل و بررسی فعالیت‌ها و داده‌ها در این فضا تهیه و ساخته شده‌است. برای مثال می‌توان به ممکس<sup>۲۲</sup> به‌عنوان یکی از این فناوری‌ها اشاره کرد که با هدف روشن‌سازی فضای وب تارک و کشف الگوها و روابط در داده‌های آنلاین به‌منظور یاری‌رسانی به مجریان قانون و دیگران برای ردیابی فعالیت‌های غیرقانونی ساخته

<sup>21</sup> <https://documentsddsny.un.org/doc/RESOLUTION/GEN/G11/144/71/PDF/G1114471.pdf>

pdf

<sup>22</sup> Memex

شده است. این فناوری در اصل برای رصد قاچاق انسان در وب تاریک ساخته شده اما همان اصول را می‌توان تقریباً برای هر نوع فعالیت غیرقانونی در این فضا اعمال کرد. نکته‌ای که توجه به آن بسیار اهمیت دارد این است که در عین دفاع از جامعه در برابر تروریسم، این فرآیند نباید منجر به نابودی کیفیات و ارزش‌هایی شود که در وهله اول آن جامعه را قابل دفاع می‌سازد. اینترنت و وب تاریک به طرق متعددی دربرگیرنده ایده‌آل‌های دموکراتیک آزادی بیان و ارتباطات آزاد می‌باشند. اما اگر به‌خاطر ترس از حملات تروریستی، آزادی خود در استفاده از اینترنت را محدود کنیم در واقع به تروریست‌ها پیروزی را تقدیم کرده و دموکراسی را نادیده گرفته‌ایم. در این راستا، دفتر کمیساریای عالی سازمان ملل با انتشار گزارشی، رمزگذاری داده‌های دیجیتال و ناشناس ماندن ارتباطات در دنیای آنلاین را ضرورتی انکارناپذیر برای تامین آزادی بیان و حقی جهان‌شمول دانسته و از همه دولت‌ها خواسته‌است تا با حفظ این حق، پاسخ‌گوی مقتضیات عصر دیجیتال باشند. چارچوب قانونی برای حمایت از تحقیقات جنایی و همکاری متقابل کشورها در این فضا ضروری است چراکه تحقیقات، اغلب با نقض گسترده حریم خصوصی اشخاص انجام می‌شود و دولت‌ها از ابزارهایی که در قانون شناسایی نشده استفاده می‌کنند. بنابراین سیاست‌های حاکم بر وب تاریک ضمن شناخت صحیح از این فضا باید بتواند میان حریم خصوصی اشخاص و مسئولیت دولت‌ها بر توقف فعالیت‌های مجرمانه تعادل برقرار کند تا از این طریق دولت‌ها علاوه بر ایفای تعهد خود به حفاظت از حقوق بشر، تعهد به احترام و تحقق این حقوق را نیز رعایت کنند.

## مراجع

- [۱] براونلی، یان، اصول حقوق بین‌الملل عمومی، ترجمه حبیبی مجنده، محمد، ویرایش هشتم، انتشارات دانشگاه مفید، قم، ۱۳۹۶.
- [۲] میرموسوی، سیدعلی، «تعهد و مسئولیت‌های دولت در برابر حقوق بشر»، دوره ۱۶، شماره ۱، ۱۴۰۰، ۵۱-۲۶.
- [3] O. De Schutter, *International Human Rights Law: Cases, Materials, Commentary*, Cambridge: Cambridge University Press, 2010.
- [4] M. Nowak, *U.N. Covenant on Civil and Political Rights – CCPR-Commentary*, 2nd ed., Germany: N.P. Engel Publishers, 2005.
- [5] M. Shaw, *International law*, Cambridge: Cambridge University Press, 2008, p. 265.
- [6] M. Chertoff, “A public policy perspective of the Dark Web,” *Journal of Cyber Policy*, vol. 2, pp. 26-38, 2017.
- [7] R. Dingeldine, “TOR: The second-generation Onion Router,” *Journal of Management Information Systems*, vol. 18, pp. 303-319, 2014.
- [8] K. Finklea, “Dark Web,” *Congressional Research Service*, Mar. 2017.
- [9] I. Gagliardone, D. Gal, T. Alves, and G. Martinez, *Countering Online Hate Speech*, Paris: UNESCO, 2015.
- [10] N. Ghanea, “The concept of racist hate speech and its evolution over time,” Paper presented at the 81st session of the United Nations Committee on the Elimination of Racial

- Discrimination's Day of thematic discussion on Racist Hate Speech, Geneva, Aug. 2012, p.301.
- [11] S. Kaur, S. Randhawa, "Dark Web: A web of crimes," *Wireless Pers. Commun.* vol. 112, pp. 2131-2158, 2020.
- [12] S. Alayda et. al., "Terrorism on dark web," *Turkish Journal of Computer and Mathematics Education*, vol. 12, pp. 3000-3005, Apr. 2021.
- [13] L. Topor, "Dark hatred: antisemitism on the dark web," *Journal of Contemporary Anti-semitism*, vol. 2, pp. 25-42, Dec. 2019.
- [14] G. Weimann, "Going dark: terrorism on the dark web," *Studies in Conflict and Terrorism*, vol. 39, pp. 195-206, Dec. 2015.
- [15] V. Vilić, "Dark Web, cyber terrorism and cyber warfare: dark side of the cyberspace," *Balkan Social Science Review*, vol. 10, pp. 7-25, Dec. 2017.
- [16] J. Ruggie, "Guiding principles on business and human rights: implementing the United Nations 'protect, respect and remedy' framework," *Netherlands Quarterly of Human Rights*, vol. 29, pp. 224-253, 2011.



## بررسی روش‌های اجماع بلاک‌چین‌های مورد استفاده در اینترنت اشیا

حسین شعله‌رسا<sup>۱</sup>، محمدعلی آصف<sup>۱</sup>، کاظم فولادی قلعه<sup>۲</sup>

<sup>۱</sup> دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران  
{h.sholehrasa,maasef}@ut.ac.ir

<sup>۲</sup> استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛  
سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران  
kfouladi@ut.ac.ir

### چکیده

با توسعه و فراگیری مفاهیم فناوری بلاک‌چین و ملموس شدن کاربردهای متنوع آن، فناوری‌های دیگر نظیر اینترنت اشیا نیز با آن آمیخته شده‌اند. بلاک‌چین، دفتر کل توزیع‌شده‌ای است که اغلب به صورت غیرمتمرکز توسط گره‌های متصل به شبکه اداره می‌شود. این سازوکار نیاز به الگوریتم‌هایی برای اثبات درستی پردازش‌ها و عدم تقلب دارد که اجماع نامیده می‌شود. روش‌های مختلفی برای اجماع وجود دارد، اما در فضای اینترنت اشیا علاوه بر اثبات درستی نقل و انتقالات داده‌های درون شبکه، مفاهیم جدیدی مانند اثبات و راستی‌آزمایی موقعیت جغرافیایی و وجود فیزیکی نیز مطرح است. در سالیان اخیر با رواج بیشتر رمزارزها، ایده‌ها و پروژه‌های زیادی برای ایجاد چنین بستری مطرح شده است که از پروژه مطرح بازار بنام «هلیوم» تا اجماع نوآورانه‌ای مانند G-PBFT و LH-Raft که از اجماع اختصاصی خود برای ایجاد یک شبکه بیسیم امن و اثبات وجود گره‌ها در موقعیت جغرافیایی‌شان استفاده می‌کنند تا خدمات مورد نیاز دستگاه‌های مبتنی بر اینترنت اشیا را فراهم کنند. در این مقاله روش‌های اجماع متمرکز بر اثبات مکان از جنبه‌های هدف، کاربردها، نحوه کارکرد و توزیع پاداش مورد بررسی و مقایسه قرار خواهند گرفت تا گزینه‌های بهینه‌شناسایی شوند.

**کلمات کلیدی:** بلاک‌چین، الگوریتم اجماع، اینترنت اشیا، رمزارز، زنجیره‌ی بلوکی، اثبات مکان.

## ۱ مقدمه

### ۱.۱ بلاک چین

بلاک چین فناوری نوظهوری برای ذخیره سازی غیرمتمرکز<sup>۱</sup> داده است که در سالیان اخیر با توجه به مزایای پرشمار آن مورد توجه حوزه های مختلف قرار گرفته است. بلاک چین دفترکل توزیع شده ای است که شبکه ای نظیر به نظیر<sup>۲</sup> تشکیل می دهد. داده ها در این شبکه که شامل تراکنش ها و قطعه کدهای قابل اجرا به نام «قرارداد هوشمند»<sup>۳</sup> هستند، به صورت تغییرناپذیر در بلوک هایی قرار می گیرند که هر یک هش<sup>۴</sup> منحصر به فردی دارند. نحوه ایجاد و تأیید هش در هر شبکه بر مبنای الگوریتم های متفاوتی می تواند باشد. معمولاً در طی استفاده از این سیستم ها، نیاز به اعتماد به شخص ثالثی نیست. همچنین مدیریت و تصمیم گیری در آنها معمولاً بر دوش یک تصمیم گیرنده ی مرکزی نیست، بلکه به صورت انجمن محور<sup>۵</sup> است. این ویژگی ها که بخشی از مشخصه های زنجیره بلوک ها هستند، منجر به ادغام این فناوری با حوزه های مختلفی مثل برنامه های مالی غیرمتمرکز<sup>۶</sup>، آثار هنری، صنعت بازی های کامپیوتری، ذخیره داده های پزشکی، زنجیره تأمین و بسیاری موارد دیگر شده است. یکی از این حوزه ها، اینترنت اشیا است [۱].

### ۲.۱ اینترنت اشیا و بلاک چین

اینترنت اشیا<sup>۷</sup> سیستمی از دستگاه های مرتبط به یکدیگر است که قابلیت انتقال اطلاعات روی شبکه بدون نیاز به انسان را دارد. چیزها/ اشیا، برای مثال می تواند ماشینی باشد که سنسورهای درونی آن به راننده اخطار زیاد یا کم بودن فشار لاستیک می دهد. همین طور میتواند دستگاهی باشد که در قلب کاشته شده و وضعیت قلب را دریافت و پردازش می کند.

اینترنت اشیا در عصر کنونی به طور گسترده ای برای جمع آوری داده ها از حسگرها و انجام وظیفه خاص با توجه به نیازمندی های تعریف شده، در حال استفاده است. برای محقق سازی این امر نیاز به شبکه های متصل به هم برای تبادل داده ها وجود دارد. این شبکه باید امن و بلادرنگ<sup>۸</sup> باشد تا اطلاعات با تأخیر بسیار کم و در پروتکلی امن جابجا شود. در بعضی از حوزه ها مثل مراقبت های بهداشتی، اطلاعات ذخیره شده نیز باید از امنیت بالایی برخوردار باشد. از مشکلات بزرگ اینترنت اشیا حریم خصوصی و امنیت آن است. یکی از حمله های بزرگی که در این مورد رخ داده است، حمله بزرگ Mirai بود. برای حل این دو مشکل می توان از بلاک چین استفاده نمود. با این وجود، در طی پیاده سازی یک سیستم مبتنی بر بلاک چین برای اینترنت اشیا، محدودیت های ذخیره سازی، برق و توانایی محاسباتی دستگاه های اینترنت اشیا چالش برانگیز

<sup>1</sup>Decentralized

<sup>2</sup>Peer-to-peer

<sup>3</sup>Smart Contract

<sup>4</sup>Hash

<sup>5</sup>Community-based

<sup>6</sup>Decentralized Finance Applications (dApps)

<sup>7</sup>Internet of Things

<sup>8</sup>Real-time



است [۲]، [۳].

### ۳.۱ مکانیزم‌های اجماع

همان‌طور که پیش‌تر گفته شد، معمولاً مدیریت و تصمیم‌گیری پروژه‌های غیرمتمرکز بر عهده گروهی از تصمیم‌گیران دخیل در پروژه می‌باشد. معنای کلمه اجماع<sup>۹</sup> به صورت خلاصه توافق اعضای یک گروه برای تصمیم‌گیری است. اجماع از اجزای مهم یک سیستم غیرمتمرکز قدرت گرفته از زنجیره بلوکی است [۴].

### ۴.۱ اهمیت استفاده از اجماع بهینه

با استفاده از پروتکل‌های اجماع کلاسیک‌تر احتمال آسیب‌پذیری به حمله سیبیل<sup>۱۰</sup> [۵]، هزینه زیاد محاسباتی و مقیاس‌پذیری وجود دارد. الگوریتم‌های اجماع که به موقعیت جغرافیایی دستگاه‌ها توجه می‌کنند تا حد خوبی مشکل مقیاس‌پذیری و هزینه زیاد محاسبات را حل کرده‌اند. بعضی از این الگوریتم‌ها به جای استفاده از تمامی دستگاه‌های اینترنت اشیا، از منتخبی از آنها برای الگوریتم اجماع خود استفاده می‌کنند. در ادامه این مقاله، موضوعات زیر را مورد بررسی قرار می‌دهیم:

- سیر تکاملی و جزئیات روش‌های اجماع مورد استفاده در بلاک‌چین‌ها را مرور می‌کنیم.
- به بررسی دقیق‌تر اجماع‌های بهینه می‌پردازیم.
- و مشخصه‌هایی برای سنجش روش‌های اجماعی که موقعیت مکانی را مد نظر دارند تعریف می‌کنیم.

## ۲ الگوریتم‌های اجماع

### ۱.۲ پیش‌نیاز: مفهوم اجماع

در یک سیستم متمرکز مثل شرکت، کارمندان در زمان مشخصی حاضر و در دسترس هستند اما در سیستم‌های غیرمتمرکز بدین شکل نیست. در نتیجه، الگوریتم‌های اجماع باید دارای یک حداقل برای تصویب یک تغییر باشند. به طور مثال اگر ۵۱٪ از گره‌های یک شبکه در الگوریتم اجماع بلاک‌چین به توافق برسند که اطلاعات را آپدیت و به روزرسانی کنند، این اتفاق خواهد افتاد. الگوریتم اجماع یک روش است که از طریق آن، تمام افراد فعال در شبکه بلاک‌چین به یک توافق مشترک درباره وضعیت حال حاضر دفترکل توزیع شده دست می‌یابند. بدین ترتیب، الگوریتم‌های اجماع، اعتبار را در شبکه بلاک‌چین و اعتماد را بین گره‌ها یا همتایان ناشناس در محیط محاسباتی توزیع شده ایجاد می‌کنند. اساساً پروتکل اجماع اطمینان حاصل می‌کند هر بلاک جدید که به بلاک‌چین اضافه می‌شود، تنها نسخه واقعی است که توسط تمام گره‌ها مورد توافق واقع شده است. پروتکل اجماع بلاک‌چین شامل اهداف خاصی نظیر دستیابی به توافق، همکاری، حق مساوی

<sup>9</sup>Consensus

<sup>10</sup>sybil

هر گره و حضور اجباری هر گره در فرایند اجماع است. در نتیجه، الگوریتم اجماع در صدد دستیابی به توافق مشترکی است که توسط کل شبکه حاصل شده باشد. الگوریتم‌های اجماع کاربردهای دیگری هم دارند، مانند:

- تصمیم‌گیری در مورد اینکه آیا یک تراکنش صلاحیت تأیید و ذخیره روی دفترکل توزیع‌شده را دارد یا خیر؛
- انتخاب گره‌ها برای مدیریت امور روی دفترکل توزیع‌شده؛
- تضمین یک‌دست‌سازی اطلاعات روی سیستم‌های سرویس‌دهنده به شبکه.

## ۲.۲ پیش‌نیاز: روش‌های اجماع متداول مورد استفاده در شبکه‌های بلاک‌چین

در این بخش به بررسی اجمالی تعدادی از روش‌های اجماع متداول می‌پردازیم.

**اثبات کار (Proof-of-work).** اجماع مورد استفاده در اولین شبکه بلاک‌چین بود که در سال ۲۰۰۹ در رمزارز بیت‌کوین<sup>۱۱</sup> [۶] استفاده شد. در این مدل، داده‌هایی به کمک تابع هش ۲۵۶-SHA در بلاک‌ها ذخیره می‌شوند. در میان گره‌های حاضر در شبکه، عضوی که هش با مشخصه‌های مورد نیاز و تعریف شده را بیابد، برای گرفتن تأیید، آن را به همه شبکه ارسال می‌کند. در صورتی که بیشتر از نیمی از شبکه آن را تأیید کنند، بلاک معتبر شناخته می‌شود و با هش پیدا شده بسته می‌شود. سپس گره‌ای که هش را پیدا کرده است، پاداش دریافت می‌کند. لازم به ذکر است که این عملیات به وسیله پردازش سخت‌افزارهای متصل به شبکه انجام می‌شود. از معایب آن می‌توان به مصرف برق و حمله ۵۱٪ اشاره کرد.

**اثبات سهام (Proof-of-stake).** کارکرد این مدل اجماع نیازی به دستگاه سخت‌افزاری ندارد، چرا که گره‌های حاضر در شبکه، طبق تعداد سهامشان به صورت تصادفی (تعداد توکن یا همان سهام بیشتر باعث افزایش شانس و قدرت می‌شود) در بستن بلاک معتبر ایفای نقش می‌کنند. در واقع با اختصاص رمزارز به یک شبکه، در یک مسابقه شرکت داده می‌شویم. همانند قرعه‌کشی بانکی که به عنوان مثال هر ۲۰ دلار یک امتیاز برای شما محاسبه می‌شود و هرچه امتیاز شما بیشتر باشد قاعدتاً شانس بیشتری هم برای برنده شدن خواهید داشت.

**اثبات فعالیت (Proof-of-activity).** در واقع ترکیبی از الگوریتم اجماع اثبات کار و اثبات سهام است. مرحله ابتدایی که استخراج است، از الگوریتمی مشابه گواه اثبات کار استفاده می‌شود و سپس با رفتن به بلوک بعدی از الگوریتمی شبیه به الگوریتم گواه اثبات سهام کمک می‌گیرد [۷].

<sup>11</sup>Bitcoin

## ۳.۲ اجماع‌های متمرکز بر موقعیت مکانی

### ۱.۳.۲ PoC (Proof of Coverage)

شبکه هلیوم. PoC الگوریتم اجماع مورد استفاده در رمزارز هلیوم<sup>۱۲</sup> [۷] است. در ادامه به بررسی اجماع مورد استفاده در این شبکه می‌پردازیم. این شبکه توسط تیم باتجربه‌ای با هدف فراهم کردن ارتباط دستگاه‌های اینترنت اشیا در شبکه‌ای غیرمتمرکز و برطرف کردن کمبودها و نقص‌های فعلی زیرساخت‌های موجود راه اندازی شده است. هلیوم یک شبکه بی‌سیم گسترده و غیرمتمرکز قدرت گرفته از بلاک‌چین برای اینترنت اشیا است که در سال ۲۰۱۹ راه‌اندازی شد. گره‌های شبکه دارای هات‌اسپات<sup>۱۳</sup> هایی هستند که ترکیبی از دستگاه‌های مودم روتر بی‌سیم و ماینر بلاک‌چین می‌باشند. ماینرهای متصل به شبکه با توکن HNT با توجه به پارامترهای مختلفی پاداش خود را دریافت می‌کنند. هلیوم شبکه خودش را «شبکه مردم»<sup>۱۴</sup> نامیده است. برای تبدیل شدن به یک ماینر می‌توان یکی از دستگاه‌های برندهای ارائه دهنده آن را خریداری کرد و یا به دست خود ساخت. هر دستگاه می‌تواند تا محدوده‌ای بالغ بر ۱۰ کیلومتر (محدوده فرکانسی تحت پروتکل Lora WAN [۸]) را پوشش دهد. این محدوده فرکانسی معمولاً طبق قانون‌گذاری مقررات رادیویی کشورها مشکلی ندارد و برای عموم آزاد است.

در این شبکه هر چند بلاک یک بار، وضعیت هات‌اسپات‌ها به صورت مداوم با سازوکاری به نام PoC Challenge مورد بررسی قرار می‌گیرد. داده‌های اثبات‌ها در بلاک‌ها ذخیره می‌شود که تأیید قطعی از پوشش وایرلسی است که توسط گره‌های شبکه ساخته شده است. تا به امروز میلیون‌ها چالش صادر و پردازش شده است.

نحوه دقیق کارکرد چالش‌ها بدین شکل است [۷]:

- چالشگر<sup>۱۵</sup>: هات‌اسپاتی که چالش را می‌سازد و ارسال می‌کند. هات‌اسپات‌ها به طور متوسط یک بار در هر ۳۰۰ بلاک چالش ارسال می‌کنند.
- انتقال دهنده<sup>۱۶</sup>: مخابره‌کننده یا چالش‌شونده نیز می‌تواند نامیده شود. این هات‌اسپات هدف چالش می‌باشد و مسئول انتقال داده‌ی چالش به هات‌اسپات‌های مجاور (شاهدها) برای ثبت شاهد می‌باشد.
- شاهد<sup>۱۷</sup>: هات‌اسپات‌هایی که از لحاظ جغرافیایی به چالش‌شونده نزدیک هستند و وجود هات‌اسپات چالش‌شونده در فرایند چالش را بعد از اینکه به آنها منتقل شد گزارش می‌کنند و در واقع شهادت می‌دهند.

<sup>12</sup>Helium

<sup>13</sup>Hotspot

<sup>14</sup>The People's Network

<sup>15</sup>Challenger

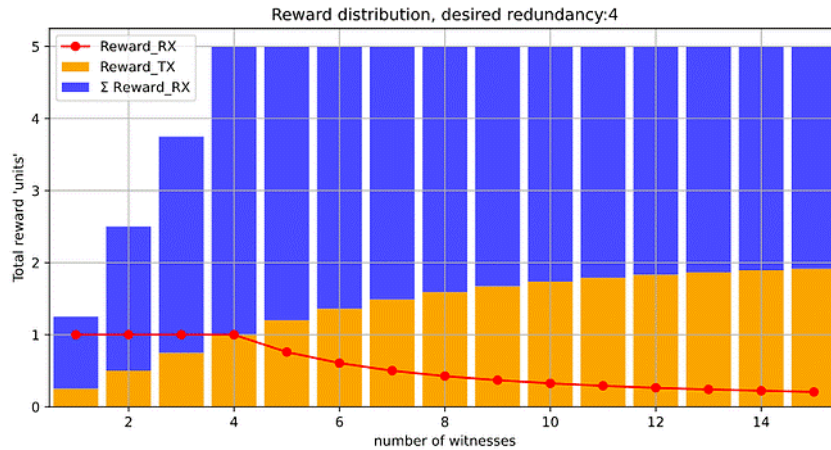
<sup>16</sup>Transmitter or Challengee

<sup>17</sup>Witness

**جزئیات عملیات چالش.** هات اسپات‌ها پس از انجام چالش مقداری توکن HNT (توکن شبکه هلیوم) را به عنوان پاداش دریافت می‌کنند. چالشگر ابتدا یک کلید عمومی و خصوصی زودگذر می‌سازد تا در چالش استفاده شود. کلید عمومی و خصوصی SHA256 هر دو همراه با هش بلاک فعلی به عنوان یک درخواست PoC ذخیره می‌شوند. اگر درخواست معتبر باشد و توسط بلاک چین تأیید شود، هش بلاکی که رسید در آن ظاهر می‌شود با هش کلید عمومی زودگذر و هویت و اطلاعات چالشگر برای ایجاد آنتروپی قابل تأیید ترکیب می‌شود. سپس یک عدد رندوم از طریق این آنتروپی ایجاد می‌شود و برای انتخاب یک هات اسپات تصادفی از کل شبکه (نه لزوماً مودم‌های نزدیک چالش‌شونده) استفاده می‌شود. وقتی بسته چالش ساخته شد، به انتقال دهنده از طریق شبکه هم‌تا به هم‌تا هلیوم منتقل می‌شود. چالش‌شونده مورد هدف، بسته چالش را دریافت می‌کند و بیرونی‌ترین لایه را به وسیله کلید خصوصی و کلید عمومی زودگذر این چالش رمزگشایی می‌کند. کلید عمومی زودگذر در بسته PoC نمایش داده می‌شود و هات اسپات دریافت کننده بلاک چین را برای دریافت PoC فعال، SHA256 مربوطه کلید عمومی بررسی می‌کند و سریعاً نتیجه را به بسته در شبکه هلیوم منتقل می‌کند. هر تعداد از هات اسپات‌های نزدیک به چالشگر از لحاظ جغرافیایی، این داده را دریافت می‌کنند و به عنوان شاهد، وجود چالش‌شونده را اثبات خواهند کرد.

**پاداش دهی در فرایند PoC.** به صورت کلی دو متغیر برای پاداش دهی وجود دارد: تعداد شاهدین در مدل HIP15 و تعداد هات اسپات‌ها در هر فضای ۶ ضلعی تعریف شده در HIP17. در مدل HIP15 برای هر چرخه چالش، هر پاداش بین هات اسپات‌هایی که در فرایند نقش داشته‌اند تقسیم می‌شود. اگر هات اسپاتی در این چرخه به عنوان شاهد نقش داشته باشد، سهم ۳۱٪.۵ از پاداشی که به انتقال دهنده‌ها داده می‌شود خواهد داشت. برای مثال اگر ۵ هات اسپات شاهد در یک چالش موفق، شرکت داشته باشند، هر هات اسپات یک پنجم از ۳۱٪.۵ از پاداش در نظر گرفته شده برای چالش را می‌گیرد. برای هر انتقال دهنده، هرچه تعداد شاهدان بیشتر باشد، پاداش انتقال دهنده بیشتر خواهد بود. در مدل HIP17 اگر تعداد هات اسپات‌های هر منطقه از هدف تراکمی مورد نظر بیشتر شود، شاهد کمتر پاداش می‌گیرد. هر محدوده‌ی جغرافیایی هدف تراکمی خود را دارد و با بیشتر شدن تعداد ماینرها و در واقع شاهد‌ها از تعداد مشخصی، درآمد چالش‌شونده افزایش پیدا نمی‌کند و درآمد شاهد‌ها کم می‌شود.

**تأیید اثبات.** زمانی که چالشگر مجموعه کامل رسید شاهد‌ها و انتقال دهنده‌های فرآیند را دریافت کرد یا زمان سپری شده از زمان صدور چالش، از زمان تعیین شده بالاتر رفت چالش PoC کامل در نظر گرفته می‌شود. در این مرحله چالشگر رسید اثبات را به عنوان یک تراکنش به بلاک چین ارائه می‌کند تا توسط گروه اجماع فعلی تأیید شود. به دلیل آنکه مراحل انجام شده توسط چالشگر برای ساخت و کامل کردن اثبات به راحتی قابل انجام مجدد هستند، اعضای گروه اجماع می‌توانند مشروعیت اثبات را تأیید کنند. به طور مشخص، چالشگر کلید زودگذر سری را که برای به انجام درخواست اصلی PoC و رمزگذاری هر لایه از بسته چالش استفاده می‌کند را فاش می‌کند. این اطلاعات مهم، که تا زمان انتشار رسید پنهان بوده است، امکان ایجاد مجدد آنتروپی قطعی را می‌دهد.



شکل ۱: میزان پاداش به ازای تعداد هات اسپات‌های فعال در یک منطقه [۷]

هلیوم از پروتکل اجماع نوآورانه و اختصاصی خود استفاده می‌کند. این پروتکل به منظور اهمیت بخشیدن به ویژگی‌های کلیدی زیر ایجاد شده است:

- بدون نیاز به اجازه: هر هات اسپات مطابق با قوانین اجماع و مشخصه‌های شبکه باید بتواند به صورت آزادانه در شبکه هلیوم شرکت کند.
- طراحی کاملاً غیرمتمرکز: هیچ مشوق و انگیزه‌ای برای استفاده از عواملی مثل مصرف کم انرژی برای استقرار سخت‌افزار بیشتر از حد نیاز و متمرکز شدن در یک نقطه وجود ندارد.
- بر اساس کار مفید: دستیابی به اجماع شبکه باید مفید و قابل استفاده مجدد برای شبکه باشد. در سیستم‌های مبتنی بر توافق مثل بیت‌کوین، کارهایی که برای دستیابی به اجماع انجام می‌شود فقط برای یک بلوک خاص معتبر است. در مقابل، در سیستم اجماع هلیوم باید کارهایی انجام شود که علاوه بر ایمن‌سازی شبکه بلاک‌چین، برای شبکه مفید و قابل استفاده باشد.
- نرخ بالای تراکنش‌های تأییدشده: پروتکل باید بتواند به تعداد زیادی تراکنش در ثانیه دست یابد و هنگامی که تراکنش توسط بلاک‌چین مشاهده شد، تأیید شده منظور می‌گردد. کاربرانی که داده‌های دستگاه را از طریق شبکه هلیوم ارسال می‌کنند، نمی‌توانند زمان‌های طولانی حل و فصل بلاک را که معمولاً در سایر بلاک‌چین‌ها وجود دارد را متحمل شوند.

**Honey Badger BTF**. پروتکل اجماع هلیوم بر اساس توزیعی از پروتکل Honey Badger BFT (HBBFT) [۹] نوشته شده است. HBBFT بر اساس مجموعه‌ای از تحقیقات است که در ابتدا توسط اندرو میلر در دانشگاه Illinois آغاز شد. پروتکل HBBFT یک پروتکل پخش اتمی با زمان غیریکسان است که برای ایجاد گروهی از گره‌های شناخته‌شده برای دستیابی به اجماع در مورد پیوندهای غیرقابل اعتماد

طراحی شده است. در هلیوم، یک گروه اجماعی از اعتبارسنج‌های منتخب، تراکنش‌های رمزگذاری شده را به عنوان ورودی دریافت می‌کنند و قبل از تشکیل یک بلاک و افزودن آن به بلاک‌چین به توافق مشترک در مورد ترتیب این تراکنش‌ها می‌رسند.

پروتکل HBBFT متکی بر طرحی است که به عنوان Threshold encryption شناخته می‌شود. با استفاده از این طرح، معاملات با استفاده از یک کلید عمومی مشترک رمزگذاری می‌شوند و تنها زمانی رمزگشایی می‌شوند که گروه اجماع انتخاب شده برای رمزگشایی آنها باهم همکاری کنند. استفاده از Threshold encryption هلیوم را قادر می‌سازد تا به تراکنش‌های غیرقابل سانسور دست یابد.

**انتخابات گروه اجماع و سوددهی** یک گروه اجماع جدید، یکبار در هر دوره انتخاب می‌شود. در حال حاضر ۴۰ عضو برای هر گروه اجماعی انتخاب شده‌اند، همان‌طور که در متغیر زنجیره‌ای num\_consensus\_members تعریف شده است. با توجه به پارامترهایی که پیش‌تر توضیح داده شد، می‌توان برآورد کلی از درآمد تخمینی یک هات‌اسپات با در نظرگیری تعداد هات‌اسپات‌های اطراف صفر، کمی و تعدادی زیادی را بیان کرد که در این لحظه در حدود 12 HNT به ازای هر دستگاه به صورت ماهیانه می‌باشد.

## LH-Raft ۲.۳.۲

این الگوریتم از پروتکل اصلی Raft [۱۰] الهام گرفته است. الگوریتم Raft از نظر کارایی و تحمل خطا<sup>۱۸</sup> همانند الگوریتم Paxos [۱۱] می‌باشد و ساده شده این الگوریتم است. Paxos, Raft و PBFT [۱۲] از نظر توان عملیاتی<sup>۱۹</sup> توانایی رسیدگی به هزاران درخواست، زمان پردازش کم و هزینه محاسبات کم را دارا هستند. این ویژگی‌ها، این الگوریتم‌ها را برای استفاده در اینترنت اشیا مناسب می‌کنند. همچنین مقیاس‌پذیری آنها کم است به همین خاطر بهتر است در بلاک‌چین‌های خصوصی که اهراز هویت دارند مورد استفاده قرار گیرند. الگوریتم LH-Raft [۱۳] با استفاده از پروتکل اجماع سلسله‌مراتبی و آگاه از مکان<sup>۲۰</sup> مشکل مقیاس‌پذیری را حل کرده است. برای جلوگیری از حمله‌های مختلف و تشکیل یک گره اجماع داخلی، اطلاعات جغرافیایی دستگاه شامل طول و عرض جغرافیایی و برچسب زمانی<sup>۲۱</sup> جمع‌آوری می‌شوند. این الگوریتم کارایی بهتری دارد و همچنین هزینه ارتباط و تأخیر اجرای الگوریتم آن نیز کم است. زمانی که تعداد گره‌های در شبکه زیاد شود، اختلاف زیادی در هزینه ارتباط و تأخیر اجرای الگوریتم با دیگر الگوریتم‌ها ایجاد می‌شود که نشان‌دهنده مقیاس‌پذیری بالا این الگوریتم می‌باشد.

الگوریتم LH-Raft ابتدا گره‌های داوطلبی را انتخاب می‌کند که در هر زیرلایه شامل لایه برگ<sup>۲۲</sup>، لایه وسطی (میانی)<sup>۲۳</sup> و لایه بالایی شبکه بلاک‌چینی، به اجماع کمتری نیاز دارد. سپس یک گروه محلی از کاندیداها بر اساس امتیاز فاصله و شهرت گره‌ها تشکیل می‌دهد. وظیفه‌ی این گره‌ها انتخاب رهبران محلی

<sup>18</sup>Fault-tolerance

<sup>19</sup>Throughput

<sup>20</sup>Location-aware

<sup>21</sup>Timestamp

<sup>22</sup>Leaf layer

<sup>23</sup>Middle layer



جدول ۱: مقایسه نتایج Raft و LH-Raft؛  $n$  تعداد تمام دستگاه‌های اینترنت اشیا و  $c$  تعداد گروه‌های منتخب است.

الگوریتم	سر بار ارتباط	هزینه ارتباط
Raft	$O(n^2)$	$n^2$
LH-Raft	$O(c^2)$	$n^2/c^2$

می‌باشد. در مرحله بعد، تمام رهبران محلی از چند لایه برگ و بقیه گره‌های کاندیدا دوباره رهبر بالاتر را انتخاب می‌کنند. برای اجماع لایه بالاتر از طرح امضای آستانه<sup>۲۴</sup> استفاده می‌شود. در آخر رهبر اصلی انتخاب می‌شود. این طرح شبکه بلاک‌چینی، یک سلسله‌مراتبی است که بر اساس اطلاعات منطقه‌ای دستگاه‌های اینترنت اشیا و استفاده از رونوشت‌های محلی و جهانی است. این امر سبب حفظ ثبات برای تمام تراکنش‌های بلاک‌چینی در تمام لایه‌ها است.

اگر گره‌های متقلب در الگوریتم PoW بیشتر از ۵۰٪ تعداد، الگوریتم PBFT بیشتر از ۳۳٪.۳۳ تعداد و الگوریتم LH-Raft در حالت غیر بی‌زانشی (خرابی گره، تأخیر شبکه، گم شدن بسته) بیشتر از ۵۰٪ تعداد و در حالت بی‌زانشی بیشتر از ۳۳٪.۳۳ تعداد باشد می‌توانند دفترکل تراکنش‌ها را عوض کنند. دو مورد مهم از نتایج تئوری این الگوریتم می‌توان به جدول ۱ اشاره کرد [۱۳].

### ۲.۳.۲ GPBFT

این الگوریتم از الگوریتم اجماع PBFT بهره برده است. الگوریتم G-PBFT [۱۴] به اطلاعات جغرافیایی دستگاه‌های اینترنت اشیا ارزش بیشتری می‌دهد. این امر سبب محافظت در مقابل حمله سیبیل می‌شود. الگوریتم PBFT [۱۲] پروتکلی مناسب برای اینترنت اشیا با شبکه‌ای با اندازه کوچک است. گره‌های شرکت کننده به راحتی نمی‌توانند به شبکه اضافه یا حذف شوند. ترافیک بالا سر بار شبکه ( $O(n^2)$ ) و پویا نبودن سبب این می‌شود که برای شبکه اینترنت اشیا با گره‌های زیاد و پویا مناسب نباشد. الگوریتم G-PBFT این دو مشکل را حل می‌کند. دستگاه‌های اینترنت اشیا که به صورت ثابت هستند معمولاً از قدرت پردازشی بیشتری نسبت به بقیه دستگاه‌های اینترنت اشیا مثل موبایل دارند. لامپ هوشمند خیابان یک نمونه از دستگاه‌های ثابت می‌باشد. از جهتی دیگر، معمولاً شرکت‌ها صاحب این دستگاه‌ها هستند پس احتمال اینکه یک گره مخرب باشد کمتر است. به همین خاطر G-PBFT از دستگاه‌های ثابت استفاده می‌کند و برای بلاک‌چین‌های خصوصی و کنسرسیومی<sup>۲۵</sup> مناسب است.

در این الگوریتم دو نوع گره مشتری و تأییدکننده وجود دارد. تمام تأییدکننده‌ها باهم یک کمیته اجماع تشکیل می‌دهند. تراکنش‌هایی که توسط مشتری ساخته می‌شود را بین خود جابه‌جا می‌کنند تا سر بار ارتباطات کم شود. علاوه بر اینکه اطلاعات جغرافیایی دستگاه‌ها توی هر تراکنش هست، باید به صورت دوره‌ای نیز موقعیت و پرچسب زمانی خود را بفرستند. برای این کار از Crypto Spatial Coordinates (CSC)

<sup>24</sup>Threshold Signature Scheme

<sup>25</sup>consortium

جدول ۲: جدول انتخابات [۱۴]: چند نمونه CSC به همراه برچسب زمانی و تایمر جغرافیایی در الگوریتم G-PBFT

تایمر جغرافیایی	برچسب زمانی	CSC	
0	29/8/2022 18:00:00	5AH71r9wTRp9eHsqR	۱
56:04	29/8/2022 18:56:04	5AH71r9wTRp9eHsqR	۲
06:56:04	30/8/2022 00:00:00	5AH71r9wTRp9eHsqR	۳
12:56:04	30/8/2022 06:00:00	5AH71r9wTRp9eHsqR	۴
18:56:04	30/8/2022 12:00:00	5AH71r9wTRp9eHsqR	۵

استفاده می‌شود. قبل از اینکه انتخابات تأییدکننده اجرایی شود، یک سری گره وجود دارند که به‌عنوان تأییدکننده هستند. این گره‌ها اطلاعات دستگاه‌های اینترنت اشیاء که شامل CSC و برچسب زمانی‌شان می‌باشد را اعتبارسنجی می‌کنند.

الگوریتم G-PBFT همانند الگوریتم PBFT از Views و Phases یکسانی استفاده می‌کند ولی در الگوریتم G-PBFT لفظ جدید era معرفی شده است که می‌توان به‌عنوان یک اتصال چند PBFT متوالی در نظر گرفت. اگر زنجیره ثابت PBFTها عوض شود زنجیره از era آن به یک era جدید می‌رود.

## ۳ تحلیل مشخصه‌ها و خروجی اجماع‌های مبتنی بر موقعیت مکانی

### ۱.۳ مقایسه پروژه‌های کاربردی در اینترنت اشیا و بلاک‌چین

در جدول ۳ مقایسه بین چند پروژه کاربردی که به منظور همگام‌سازی بلاک‌چین و اینترنت اشیا طراحی شده‌اند انجام شده است. در این جدول اجماع اختصاصی هر پروژه، جزئیات هدف و سرویس اصلی و سخت‌افزار مرتبط با اینترنت اشیا بررسی شده است. بعضی از پروژه‌ها مانند هلیوم بخش بزرگی از بازار را تصاحب کرده‌اند، در حالی که بعضی دیگر در مراحل ابتدایی هستند و حتی به‌طور کامل برای استفاده عموم عرضه نشده‌اند. همچنین برخی پروژه‌ها از اجماع اختصاصی خود استفاده می‌کنند و برخی دیگر از الگوریتم‌های کلاسیک نظیر PoS بهره می‌گیرند. در بخش سخت‌افزاری نیز شاهد طیف قابل توجهی از دستگاه‌های گوناگون با اهداف مختلف هستیم.

### ۲.۳ مقایسه الگوریتم‌های اجماع

در جدول ۴ مقایسه‌ای بین الگوریتم‌های اجماع متداول و الگوریتم‌های جدیدتر و کاربردی در اینترنت اشیا انجام شده است. نمونه‌های با مدل بلاک‌چین بدون اجازه رویکرد غیرمتمرکزی را دنبال می‌کنند در حالی که نمونه‌های با اجازه کاربردی اغلب سازمانی دارند. الگوریتم‌های جدیدتر معمولاً از سرعت و مقیاس پذیری بیشتری برخوردار هستند و سربار محاسباتی را کاهش داده‌اند. الگوریتم‌های بررسی شده در این مقاله با

جدول ۳: مقایسه مشخصه‌های بلاک‌چین‌های مورد استفاده در حوزه اینترنت اشیا

دستگاه‌های اینترنت اشیا	سرویس	الگوریتم اجماع	بلاک‌چین	پروژه
دستگاه‌های اینترنت اشیا	شبکه غیر متمرکز	Proof of Coverage	Helium	Helium [7]
قفل الکترونیکی	فروشگاه کمیسیون	PoW	Ethereum	Slock.it [15]
پنل خورشیدی	پردازش اطلاعات پنل‌های خورشیدی	PoS	SolarCoin	ElectricChain [16]
تراشه بلوک	سرویس تراکنش برای اینترنت اشیا تعبیه شده (embedded)	PoS PoW	Hardware-based Consortium Blockchain	Filament [17]
دستگاه‌های اینترنت اشیا	پلتفرم بلاک‌چین	BFT	BFT Blockchain	JD.com [18]
ربات‌ها و دستگاه‌های صوتی	راه حل‌های اینترنت اشیا - بلاک‌چین	PoW	Public Blockchain	LeewayHertz [19]
پنل خورشیدی	بازارگاه انرژی خورشیدی	PoW	Public Blockchain Solution	LO3 Energy [20]
دستگاه و خانه‌های هوشمند	راه حل‌های اینترنت اشیا - بلاک‌چین	Atonomi	Atonomi	Atonomi [21]
سنسورها، عملگرها و لوازم خانگی	خدمات یکپارچه در اینترنت اشیا و بلاک‌چین	PoW	Litecoin	UniquID [22]
دلالت‌های اقتصادی (brokers)	سرویس امنیتی	PBFT	Fabric	Xage [23]

علامت \* مشخص شده‌اند. به صورت کلی می‌توان گفت الگوریتم‌های G-PBFT و Proof Of Coverage و LH-Raft سرعت تراکنش و مقیاس‌پذیری بالا، سربار کم شبکه و محاسبات را به نسبت بقیه مکانیزم‌های اجماع دارا هستند.

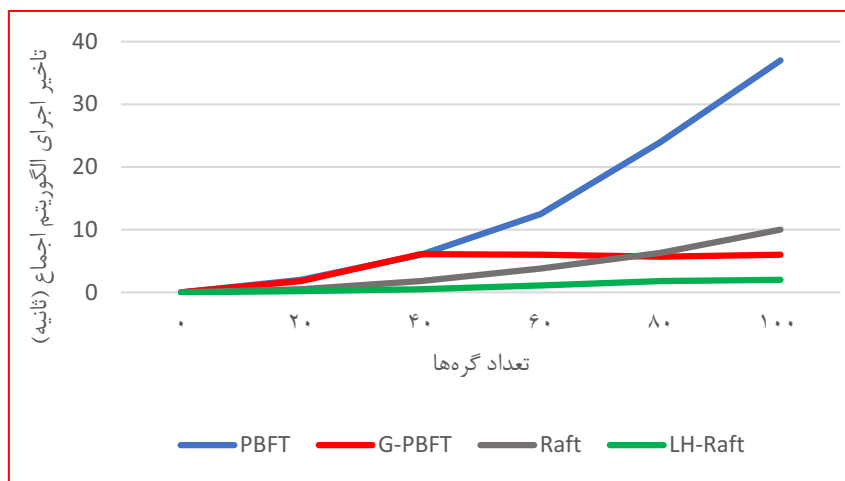
### ۳.۳ مقایسه کارایی الگوریتم‌های اجماع مورد بررسی

در شکل ۲ به بررسی کارایی الگوریتم‌های اجماع مورد بررسی پرداخته‌ایم. برای محاسبه کارایی الگوریتم‌ها، به جای معیار تراکنش بر ثانیه (TPS) از معیار تأخیر اجرا الگوریتم اجماع استفاده می‌کنیم. در واقع تأخیر را از زمانی که تراکنش به گره فرستاده می‌شود و بعد از اجرای الگوریتم اجماع در دفتر توزیع کل نوشته می‌شود، محاسبه می‌گردد. طبق نمودار، رشد الگوریتم PBFT به صورت نمایی می‌باشد. الگوریتم G-PBFT در تعداد گره کمتر، مثلاً ۴۰ عدد، به دلیل این که تأییدکنندگان به کمیته اضافه می‌شوند، رفتاری همچون

PBFT دارد. این در حالی است که از زمانی که انتخاب کنندگان جدید به کمیته اضافه نمی شوند مقدار تأخیر اجرای الگوریتم اجماع آن بیشتر نمی شود [۱۴]. الگوریتم Raft با افزایش گره، تأخیر اجماع آن افزایش می یابد. در بعضی قسمت ها با شیب ملایم این افزایش صورت می گیرد. در مقابل، الگوریتم LH-Raft تعداد کاندیداها کمتر است، چرا که با توجه به موقعیت مکانی گره ها انتخاب می شوند و این امر سبب تأخیر کم تر است. می توان گفت از گره ۱ تا ۱۰۰، تأخیر الگوریتم LH-Raft ۷۲٪ کمتر از Raft است [۱۳].

جدول ۴: مقایسه مشخصه‌های روش‌های اجماع متداول و روش‌های مورد استفاده در بلاک چین‌های مرتبط با اینترنت اشیا

الگوریتم	نوع بلاک چین	سرعت	مقیاس پذیری	سربار شبکه	سربار محاسباتی	تحمل تقلب	مثال استفاده شده
PoW	بدون اجازه	کم	کم	زیاد	زیاد	$25\% >$ قدرت محاسبات	BTC
PoS	بدون اجازه	کم	کم	زیاد	کم	$50\% >$ سهام	Peercoin
DPoS [24]	بدون اجازه	زیاد	کم	کم	کم	$50\% >$ اعتبارسنج‌ها	BitShares
PoA	بدون اجازه	کم	زیاد	کم	کم	$50\% >$ سهام آنلاین	Decred
PoSpace [25]	بدون اجازه	کم	کم	زیاد	کم	$50\% >$ فضا	SpaceMint
PoI [26]	بدون اجازه	کم	کم	زیاد	کم	$50\% >$ سهام	NEM
PoB [27]	بدون اجازه	کم	کم	زیاد	کم	$50\% >$ سکه‌ها	XCP
Proof of Coverage *	بدون اجازه	زیاد	زیاد	کم	کم	$33.3\% >$ کپی‌ها	Helium
G-PBFT*	بدون اجازه	زیاد	زیاد	کم	کم	$33.3\% >$ تأیید	
BFT	با اجازه	زیاد	کم	زیاد	کم	$33.3\% >$ کپی‌ها	Tendermint
PBFT*	با اجازه	زیاد	کم	زیاد	کم	$33.3\% >$ کپی‌های معیوب	Hyperledger
dBFT [28]	با اجازه	کم	زیاد	زیاد	کم	$33.3\% >$ کپی‌های معیوب	NEO
Hot Stuff [29]	با اجازه	زیاد	کم	کم	کم	$33.3\% >$ کپی‌ها	Libra
RAFT	با اجازه	زیاد	کم	کم	کم	$50\% >$ کپی‌ها	IPFS
LH-RAFT*	بدون اجازه	زیاد	زیاد	کم	کم	$33.3\% >$ گره‌ها	



شکل ۲: مقایسه کارایی الگوریتم‌های اجماع مورد بررسی [۱۳]، [۱۴]

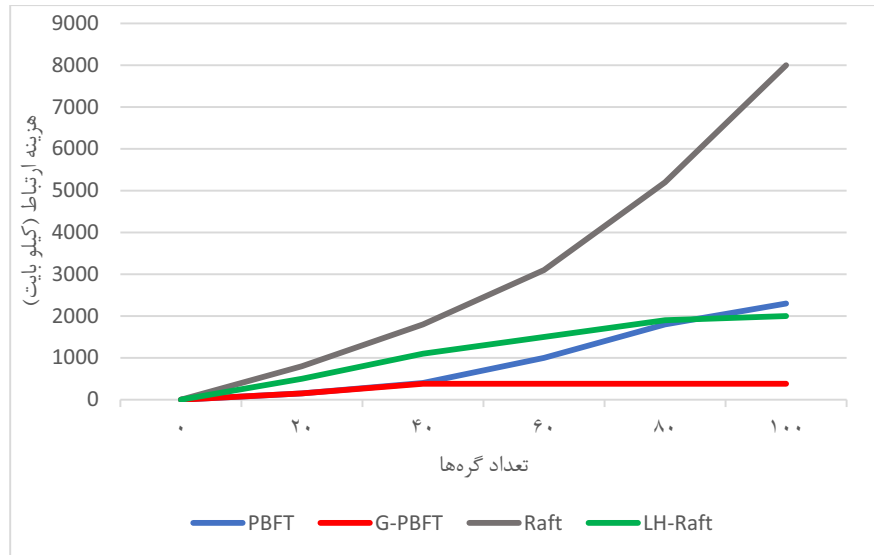
### ۴.۳ مقایسه هزینه‌های ارتباطی در الگوریتم‌های اجماع مورد بررسی

در شکل ۳ به بررسی هزینه‌های ارتباطی در اجماع‌های مورد بررسی پرداخته‌ایم. برای محاسبه هزینه‌ی ارتباط از معیار هزینه ارتباط تمام گره‌ها که فقط یک تراکنش بلاک‌چینی انجام می‌شود، استفاده شده است. در الگوریتم PBFT با افزایش تعداد گره‌ها هزینه ارتباط با شیبی ملایمی در حال افزایش است ولی در G-PBFT بعد از حدود ۴۰ گره مقداری نزدیک به ۴۰۰ کیلوبایت را دارد و این روند به صورت تقریباً ثابت ادامه دارد [۱۴]. همچنان در حدود ۴۰ گره مقدار هزینه این دو الگوریتم یکسان است. در الگوریتم LH-Raft مقدار گره‌های زیر لایه‌ی برگ، میانی و بالایی به ترتیب ۲۰، ۴۰ و ۸۰ گره در حداکثر تعداد در نظر گرفته شده است [۱۳]. از ۱ تا ۲۰ گره به صورت رشد خطی به حدود ۵۰۰ کیلوبایت می‌رسد. به طور مشابه می‌توان گفت از ۱ تا ۸۰ گره نیز به صورت خطی رشد می‌کند و به نزدیک ۱۸۵۰ کیلوبایت می‌رسد. در مقابل، الگوریتم Raft با افزایش گره‌ها هزینه ارتباط نیز با شیب بسیار افزایش می‌یابد.

### ۵.۳ ویژگی‌های مقایسه‌های انجام شده

در مقایسه‌های انجام شده به صورت مرحله به مرحله طیف گسترده‌ای از متغیرهای کیفی و کمی را در پروژه‌های این حوزه، الگوریتم‌های اجماع این حوزه و در نهایت جزئیات مشخصه‌های هر یک از الگوریتم‌های اجماع مورد توجه در این مقاله را بررسی و مقایسه نمودیم. در اغلب بررسی‌های ترویجی انجام شده در این حوزه، تنها مشخصه‌های مرسوم که در همه اجماع‌ها وجود دارد به عنوان متغیر در نظر گرفته شده‌اند، و در مدل‌های مبتنی بر موقعیت مکانی هم صرفاً مشخصه‌های مرتبط با راستی‌آزمایی داده‌ها مورد توجه قرار گرفته بود؛ اما در بررسی‌های انجام شده تلاش کردیم تا ویژگی‌های خاصی و تعیین‌کننده برای این رشته از اجماع‌های متمرکز بر اثبات موقعیت مکانی نیز در نظر گرفته شود تا روش بهینه مشخص شود. همچنین در اغلب بررسی‌های پیشین، مشخصه‌های فنی پروژه و الگوریتم محصولات برجسته در بازار همانند پروژه هلیوم،





شکل ۳: مقایسه هزینه ارتباط نمودارهای مورد بررسی [۱۲]، [۱۴]

در کنار روش‌های نوین، قرار نگرفته بود اما در این مقاله تلاش کردیم تا با کنار هم قرار دادن و مقایسه‌ی آنها، به دید کلی جامع‌تر و بهتری دست یابیم.

## ۴ نتیجه‌گیری

الگوریتم‌های اجماع با به‌کارگیری در شبکه‌های بلاک‌چین در سالیان اخیر، به جایگاه بسیار مورد توجهی دست یافته‌اند. متخصصین تلاش می‌کنند تا با تحلیل مدل‌های پیشین و در نظر گرفتن تقاضاهای فعلی این حوزه، آنها را بهبود بخشند و روش‌های نوینی ابداع کنند. در این مقاله تلاش کردیم تا با انجام تحلیل‌های چند جانبه در خصوص الگوریتم‌های اجماع مورد استفاده در بلاک‌چین‌های توسعه داده شده برای ارتباط با اینترنت اشیا، بهینگی آنها را در زمینه‌های مختلف بسنجیم. در پایان می‌توان گفت با توجه به داده‌های به‌دست آمده، در صورت اولویت داشتن سرعت LH-Raft می‌تواند گزینه مناسب‌تری باشد. در صورت اهمیت بالاتر هزینه کم و پهنای باند بیشتر الگوریتم G-PBFT می‌تواند مورد استفاده قرار گیرد، و در حالتی که پیاده‌سازی در مقیاس انبوه و عرضه در بازار به‌مدت طولانی‌تر مهم باشد، الگوریتم Proof-of-Coverage مورد استفاده در هلیوم می‌تواند شبیه‌سازی شود.

الگوریتم‌های اجماع در سالیان اخیر دچار دگرگونی‌های بسیاری شده‌اند و همچنان فضای بسیاری برای رشد و به بلوغ رسیدن این حوزه‌ی نوظهور وجود دارد. الگوریتم‌های جدیدتر و مقایسه جنبه‌های دیگر این روش‌ها به‌عنوان سنج تحلیل‌ها، و مقایسه و دسته‌بندی الگوریتم‌های کاربردی در موضوعات دیگر مثل ذخیره‌سازی داده‌های پزشکی و یا زنجیره تأمین می‌تواند موضوعات جالب توجه دیگر به‌عنوان موضوع پژوهش بیشتر علاقه‌مندان به این فضا قرار گیرد.

## مراجع

- [1] Zheng, Zibin, et al. "Blockchain challenges and opportunities: A survey". International journal of web and grid services 14.4 (2018): 352-375.
- [2] G. D. Putra, V. Dedeoglu, S. S. Kanhere, R. Jurdak, and A. Ignjatovic, "Trust-based blockchain authorization for iot," IEEE Transactions on Network and Service Management, 2021.
- [3] L. Zhu, Y. Wu, K. Gai, and K.-K. R. Choo, "Controllable and trustworthy blockchain-based cloud data management," Future Generation Computer Systems, V. 91, pp. 527-535, 2019.
- [4] Bach, Leo Maxim, Branko Mihaljevic, and Mario Zagar. "Comparative analysis of blockchain consensus algorithms". 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). Ieee, 2018.
- [5] J. R. Douceur, "The sybil attack," International workshop on peer-to-peer systems, pp. 251-260, 2002.
- [6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- [7] Amir Haleem, Andrew Allen, Andrew Thompson, Marc Nijdam, Rahul Garg, "Helium A Decentralized Wireless Network," 2018.
- [8] LoRa Alliance, "LoRaWAN - LoRa Alliance Technology," 2014.
- [9] Andrew Miller and Yu Xia and Kyle Croman and Elaine Shi and Dawn Song, "The Honey Badger of BFT Protocols," 2016.
- [10] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," Annual Technical Conference, p. 305-319, 2014.
- [11] L. Lamport et al, "Paxos made simple," ACM Sigact News, V. 32, pp. 18-25, 2001.
- [12] M. Castro, B. Liskov et al, "Practical byzantine fault tolerance," OSDL, V. 99, pp. 173-186, 1999.
- [13] W. L. M. N. Hao Guo, "A Hierarchical and Location-aware Consensus Protocol for IoT-Blockchain Applications," IEEE Transactions on Network and Service Management, 2020.
- [14] L. Lao, X. Dai, B. Xiao and S. Guo, "G-PBFT: A Location-based and Scalable Consensus Protocol for IoT-Blockchain Applications," IEEE International Parallel and Distributed Processing Symposium, pp. 664-673, 2020.
- [15] SlockIt, <http://slock.it>, (accessed: 2022/09/10).
- [16] ElectricChain, "Electricchain the solar energy blockchain project for climate change and beyond," <https://www.crunchbase.com/organization/electricchain>, (accessed: 2022/09/10).
- [17] Filament, "Filament's industrial internet of things blockchain solution wins 2018 IoT innovator award," 2018, <https://www.crunchbase.com/organization/filamenthq>, (accessed: 2022/09/10).

- [18] JDChain, “JD enterprise blockchain service,” <https://blockchain.jd.com>, (accessed: 2022/09/10).
- [19] LeewayHertz, “Blockchain development for startups and enterprises,” 2019.
- [20] LO3, “LO3 energy the future of energy,” <https://lo3energy.com>, (accessed: 2022/09/10).
- [21] Atonomi, “Atonomi - bringing trust and security to IoT,” <https://atonomi.io>, (accessed: 2022/09/10).
- [22] UniquID, “UniquID incorporation blockchain identity access management,” <http://uniquid.com>, (accessed: 2022/09/10).
- [23] Xage, “Xage security,” <https://xage.com>, (accessed: 2022/09/10).
- [24] D. Larimer, “Delegated proof-of-stake (DPoS),” Bitshare whitepaper, 2014, <https://www.geeksforgeeks.org/delegated-proof-of-stake/>.
- [25] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, “Proofs of space,” Advances in Cryptology, p. 585–605, 2015.
- [26] NEM, “NEM whitepaper,” <https://www.crunchbase.com/organization/nem>, (accessed: 2022/09/10).
- [27] J. Frankenfield, “Proof of burn,” <https://www.investopedia.com/terms/p/proof-burn-cryptocurrency.asp>, (accessed: 2022/09/10).
- [28] NeoDocsBuilder, “NEO consensus mechanism,” <https://docs.neo.org/docs/en-us/basic/consensus/dbft.html>, (accessed: 2022/09/10).
- [29] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, “Hotstuff: Bft consensus with linearity and responsiveness,” Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, p. 347–356, 2019.



## ضرورت اصلاح قوانین و مقررات تبلیغاتی فضای سایبر در جهت حمایت از حقوق کودکان و نوجوانان

محمد امینی<sup>۱</sup>، رسول مظاهری کوهانستانی<sup>۲</sup>

<sup>۱</sup> دانشجوی دکتری حقوق خصوصی، دانشگاه اصفهان، اصفهان  
m.aminiphdlaw74@ase.ui.ac.ir

<sup>۲</sup> استادیار، گروه حقوق دانشکده علوم اداری و اقتصاد، دانشگاه اصفهان، اصفهان  
r.mazaheri@ase.ui.ac.ir

### چکیده

استفاده کودکان و نوجوانان از وسایل الکترونیکی ارتباط جمعی و پیام‌های مختلف تبلیغاتی که روزانه از این طریق به آن‌ها ارسال می‌شود، امری اجتناب‌ناپذیر است. راجع به رعایت حقوق کاربران نابالغ هنگام تنظیم و ارسال این گونه پیام‌ها در فضای سایبر، قوانین و آیین‌نامه‌هایی به طور پراکنده در حقوق ایران وجود دارد، اما پرسش اصلی تحقیق حاضر آن است که آیا طبق قوانین موجود، سازندگان تبلیغات و بازاریاب‌ها هنگام فرستادن پیشنهادات تبلیغاتی، وظیفه‌ای در شناسایی مخاطبان خود دارند؟ آیا این قوانین در منع ارسال تبلیغاتی که مغایر با رشد و ارتقای توانایی کودکان و نوجوانان است مقررهای دارند یا مواد مربوط به بخش حمایت از کاربران نابالغ، منحصر می‌شود در به‌کارگیری روش‌هایی که در هر حال امکان دور زدن آن‌ها و دستیابی به چنین تبلیغاتی را فراهم می‌سازد؟ نگارندگان با روش توصیفی-تحلیلی و انتقادی، پس از بررسی قوانین مربوط به تبلیغات در فضای سایبر، مشخص می‌کنند که نقص‌ها و خلاءهای اساسی در این زمینه و در جهت حمایت از کودکان و نوجوانان وجود دارد و پیشنهاد می‌دهند تا مقررهای با مضمون منع ارسال پیام‌های تبلیغاتی نامناسب و مغایر با رشد و توانایی کاربران کودک و نوجوان، در آیین‌نامه اجرایی مواد ۵۶ و ۵۷ قانون تجارت الکترونیکی اضافه شود.

**کلمات کلیدی:** قوانین تبلیغاتی، فضای سایبر، حقوق کودکان و نوجوانان، آیین‌نامه اجرایی مواد ۵۶ و ۵۷ قانون تجارت الکترونیکی.

### ۱ مقدمه

توسعه و پیشرفت روزافزون فضای سایبر و فناوری‌های ارتباطاتی و نیز افزایش استفاده از فضای مجازی نقش مؤثری در تولید، انتشار و انتقال اطلاعات داشته و سطح دسترسی به محتوای برخط را برای آحاد جامعه فراهم ساخته است، اما در عین حال، شرایطی را فراهم می‌سازد تا در آن حقوق افراد نقض یا محدود شود. در این میان حقوق کودکان به عنوان یکی از آسیب‌پذیرترین اقشار جامعه معمولاً مورد تعرض و سوء استفاده قرار

می‌گیرد. چنانکه برخی در این زمینه و در بحث حریم خصوصی تبلیغاتی، به اقدامات بازاریاب‌ها در ترغیب کودکان به ارائه اطلاعات بیشتر و تبدیل فعالیت‌های مجازی آنان به پول اشاره کرده‌اند [۲۵]. بعضی نیز در تعریف ارزش نمایی، نقض حریم خصوصی از طریق پلتفرم‌های مختلف را در تبدیل تعاملات اجتماعی کودکان به اهداف ابزاری و پولی صاحبان مشاغل معنی کرده‌اند، هم‌چنان که در بُعد رابطه‌ای نیز رابطه بین کسب‌وکارها و تبلیغ با کاربران کودک را یک طرفه و عاری از ارزش اجتماعی حریم خصوصی دانسته‌اند [۲۶]. کودکان ممکن است با دریافت محتواهای قانونی، ولی نامناسب، از طریق تماس، تلکس، ارسال پیام و ... تحت تأثیر فضای مجازی قرار گیرند. برای مثال، در حین بازدید از وبسایت‌ها، کوکی‌ها، یا سایر روش‌های تبلیغاتی، یک کودک ممکن است محتواهای خشونت آمیز، نفرت‌انگیز و مستهجن را به صورت آنلاین دریافت کند که در رفتار پرخاشگرانه کودک ناخوشایند باشد و بر سیستم روحی - روانی و ارزش‌های او تأثیر گذارد و او را سوق به پذیرش ارزش‌های غلط دهد. هم‌چنین، سازمان‌های تجاری قادر هستند تا برای کودکان پیام تبلیغاتی، اسپم، اسپانسر و ... ارسال کنند و اطلاعات شخصی آنان را دریافت نمایند.

شرکت‌های تبلیغاتی و ارائه‌کنندگان خدمات اینترنتی، در کنار دولت‌ها نسبت به محافظت از کودکان در برابر محتواها و نیز کنترل رفتارهای مضر در فضای سایبر مسئولیت خطیر و مهمی را بر عهده دارند. آن‌ها مسئولیت فراهم آوردن زمینه ارتقای نگرش، مهارت، دانش، درک، ارزش‌های حقوق بشری و رفتارهای لازم برای شرکت فعالانه کودکان و نوجوانان در عرصه زندگی عمومی و اجتماعی و مسئولیت‌پذیری آنان با محفوظ داشتن رعایت حقوق دیگران را بر دوش دارند و باید تمام تلاش خود را به کار گیرند تا از بروز خطرات احتمالی به کودکان و نوجوانان آنلاین در فضای سایبر جلوگیری به عمل آید و رفتار آنها در چنین محیط‌هایی کنترل شود [۳].

براین اساس و باتوجه به در دسترس بودن فضای سایبر و آسان بودن برقراری ارتباط و ارسال تبلیغات در این گونه از محیط‌های مجازی، پرسش اصلی مقاله آن است که آیا هرگونه تبلیغی برای افراد نابالغ از نظر قوانین کشور ممکن است؟ آیا شرکت‌های تبلیغاتی در شناسایی مخاطبان خود هیچ وظیفه‌ای ندارند و در ارسال تبلیغات و پیشنهاد برای خرید و استفاده از آن‌ها، آزادند؟ قوانین موجود برای سازمان‌ها و مؤسسات تجاری و شرکت‌های تبلیغاتی، چه تکالیفی را از این حیث پیش‌بینی کرده است و یا آنکه در این زمینه ناقص می‌باشند؟

روش تحقیق حاضر به صورت توصیفی - تحلیلی و انتقادی است و شیوه‌ی گردآوری داده‌ها به شکل کتابخانه‌ای و اسنادی می‌باشد و براساس عنوان مقاله، به ترتیب توضیحاتی راجع به رعایت حقوق کودکان و نوجوانان در ارسال پیام‌های تبلیغاتی، قوانین و مقررات تبلیغاتی ایران در جهت حمایت از کاربران نابالغ و لزوم بازنگری و اصلاح مقررات تبلیغاتی، با ملاحظه‌ی حقوق کودکان و نوجوانان، داده می‌شود و در انتها به نتیجه‌ی حاصل از تحقیق پرداخته خواهد شد.



## ۲ مروری بر کارهای دیگران

حبیب‌الهی و همکاران (۱۴۰۱)، در مقاله «وضعیت قوانین تبلیغات تلویزیونی برای کودکان در ایران»، قوانین و مقررات حاکم بر تبلیغات بازرگانی برای کودکان را آسیب‌شناسی کرده تا از این طریق گامی در مسیر مناسب‌سازی فضاهای رسانه‌ای مرتبط با کودکان برداشته باشد و در انتها به صورت کلی پیشنهاد می‌دهد که کارگروهی برای تدوین دستورالعمل‌های محتوایی و شیوه‌نامه‌های پخش برای رده‌های مختلف سنی کودک و نوجوان ایجاد شود، اما راجع به وضع ماده یا موادی در جهت اصلاح قوانین موجود، پیشنهادی نمی‌دهد. فرامرزبان و همکاران (۱۴۰۰)، در مقاله‌ی «طراحی الگوی راهکارهای حمایت از حریم خصوصی کودکان در فضای مجازی»، به بررسی راهکارهایی که برای حمایت از حریم خصوصی کودکان در فضای مجازی وجود دارد می‌پردازد، اما در مورد قوانین و مقررات موجود در این زمینه بحثی نمی‌کند. اسماعیلی (۱۳۸۹)، در مقاله‌ی «حقوق کودک در برابر رسانه‌ها»، راجع به رسانه‌ها در جهان معاصر، ارتباط ویژه کودک و رسانه، شفاف‌سازی مبانی حقوقی و ... توضیح می‌دهد، اما تحقیق مزبور به دلیل قدمت تقریباً ده ساله‌اش، از بررسی قوانین جدیدی که در حوزه‌ی حمایت از کاربران نابالغ در فضای سایبر و محیط دیجیتال وجود دارد، خالی است.

## ۳ رعایت حقوق کودکان و نوجوانان در ارسال پیام‌های تبلیغاتی

با پیشرفت گسترده در حوزه‌های فناوری ارتباط، دوران امروز به رسانه‌ها تعلق یافته است (Age of Media) و در این زمینه اصطلاحی به نام فاصله کم‌رنگ شده و به عبارتی با «مرگ فاصله» (The Death of Distance) روبه‌رو هستیم [۵]، لذا می‌بایست اقدامات و آموزش‌های لازم برای مواجهه با چنین فضایی انجام شود. کودکان از جدی‌ترین متقاضیان و علاقه‌مندان رسانه‌های نوین هستند؛ به عبارتی هم مقتضیات زندگی ماشینی، زمینه را برای برقراری پیوند مستحکم‌تر کودک با رسانه آماده‌تر ساخته است و هم رسانه‌ها شدیداً به دنبال یافتن مخاطب در سنین پایین‌تر هستند، زیرا کودکان و نوجوانان فرصت و علاقه بیشتری برای استفاده از تولیدات رسانه‌ای در اختیار دارند و نیز میزان تأثیرپذیری آنان از رسانه‌ها به مراتب بیشتر و ماندگارتر است. هم‌چنین ارتباط افراد نابالغ برای قدرت‌های مسلط بر جهان و رسانه‌ها که در پی شکل دادن فرهنگی نو و تحول فکری نسل‌های آینده هستند، معبری مطمئن و کوتاه برای تضمین اهداف و منافع آتی به‌شمار می‌رود [۵]. از این‌رو در عصر حاضر با توجه به توسعه فضای سایبر و مجازی در زندگی، از مهم‌ترین عرصه‌هایی که باید حقوق کودک در آن حفظ و مورد توجه قرار گیرد محیط دیجیتال و فضای سایبر است. کودکان بخش گسترده‌ای از کاربران اینترنت را شامل می‌شوند. دسترسی خواسته یا نخواست‌ه کودک به اطلاعاتی که نباید بدان‌ها دسترسی داشته باشد، این قشر را در معرض انحراف و قربانی شدن قرار می‌دهد [۱۷].

التفات ویژه به ابعاد مختلف حقوق معنوی کودکان مانند القای صحیح خط فکری (بقره، آیات ۱۳۲ و ۱۳۳)، علم آموزی (آل عمران، آیه ۱۶۴) و تربیت شایسته (تحریم، آیه ۶)، از جمله موضوعات اساسی و مهمی می‌باشد که در مصحف شریف نیز بدان اشاره شده است [۱۵].

در کلام معصوم (علیه السلام) هم لزوم رعایت حقوق افراد نابالغ از حیث آنچه به او مخابره می‌شود،

مورد توجه و تأکید قرار گرفته است. همان‌طور که حضرت علی (ع)، در بخش‌هایی از نامه ۳۱ نهج البلاغه، می‌فرماید: «... قلب نونهالان همانند زمین کاشته نشده، آماده پذیرش هر بذری است که در آن پاشیده شود». و خطاب به فرزندشان امام حسن مجتبی (ع) می‌گویند: «... از آن ترسیدم که مبادا خواسته‌های نفسانی و نظریاتی که مردم را دچار اختلاف و گمراهی کرد و کار را بر آنان شبهه ناک ساخت، به سمت تو نیز هجوم آورد. گرچه آگاه کردن تو را نسبت به این امور خوش نداشتیم، اما آگاه شدن و استوار ماندن را ترجیح دادم تا دچار هلاکت‌های اجتماعی نگردی» [۲]. نکته‌ی بسیار پراهمیت در این فراز آن است که مولا علی (ع) از روبه‌رو شدن فرزند نوپای خویش با پیام‌آفرینان مغرض و امکان هجوم آنها به فضای ذهن و اندیشه [۵] فرزندشان، اظهار هراس و دلواپسی می‌کنند، یعنی در مرحله اول این دغدغه وجود دارد و باید اقدامات لازم را برای جلوگیری از آن انجام داد، اما در مرحله دوم، آنچه را که مهم‌تر از هجوم پیام‌های مضر و شبهه‌ناک می‌دانند، آگاه ساختن فرزندشان می‌باشد تا با شناخت مسیر صحیح از غلط، خود به تصمیم‌گیری درست اقدام نماید؛ چراکه گذر از لغزش‌گاه‌ها و نهادن گامی استوار در زمان بروز هلاکت‌های اجتماعی، منوط به شناخت و یادگیری صحیح و آگاهانه خواهد بود.

علاوه بر این در احادیث معصومین (علیهم السلام)، بر ضرورت توجه به تحرک، نشاط و بازی‌های کودکانه و تقدم آن بر آموزش سواد و احکام دینی سفارش شده است [۱۲]. در این زمینه و باتوجه به اینکه امروزه انجام بازی‌ها، غالباً از طریق رایانه یا ابزاری مشابه و به شکل آنلاین توسط کودکان و نوجوانان صورت می‌گیرد، نباید این قشر که هنوز بالغ نشده یا در ابتدای بلوغ خود هستند، از سوی شرکت‌ها و بنگاه‌های تبلیغاتی مورد سوءاستفاده قرار گیرند و از آنها به عنوان ابزاری برای تجارت بهره برد. به عبارتی کمی سن کودکان و نوجوانان و کامل نشدن قوه تمییز آن‌ها، نباید عاملی باشد برای تبلیغ‌کنندگان سایبری تا هرگونه تبلیغی را برای آنان ارسال کرده و اقماعشان نمایند جهت خرید کالا یا خدمات پیشنهاد شده است.

در اسناد بین‌المللی نیز به حقوق کودکان و رعایت آن به خصوص از سوی رسانه‌ها، تأکید شده است. برای مثال، یونسکو در سال ۱۹۹۹ برای حمایت از حقوق کودکان اعلامیه و طرح اقدام برای حمایت از کودکان را تصویب کرد. یونیسف در گزارش سالانه وضعیت کودکان در سال ۲۰۱۷م، از همه‌ذی‌نفعان خواسته است تا حقوق کودکان را در فضای سایبر تحقق بخشند. شورای اروپا نیز در سال ۲۰۱۸ م، به توصیه کشورهای عضو، بخشی از استراتژی خود را در مورد دستورالعمل‌های احترام، محافظت و تحقق حقوق کودک در محیط دیجیتال اختصاص داد.

به عنوان یک اصل و قاعده کلی، بند ۳ ماده ۱۰ میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی مجمع عمومی سازمان ملل متحد مصوب ۱۶ دسامبر ۱۹۶۶ میلادی<sup>۱</sup> بیان می‌دارد: «تدابیر خاص در حمایت و مساعدت به نفع کلیه‌ی اطفال غیرممیز و ممیز، بدون هیچ‌گونه تبعیض به علت نَسَب یا علل دیگر باید اتخاذ شود. اطفال غیرممیز و ممیز باید در مقابل استثمار اقتصادی و اجتماعی حمایت شوند. واداشتن اطفال به کارهایی که برای جهات اخلاقی یا سلامت آن‌ها زیان‌آور است یا زندگی آن‌ها را به مخاطره می‌اندازد یا مانع رشد طبیعی آنان می‌گردد باید به موجب قانون قابل مجازات باشد».

<sup>۱</sup> مطابق با ۲۵/۹/۱۳۴۵ هجری شمسی

یا در ماده ۱۷ کنوانسیون حقوق کودک<sup>۲</sup> (مصوب ۲۰ نوامبر ۱۹۸۹م)<sup>۳</sup> چنین آمده است: «کشورهای طرف کنوانسیون به عملکرد مهم رسانه‌های گروهی واقف بوده و دسترسی کودک را به اطلاعات و مطالب از منابع گوناگون ملی و بین‌المللی، خصوصاً مواردی که مربوط به اعتلای رفاه اجتماعی، معنوی یا اخلاقی و بهداشت جسمی و روحی وی می‌شود را تضمین می‌کنند. در این‌راستا، کشورها اقدامات ذیل را به عمل خواهند آورد:

الف. تشویق رسانه‌های گروهی به انتشار اطلاعات و مطالبی که برای کودک استفاده‌های اجتماعی و فرهنگی داشته و با روح ماده ۲۹<sup>۴</sup> نیز مطابق است.

ب. تشویق همکاری‌های بین‌المللی در جهت تولید، مبادله و انتشار این‌گونه اطلاعات و مطالب از منابع گوناگون فرهنگی، ملی و بین‌المللی.

ج. تشویق تولید و انتشار کتاب‌های کودکان.

د. تشویق رسانه‌های گروهی جهت توجه خاص به احتیاجات مربوط به آموزش زبان کودکانی که به گروه‌های اقلیت تعلق دارند یا مری هستند.

ه. تشویق توسعه خط‌مشی‌های مناسب در جهت حمایت از کودک در برابر اطلاعات و مطالبی که به سعادت وی آسیب می‌رساند با توجه به مفاد مواد ۱۳ و ۱۸».

<sup>۲</sup> در ماده یک آن منظور از کودک هر انسان کمتر از ۱۸ سال سن است، مگر آنکه قانون قابل اعمال در مورد کودک (مطابق با قانون هر کشور)، سن قانونی کمتری را تعیین کرده باشد [۹].  
<sup>۳</sup> به موجب قانون اجازه الحاق دولت جمهوری اسلامی ایران به کنوانسیون حقوق کودک مصوب ۰۱/۱۲/۱۳۷۲، ایران به این کنوانسیون پیوسته است. کنوانسیون حقوق کودک از اسناد لازم‌الاجرا و بسیار مهم مربوط به حقوق بشر است که مورد توافق جامعه بین‌المللی می‌باشد. این کنوانسیون کامل‌ترین سند مربوط به حقوق کودکان است که تاکنون تدوین شده و اولین سندی است که این حقوق را در عرصه بین‌المللی به صورت لازم‌الاجرا مطرح کرده است [سیدفاطمی، ۱۳۹۳، ۳۵۹].  
<sup>۴</sup> ماده ۲۹ کنوانسیون: (۱) کشورهای طرف کنوانسیون موافقت می‌نمایند که موارد ذیل باید جزء آموزش و پرورش کودکان باشد:

الف. پیشرفت کامل شخصیت، استعدادها و توانایی‌های ذهنی و جسمی کودکان.

ب. توسعه احترام به حقوق بشر و آزادی‌های اساسی و اصول مذکور در منشور سازمان ملل.

ج. توسعه احترام به والدین کودک، هویت فرهنگی، زبان و ارزش‌های ملی کشوری که در آن زندگی می‌کند، به موطن اصلی وی و به تمدن‌های متفاوت با تمدن وی.

د. آماده نمودن کودک برای داشتن زندگی مسئولانه در جامعه‌ای آزاد و با روحیه‌ای (مملو) از تفاهم صلح، صبر، تساوی زن و مرد و دوستی بین تمام مردم، گروه‌های قومی، مذهبی و ملی و اشخاص دیگر.

ه. توسعه احترام نسبت به محیط طبیعی.

(۲) از هیچ‌یک از بخش‌های این ماده و ماده ۲۸ نباید چنان تعبیر شود که مداخله‌ای در آزادی افراد و ارگان‌ها برای تأسیس و اداره مؤسسات آموزشی‌ای که همواره طبق اصول ذکر شده در پاراگراف ۱ ماده حاضر و با شرط ارائه آموزش مطابق با حداقل استاندارد ذکر شده توسط دولت ایجاد می‌شوند، تلقی شود. (۳) کشورهای طرف کنوانسیون همکاری‌های بین‌المللی را در موضوعات مربوط به آموزش و پرورش، خصوصاً در زمینه زدودن جهل و بیسوادی در سراسر جهان و تسهیل دسترسی به اطلاعات فنی و علمی و روش‌های مدرن آموزشی، تشویق و افزایش خواهند داد. در این ارتباط، به نیازهای کشورهای در حال توسعه توجه خاصی خواهد شد.

مفهوم صدر ماده ۱۷ کنوانسیون و بند الف آن، که اشاره به تضمین اعتلای رفاه اجتماعی، معنوی یا اخلاقی و بهداشت جسمی و روحی کودکان و نوجوانان و نیز تشویق رسانه‌های گروهی به انتشار اطلاعات و مطالب قابل استفاده اجتماعی و فرهنگی می‌کند، بدان معناست که هرگونه ارسال تبلیغ برخلاف این اصول و گزاره‌ها، ممنوع می‌باشد و باید رسانه‌ها و موسسات تبلیغاتی را از دانستن این مهم آگاه نمود و بیش از آنکه مقرراتی وضع شود تا احتیاط‌های لازم در ارسال تبلیغات و پیغام‌های نامناسب برای کودکان و نوجوانان مورد لحاظ قرار گیرد (و به عبارتی راه‌گریز ارائه و پیش‌بینی کرد)، باید اقدام به وضع و تدوین قوانینی نمود تا فرستادن این‌گونه از پیام‌ها و تبلیغات را منع کند و جنبه و ماهیت بازدارنده داشته باشد.

علاوه بر این، در حقوق داخلی کشورها نیز به صیانت از حقوق افراد نابالغ در ارسال پیام‌های تبلیغاتی از طریق عرصه فضای سایبر، توجه شده است و قوانین خود را با لحاظ این مهم تدوین کرده‌اند. برای نمونه در آلمان، طبق آیین‌نامه توافقی اپراتورهای همراه این کشور، اپراتورهای موبایل موظف می‌شوند که دسترسی به مطالب غیرقانونی را محدود کنند و با تعبیه ابزارها و نظام‌های شناسایی، برخورد نکردن کاربران زیر سن قانونی با مطالب پورنوگرافی را تضمین نمایند و یا در آمریکا، همزمان با تصویب قانون کویا در سال ۱۹۹۸م، قانون حفاظت از حریم شخصی کودکان به عنوان یک قانون فدرال ایالات متحده تصویب شد و اجرای آن از آوریل ۲۰۰۰م با قوت پیگیری شد. براین اساس اطلاعات شخصی کودکان زیر ۱۳ سال باید مورد حفاظت قرار گرفته و کسی حق اطلاع یا فروش آن‌ها را ندارد. اگر یک پایگاه یا ارائه‌کننده خدمات به این اطلاعات نیاز داشته باشد باید رضایت والد یا سرپرست کودک را اخذ کند. طبق این قانون، کودکان زیر ۱۳ سال می‌توانند به‌طور قانونی اطلاعات شخصی خود را با اجازه والدین خود ارائه دهند اما بسیاری از وبسایت‌ها، اجازه نمی‌دهند که کودکان زیر سن قانونی از خدمات آنها استفاده کنند [۳].

تبلیغاتی که در فضای سایبر صورت می‌گیرد، در خصوص محصولاتی که تابع قوانین خاصی می‌باشند و یا محصولات ممنوعه برای برخی از سنین، مانند سیگار و دیگر محصولاتی که مصرف آن‌ها موجب اعتیاد می‌شود، و یا محصولات خوردنی و نوشیدنی‌ای است که حاوی مقادیر زیادی چربی، شکر و نمک می‌باشد [۲۳]، که می‌توانند سبب چاقی کودک شود، نگرانی‌ها در خصوص چنین تبلیغاتی که سبب زندگی پرخطر را کم اهمیت جلوه می‌دهد و کودکان را به تهیه‌کنندگان آنلاین وصل می‌کند، افزایش می‌دهد. ترویج و فروش محصولات غیرقانونی مانند مواد مخدر و ملزومات دوپینگ در اینترنت سبب خطرات ابتدایی بر نوجوانان می‌شود. مارکتینگ آنلاین که کودکان را هدف قرار می‌دهد و یا بر روی سایت‌هایی نمایش داده می‌شود که کودکان به‌طور رایج به آن‌ها مراجعه می‌کنند، در حالی که اختلاف و تمایزی میان محتوا و تبلیغات وجود ندارد، مشکل‌آفرین است [۱۷].

بنابراین و باتوجه به ویژگی بدون مرز و ناملموس بودن فضای سایبر، که موجب می‌شود اولیا از نقض حریم خصوصی اطلاعاتی و ارتباطی کودک خود و به تبع آن از نیازهای تربیتی وی غافل بمانند [۴] و نیز با عنایت به حیاتی بودن حفاظت از کرامت، امنیت و حریم خصوصی کودکان و نوجوانان در اینترنت [۲۴]، ضروری است تا حقوق کاربران نابالغ در هنگام ارسال تبلیغات در فضای سایبر، مورد توجه ویژه قرار گیرد و بنگاه‌های تبلیغاتی را ملزم نمود تا از فرستادن برخی تبلیغات و پیشنهادات خرید، برای این قشر خودداری کنند، نه آنکه راه‌های احتیاطی در ارسال چنین تبلیغاتی مانند اخذ اطلاعات سنی فرد یا رضایت والدین او،

در پیش گرفته شود؛ زیرا دور زدن این گونه از مقدمات، امری ساده و امکان‌پذیر می‌باشد.

## ۴ قوانین و مقررات تبلیغاتی ایران در جهت حمایت از کاربران نابالغ

در حقوق ایران، بخش‌هایی از برخی قوانین به مقررات تبلیغ و مسائل مربوط به آن اختصاص یافته است. از جمله مهم‌ترین و اولین قوانین پس از انقلاب که در نظام حقوقی ایران، اصول و مقررات ناظر بر تبلیغات تجاری را بیان کرده است، آیین‌نامه تأسیس و نظارت بر نحوه کار و فعالیت کانون‌های آگهی و تبلیغاتی، مصوب ۱۳۵۸ شورای انقلاب می‌باشد. این آیین‌نامه به پیشنهاد وزارت ارشاد ملی وقت به استناد ماده ۶ قانون تأسیس وزارت اطلاعات و جهانگردی سابق در جلسه مورخ ۲۷ اسفندماه ۱۳۵۸ شورای انقلاب به تصویب رسیده است. این مصوبه از لحاظ شمول موضوعی کاملاً عام بوده و همه رسانه‌ها را در برمی‌گیرد. در ماده ۱۵ چنین آمده است که: «آگهی‌های تبلیغاتی که از طریق رسانه‌های همگانی (رادیو، تلویزیون، سینما، روزنامه، مجله، سال‌نامه ویزیتوری و مانند آن) پخش می‌شود، تابع مقررات این آیین‌نامه است». آیین‌نامه مزبور با قرار دادن نام رسانه<sup>۵</sup> در پرانتز و افزودن قید «و مانند آن»، هیچ نوع تبلیغ عمومی تجاری را از دایره شمول خود خارج ندیده است [۱۸]. هرچند در ماده ۱۲ این آیین‌نامه رعایت نکاتی راجع به تنظیم آگهی‌های تبلیغاتی بیان شده است، اما نمی‌توان به موردی اشاره نمود که در حمایت از کودکان در تبلیغات تجاری و از جمله در محیط دیجیتال، سخنی به میان آورده باشد و گزاره‌های مربوط به تبلیغات سایبری برای این گروه را ترسیم نموده باشد. راجع به قواعد تبلیغ در مواد ۵۰ الی ۵۷ قانون تجارت الکترونیکی، مقرراتی در مورد تبلیغات تجاری آمده است. مواردی که در مقررات حمایتی قانون تجارت الکترونیک، طی مواد مذکور در نظر گرفته شده است، عبارتند از:

۱. **روشن بودن عنوان تبلیغات.** این مهم بدان جهت است که گاهی بین تبلیغات بازرگانی با دادن اطلاعات علمی و یا با توصیه‌های کارشناسی برای استفاده از کالا یا خدمات، تفاوت وجود دارد و به طور معمول، کاربران اینترنتی در مقابل هریک واکنش و موضع‌گیری متفاوتی نشان می‌دهند.
۲. **مشخص بودن ذی‌نفع.** ماده ۵۳ ق.ت.ا در این مورد بیان می‌دارد: «در تبلیغات و بازاریابی باید هویت شخص یا بنگاهی که تبلیغات به نفع اوست روشن و صریح باشد». زمانی که مصرف‌کننده از طریق اینترنت در نتیجه تبلیغات، کالا یا خدماتی را می‌خرد، باید از هویت تبلیغ‌کننده که می‌تواند تاجر یا واسطه باشد، هم‌چنین از محل کسب و بنگاه وی آگاه باشد تا بتواند در صورت عدم دریافت کالا یا خدمات، عدم رضایت از کالا یا خدمات عرضه‌شده و یا ورود صدمات در نتیجه مصرف کالا یا خدمات، علیه تبلیغ‌کننده یا تأمین‌کننده اقدامات حقوقی و قضائی لازم را انجام دهد [۱۱]. آشکار است که

<sup>۵</sup> رسانه در بند ۵ ماده یک پیش‌نویس آیین‌نامه اجرایی مواد ۵۶ و ۵۷ قانون تجارت الکترونیکی این‌گونه تعریف شده است: «ابزاری است که پیام تبلیغاتی را در بستر الکترونیکی به مخاطبان منتقل می‌کند. مانند: وب سایت‌ها، اپلیکیشن‌ها، شبکه‌های اجتماعی و سایر».



نام تجاری اشخاص (اعم از حقیقی و حقوقی)، موجب خاطر جمعی و اطمینان مشتریان می‌شود و مشخص نبودن نام آن‌ها، عاملی است برای عدم اطمینان مشتریان و کاربران اینترنت.

۳. **مشخص بودن جهات تبلیغ.** معمولاً تبلیغات برای ایجاد انگیزه‌ی مشتریان صورت می‌گیرد، لذا باید جهات تبلیغ، به طور مشخص و شفاف، معلوم شود.

۴. **ممنوعیت تبلیغات زیان‌آور.** در این مورد ماده ۵۱ ق.ت.ا می‌گوید: «تأمین‌کنندگانی که برای فروش کالا و خدمات خود تبلیغ می‌کنند نباید سلامتی افراد را به خطر اندازند». در استنباط این ماده باید اذعان داشت که تبلیغات کالاها یا خدمات و نحوه استفاده از آن‌ها، می‌بایست به گونه‌ای باشد که احتمال خطر را برای استفاده‌کننده یا اشخاص ثالث، منتفی کند و اطمینان دهد که هیچ‌گونه ضرر و آسیبی به کاربران، در صورت استفاده و به کارگیری کالا و خدمات، وارد نخواهد شد.

۵. **محدودیت تبلیغات ناخواسته.** طبق ماده ۵۵ ق.ت.ا «تأمین‌کنندگان باید تمهیداتی را برای مصرف‌کنندگان در نظر بگیرند تا آنان راجع به دریافت تبلیغات به نشانی پستی و یا پست الکترونیکی خود تصمیم بگیرند». ارسال پیام‌های تبلیغاتی ناخواسته مجاز نیست و لازم است با رضایت دریافت‌کننده صورت گیرد. چنین پیام‌هایی موجب مسئولیت ارسال‌کنندگان و حتی ارائه‌کنندگان خدمات اینترنتی است و از این‌رو دریافت‌کنندگان پیام‌ها حق دارند علیه هر دوی آن‌ها دعوی حقوقی و کیفری طرح کنند [۱۳]. ماده ۷ دستورالعمل تجارت الکترونیک اروپا نیز، اولاً ارسال‌کننده پیام‌های ناخواسته را موظف به رعایت ترتیبی کرده که گیرنده حتی اگر آن را باز نکند، بتواند متوجه محتوا و ماهیت تبلیغی پیام شود و چنانچه مایل به باز نکردن یا حذف آن‌ها باشد، به راحتی این کار را انجام دهد و ثانیاً، ارسال پیام‌های ناخواسته تجاری را منوط به اقدام قبلی برای احراز رضایت‌کننده کرده است. از جمله روش‌های اجرایی برای این ترتیب آن است که اگر مخاطب در فهرست ملی یا بین‌المللی منصرفین از دریافت اسپم (Opt – Out List) نام‌نویسی کرده باشد، ارسال‌کنندگان می‌توانند قبل از هر ارسال به آن فهرست مراجعه و از ارسال پیام ناخواسته خودداری کنند؛ روشن است که این تنها یک روش است و مخاطبان تکلیفی به نام‌نویسی در فهرست مزبور ندارند و عدم نام‌نویسی آنان، رافع مسئولیت ارسال‌کنندگان نخواهد بود. با عنایت به این خلاء قانونی، ماده ۱۳ دستورالعمل ۵۸/۲۰۰۲ جامعه اروپا، در خصوص پردازش داده‌های شخصی و حمایت از حریم خصوصی در بخش ارتباطات الکترونیکی، تفصیل بیشتری به مطالب داده است و مقرر می‌دارد:

- ۱- استفاده از سامانه‌های تماس خودکار بدون دخالت انسان، نمابر، یا رایانامه به منظور ارزیابی مستقیم، تنها هنگامی مجاز است که دریافت‌کننده رضایت قبلی خود را اعلام کرده باشد.
- ۲- علی‌رغم بند ۱، وقتی شخصی از مشتری خود نشانی الکترونیکی وی را در جریان معامله دریافت می‌کند، حق دارد از آن نشانی برای کالا یا خدمات خودش که مشابه مورد معامله باشد استفاده نماید، منوط به آنکه به طور واضح امکان اعتراض بدون هزینه و آسان را به مشتری بدهد. این امر نیز در صورتی مجاز است که وی از ابتدا از چنین استفاده‌ای احراز نکرده باشد.



• ۳- به هر حال، ارسال رایانامه به منظور بازاریابی مستقیم با نام مبذل یا پنهان کاری در هويت ارسال کننده یا ذی نفع پیام، یا بدون نشانی صحیحی که دریافت کننده بتواند درخواست توقف ارسال را بنماید، ممنوع است.

بندهای ۱ و ۳ در مورد مخاطبان حقیقی اعمال می شود ولی کشورهای عضو باید منافع مشروع سایر اشخاص را نیز ملحوظ نمایند» [به نقل از: [۱۳]].

۶. ممنوعیت فریب تبلیغاتی. این قاعده در ماده ۵۰ ق.ت.ا آمده است: «تأمین کنندگان در تبلیغ کالا و خدمات خود نباید مرتکب فعل یا ترک فعلی شوند که سبب مشتبه شدن و یا فریب مخاطب از حیث کمیت و کیفیت شود». به نظر می رسد ماده اخیر، از دستورالعمل ۱۱۴/۲۰۰۶ اروپا اتخاذ شده باشد. ضمن آنکه با مقررات تدلیس در قانون مدنی مطابقت دارد؛ با این تفاوت که نقض این مقررات به موجب مبحث سوم ق.ت.ا، جنبه کیفری نیز دارد [۱۳]. ماده مزبور، دو ممنوعیت را در تبلیغات تذکر می دهد:

الف. تبلیغ کالا و خدمات، نباید به گونه ای باشد که موجب اشتباه گرفتن آن ها با کالا یا خدمات مشابه شود.

ب. تبلیغ نباید مشتری را از حیث کمیت و کیفیت فریب دهد و مثلاً وصفی از اوصاف کالا که در آن وجود ندارد، از سوی تاجر توصیف شود [۱۱].

۷. توجه به مخاطبین خاص (کاربران نابالغ). به موجب ماده ۵ ق.ت.ا، تبلیغ و بازاریابی برای کودکان و نوجوانان زیر سن قانونی به موجب آیین نامه ای است که در ماده ۷۹ این قانون خواهد آمد. هر چند پیش نویس این آیین نامه تنظیم شده است، اما هنوز تصویب و مورد تأیید قرار نگرفته است. ماده ۱۸ آن در حمایت از حقوق کاربران نابالغ مقرر می دارد: «رسانه ها موظف هستند از ثبت اطلاعات کودکان و نوجوانان بدون اجازه والدین جلوگیری کنند، زیرا ممکن است این اطلاعات مورد سوء استفاده در جهت ارسال تبلیغات نامناسب برای کودکان و نوجوانان قرار گیرد». علاوه بر این بخش سوم پیش نویس آیین نامه به مقررات مربوط به کودکان اختصاص یافته (مواد ۲۰ تا ۳۰). برای مثال در تبصره ۳ ماده ۲۱ آمده است: «در تبلیغات برای کودکان، باید به وضوح گروه سنی کودکانی که می توانند از محصول استفاده کنند، درج گردد». این راه کارها هر چند در جهت حمایت از کودکان و نوجوان مفید است، اما کافی نیست. توضیح آنکه چنین مقرراتی، صرفاً جنبه ی پیش گیرانه دارند و صراحتاً سازندگان، صاحبان و بنگاه های تبلیغاتی را در ارسال برخی از تبلیغات نامناسب و غیر لازم برای کاربران نابالغ، نهی نکرده است و همین امر موجب می شود تا امکان فرستادن چنین تبلیغاتی در چهارچوب مقررات قانون وجود داشته باشد و به گونه ای کودکان و نوجوانان را آگاه به وجود آنها نماید و عاملی باشد تا این قشر به طریقی هر چند غیرقانونی به محتوای این تبلیغات دست یابند. البته ماده ۳۰ پیش نویس مزبور، تبلیغاتی که شامل غذاهای ناسالم باشد را برای کودکان ممنوع اعلام کرده است، ولی همان طور

که مشخص می‌باشد، این ماده محدود به بعضی از تبلیغات خوراکی شده و از منع پیشنهاد و فرستادن سایر تبلیغات مضر و غیرلازم سخنی به میان نیاورده است. از این رو ضروری می‌باشد تا قبل از تصویب نهایی آیین نامه و به اجرا در آمدن آن، چنین امر مهمی مدنظر تدوین کنندگان قرار گیرد و آیین نامه را در زمینه‌ی مزبور اصلاح نمایند. هم‌چنین بسیاری از مواد بخش سوم پیش‌نویس آیین نامه مواد ۵۶ و ۵۷ قانون تجارت الکترونیک، با اصول ۶۴ تا ۸۱ مجموعه ضوابط تولید آگهی‌های رادیویی و تلویزیونی یکسان است و در محتوا با یکدیگر شباهت دارند و این تکرار و دوباره کاری، زینده‌ی مجموعه قانونی کشور نیست و جالب آنکه در اصول مجموعه‌ی مزبور نیز، به نهی از ارسال برخی تبلیغات که بدان اشاره شد، توجهی نشده است.

علاوه بر قوانین و مقررات مذکور، فصل دوم قانون حمایت از مصرف کنندگان مصوب ۱۳۸۸ به طور کلی به بیان وظایف عرضه‌کنندگان کالاها و خدمات در قبال حقوق مصرف کنندگان اختصاص داده شده است. یکی از این وظایفی که در ماده هفت آمده، ممنوعیت پخش تبلیغات خلاف واقع و ارائه اطلاعات نادرست به مصرف کننده از جمله از طریق وسایل ارتباط جمعی است (مشابه با مضمون ماده ۵۰ ق.ت.ا) و بیشتر از آن وارد جزئیات تبلیغات گمراه کننده نشده است. اما در این قانون نیز و آیین نامه اجرایی ماده ۷ آن مصوب ۱۳۹۰، حمایت خاص و ویژه‌ای از حقوق کودکان در تبلیغات تجاری از جمله در محیط دیجیتال به عمل نیامده است. حتی در دستورالعمل ساماندهی تبلیغات در فضای مجازی مصوب ۱۳۹۹ هم در خصوص حقوق کودکان در تبلیغات تجاری در محیط دیجیتال اشاره‌ای نشده است.

## ۵ لزوم بازنگری و اصلاح مقررات تبلیغاتی، با ملاحظه‌ی حقوق کودکان و نوجوانان

اینترنت و به‌طور کلی ابزار ایجادکننده ارتباطات آنلاین، با سهولتی باورنکردنی دنیایی از اطلاعات و الفانات را پیش چشم کودکان و نوجوانان نمودار ساخته و امکان ارتباط آن‌ها را با جهان فراهم می‌سازد. آن‌ها اینترنت را به عنوان ابزاری برای یادگیری، برقراری ارتباط، به اشتراک گذاری اطلاعات و مشارکت در زندگی اجتماعی به کار می‌گیرند. استفاده از اینترنت در کنار فضایی که برای خودباوری و پیشرفت آنان ایجاد می‌کند، چالش‌های زیادی را در حوزه‌های مختلف ایجاد کند [۱۴]. این ارتباط سریع و آسان، کنترل و نظارت والدین را که، لازمه شناخت کودک و نوجوان و یافته‌های او به عنوان اولین سنگ بنای تربیت است، با چالش روبه‌رو می‌سازد [۱۷]. اما چنین امری برای والدین توجیه‌پذیر نیست تا در پرورش و نظارت بر فرزندانشان کم کاری کنند. کما اینکه طبق دیدگاه شرعی و فقهی، ولی و سرپرست کودک حق انجام اقدامات مغایر با منافع و مصالح کودک را ندارد [۱۹]، [۲۱]. از این رو و به قیاس اولویت، سایر اشخاص (اعم از حقیقی و حقوقی) نیز نمی‌توانند خواسته یا ناخواسته و یا به طرق مختلف، دست به اقداماتی زنند که خلاف حقوق مسلم کودکان و نوجوانان باشد. بر این اساس انجام هرگونه اقدام تجاری که برای کودک آثار زیان‌بار به همراه داشته باشد، جایز نیست و این مهم در خصوص استفاده تبلیغاتی از کودکان در محیط دیجیتال و فضای سایبر نیز مصداق دارد [۱۷]. یونیسف اصولی را برای رعایت حقوق کاربران نابالغ در فضای مجازی، مقرر نموده است که عبارتند از:

۱. کودکان حق محافظت از حریم خصوصی و داده‌های شخصی‌شان را دارند.
۲. کودکان حق آزادی بیان و دسترسی به اطلاعات از منابع مختلف را دارند.
۳. کودکان حق دارند در معرض مسائلی که آوازه‌شان را خدشه‌دار می‌کند، قرار نگیرند.
۴. حق حریم خصوصی و آزادی بیان کودکان باید مطابق با رشد توانایی‌های آنان محافظت شود.
۵. کودکان حق دارند در مقابل خشونت و سوءاستفاده از حق حریم خصوصی و آزادی بیان و خدشه‌دار شدن آوازه‌شان، به راه‌های جبران خسارت دسترسی داشته باشند [۲۷].

موارد ۳ و ۴ از اصول مزبور، صراحتاً بیانگر آن است که ارسال برخی از تبلیغات نامناسب و مغایر با حقوق، رشد و توانایی کودکان و نوجوان از سوی بنگاه‌ها و ارسال‌کنندگان پیام‌های تبلیغاتی در فضای سایبر ممنوع خواهد بود و به عبارتی اتمام حجتی است در منع به‌کارگیری سایر روش‌هایی که در حال امکان دور زدن آن‌ها و دستیابی به چنین تبلیغاتی را فراهم می‌سازد (مانند اخذ رضایت والدین و ...). به‌کارگیری این اصول در وضع قوانین مربوط به جزئیات حفظ حقوق حریم خصوصی کودکان و نوجوانان، می‌تواند از به‌اشتراک‌گذاری داده‌های مربوط به حریم خصوصی کودکان توسط خود او، والدین یا اطرافیان وی جلوگیری کند و راهنمایی باشد برای طراحان پلتفرم‌های اینترنتی در خصوص چگونگی طراحی نرم‌افزارها، برای کاهش آسیب به کاربران نابالغ و اخذ کمترین میزان از اطلاعات شخصی آنان [۱۴].

باتوجه به آنچه بیان شد، واقعیت امر این است که نظام حقوقی ایران، در نظام‌دهی تبلیغات تجاری به طور کلی فاقد وضعیتی مطلوب است و قانون جامع و کاملی در زمینه‌ی حمایت از حقوق کودکان و نوجوانان در تبلیغات تجاری و به خصوص در محیط دیجیتال وجود ندارد [۱۷] و یا همان قوانین و آیین‌نامه‌های موجود نیز که بعضاً در مقرراتشان به رعایت حقوق کودک و نوجوان تأکید شده است، از نقص‌های اساسی برخوردار می‌باشند. لذا در ممنوعیت ارسال برخی از تبلیغات غیرلازم، نامناسب و در مواردی مضر برای کاربران نابالغ که در فضای سایبر صورت می‌گیرد، این دسته از قوانین و مقررات باید هرچه سریع‌تر اصلاح شده و مورد بازنگری قرار گیرند. در این مسیر می‌توان از کنوانسیون‌ها، اسناد بین‌المللی، قوانین و تجربه‌ی موفق سایر کشورها استمداد جست تا زودتر به مقصود نهایی نائل آمد.

## ۶ نتیجه‌گیری

توسعه‌ی اینترنت و پیشرفت ابزارهای دیجیتال، در فعالیت‌های کودکان و نوجوانان نیز تأثیر به‌سزایی گذاشته است و در این مسیر بدون هیچ شک و تردیدی، نمی‌توان امتیازات و کارکردهای مثبت رسانه‌ها را نادیده گرفت. با در اختیار داشتن وسایل الکترونیکی، روزانه پیام‌های تبلیغاتی مختلفی از طریق فضای سایبر به آن‌ها ارسال می‌شود که محتوای برخی از پیشنهادات تبلیغی برای چنین قشری مناسب نبوده و حتی بعضی از آن پیام‌ها برای کاربران نابالغ اصلاً لازم نیست؛ لذا باید به دنبال سازوکارهایی بود تا در عین پذیرش و قبول رسانه‌های نوین الکترونیکی، از دغدغه‌ها و نگرانی‌های موجود در این زمینه کاست. همان‌طور که در

متن مقاله بدان پرداخته شد، در حقوق ایران قوانین و آیین‌نامه‌هایی به طور پراکنده در زمینه تبلیغات و مسائل مربوط به آن وجود دارد که بعضاً در مقرراتشان به رعایت حقوق کودک و نوجوان هنگام تنظیم و ارسال این‌گونه پیام‌ها توجه شده است. برای رعایت این مهم پیشهادتی مانند تربیت شایسته تولیدکنندگان متعهد برای رسانه‌ها و آموزش آنان در این زمینه، تقویت نظارت در نهادهای دولتی، تهیه نظام‌نامه اخلاق حرفه‌ای ارتباطات و نهادینه‌سازی آن، تدوین راهنمای کاربردی در زمینه حقوق و روان‌شناسی کودک و ... به عمل آمده است. هرچند توصیه‌ها و راهکارهای مزبور، مفید می‌باشند، اما تا زمانی که مقررات الزام‌آور و دارای ضمانت‌اجراهی مؤثری در این زمینه نباشد، نمی‌توان به مقصود نهایی که همان رعایت حقوق کودکان و نوجوانان و عدم آسیب به رشد و توانایی‌های آن‌ها در فضای مجازی است، نائل آمد.

از آنجا که مبانی دینی و فرهنگ ایرانی - اسلامی حاکم بر کشورمان در بردارنده والاترین نگاه‌ها در حفظ و پاسداشت حقوق کودکان و نوجوانان است، لذا زبینه و قابل پذیرش نخواهد بود تا قوانین موجود در زمینه تبلیغات، فاقد قواعد الزام‌آور حقوقی برای راهنمایی رسانه‌ها و بنگاه‌های تبلیغاتی در تولید محصولات مربوط به این قشر از افراد باشد. براین اساس باید در ارسال تبلیغات از طریق فضاهای مجازی و سایبری، بازاریاب‌ها و بنگاه‌های تبلیغاتی، اقدام به مخاطب‌شناسی نمایند و در جهت ترویج امنیت محیط دیجیتال برای کودکان و نوجوانان، چنانچه پیام به واسطه‌ی داشتن شماره‌ی همراه یا آدرس و شناسه‌ی الکترونیکی شخص فرستاده می‌شود، حتماً رده‌ی سنی مخاطبین تبلیغ در نظر گرفته شود و آن دسته از تبلیغات مغایر با رشد و توانایی کاربران نابالغ، به هیچ عنوان برای آنها ارسال نگردد. از این‌رو ضروری است تا مقرره‌ای با مضمون جمله زیر به آیین‌نامه اجرایی مواد ۵۶ و ۵۷ قانون تجارت الکترونیکی اضافه شود:

ارسال آن دسته از پیام‌های تبلیغاتی در فضای سایبر و محیط دیجیتال که از حیث متن یا تصویر، نامناسب و مغایر با رشد و توانایی کاربران کودک و نوجوان است، ممنوع می‌باشد و چنانچه صاحبان تبلیغ و بازاریاب‌ها در این زمینه تخلف نمایند، مسئولیت کیفری و مدنی خواهند داشت.

## مراجع

- [۱] قرآن کریم.
- [۲] نهج‌البلاغه، (ترجمه م. دشتی). تهران: نشرامین، نامه ۳۱.
- [۳] ابوالقاسمی، ملیحه. «قوانین حقوق کودکان در فضای مجازی در کشورها / مسئولیت محافظت از کودکان با چه نهادی است؟» <https://snn.ir/fa/news/916716>، ۱۳۹۹.
- [۴] اسدی، لیلاسادات. «حریم خصوصی کودک و حق والدین بر تربیت». فقه و حقوق خانواده، ۱۴(۵۰)، ۱۳۸۸، ص ۳۵.
- [۵] اسماعیلی، محسن. «حقوق کودک در برابر رسانه‌ها»، خانواده پژوهی، ۶(۱)، ۱۳۸۹، ص ۱۱۸، ۱۱۹ و ۱۲۳.
- [۶] السان، مصطفی. حقوق فضای مجازی، چاپ دهم، تهران، انتشارات شهر دانش، ۱۳۹۸.
- [۷] انصاری، باقر، حقوق رسانه، چاپ نهم، تهران، انتشارات سمت، ۱۳۹۰.

- [۸] بارزمن، رابرت. «مستهجن نگاری کودکان در اینترنت: اسطوره، حقیقت و نظارت اجتماعی»، looksmart.com، ۲۰۰۶.
- [۹] پیوندی، غلامرضا. حقوق کودک، تهران: پژوهشگاه فرهنگ و اندیشه اسلامی، ۱۳۹۰، ص ۴۲.
- [۱۰] حبیب‌الهی، مجتبی؛ حسینی، سیدبشیر؛ شاکری‌نژاد، محسن و حاتمی، محمد. «وضعیت قوانین تبلیغات تلویزیونی برای کودکان در ایران»، پژوهش‌های ارتباطی، ۲۹(۱۰۹)، ۱۴۰۱.
- [۱۱] زرکلام، ستار. حقوق تجارت الکترونیک؛ همراه با تحلیل قانون تجارت الکترونیکی ایران، چاپ چهارم، تهران: شهردانش، ۱۳۹۶، ص ۶۵، ۶۶ و ۷۰.
- [۱۲] شیخ حر عاملی، وسائل الشیعه، چاپ ششم، جلد ۱۲، تهران: کتابفروشی اسلامی، ۱۳۶۷، ص ۷۲۲.
- [۱۳] صادقی نشاط، امیر. حقوق تجارت الکترونیک، چاپ اول، تهران: جنگل، ۱۳۹۴، ص ۱۴۶ و ۱۴۸ و ۱۴۹ و ۱۴۵.
- [۱۴] فرامرزیانی، پروانه؛ انصاری، باقر؛ سلطانی‌فر، محمد و مظفری، افسانه. «طراحی الگوی راهکارهای حمایت از حریم خصوصی کودکان در فضای مجازی»، پژوهش‌های ارتباطی، ۲۸(۱۰۶)، ۱۴۰۰، ص ۱۰-۲۱.
- [۱۵] کریمی‌نیا، محمد مهدی. حکیمی، نجیب‌الله، «بررسی تطبیقی حمایت از حقوق کودک در قرآن و حقوق بشر»، فصل‌نامه علمی - تخصصی فقه و حقوق معاصر سال پنجم، شماره دهم، صفحات ۶ تا ۳۴، ۱۳۹۸، ص ۲۹ و ۳۰.
- [۱۶] محمدی، م. اخلاق رسانه‌ها، تهران: انتشارات نقش و نگار، ۱۳۷۹.
- [۱۷] مظلوم زاده، آمنه؛ جمال زاده، عبدالرضا و شهابی، رقیه. «اصول مرتبط با حقوق کودک در محیط دیجیتال» فصلنامه علمی مطالعات فقه اقتصادی، ویژه‌نامه جستارهای نوین فقه و حقوق ۱۴۰۰، شماره ۳، ۳۵-۵۶، ۱۴۰۰، ص ۳۷، ۴۷، ۴۹، ۵۲.
- [۱۸] معتمدنژاد، کاظم. حقوق تبلیغات بازرگانی، چاپ اول، تهران، نشر دفتر مطالعات و توسعه رسانه‌ها، ۱۳۸۸، ص ۸۴.
- [۱۹] مقدس اردبیلی، احمد بن محمد، مجمع الفائده و البرهان فی شرح إرشاد ألدهان، جلد نهم و چهاردهم، قم، دفتر انتشارات اسلامی وابسته به جامعه مدرسین حوزه علمیه قم، ۱۴۰۳، ص ۴۶۴.
- [۲۰] نورائی، یوسف و نوری، نعمت. «بررسی جرم سایبری «پورنوگرافی» با تاکید بر قانون مجازات اسلامی مصوب ۱۳۹۲»، نشریه فقه، حقوق و علوم جزا، ۱۷۸-۱۸۷، ۱۳۹۵.
- [۲۱] نجفی، محمد حسن، جواهر الکالم فی شرح شرایع الاسلام، جلد چهل و یکم، تهران، نشر دارالکتب الاسلامیه، ۱۳۹۵، ص ۴۴۸.
- [22] POUDooley, J.J; Cross D; Hearn L; & Treyvaud, R. Review of existing Australian, 2009.
- [23] Fielder, A; Gardner, W; Nairn, A; & Pitt, J. "Fair game? Assessing commercial activity on children's favourite Web sites and online environments," 2007, p. 11.
- [24] Livingstone, S. Oneill. "children right's online: challenges dilemmas and emerging directions," 2014.
- [25] Livingstone, S.; Stoilove, M.; & Nandagiri, R. "Children's Data and Privacy Online," Growing up in a Digital age, Media and Communication, 2018.
- [26] Steeves, V.; & Regan, P. "Young People online and The Social Value of Privacy," Journal of In formation, Communication and Ethics in Socialy, 12(4), 2014.
- [27] United Nations Childrens Fund. "United Nations Childrens Fund Industry Toolkit," Childrens Online Privacy and Freedom of Expression, 2018. p. 8.





## ارزیابی ناامنی سایبری در منطقه خاورمیانه و پاسخ دولت‌ها

سید حامد حسینی<sup>۱</sup>

<sup>۱</sup> دانشجوی دکتری روابط بین‌الملل، دانشگاه گیلان، رشت، ایران  
hamedhoseini@ut.ac.ir

### چکیده

تهدیدات سایبری یک پدیده جهانی است که با وجود پیشرفت در فناوری‌ها و عملکرد امنیت سایبری، به طور مداوم در حال پیچیده‌تر شدن و تأثیرگذاری بیشتر است. مسائل امنیت سایبری وابسته به عوامل چندوجهی گوناگونی هستند: وابستگی فزاینده به فناوری اطلاعات برای عملکردهای گوناگون، ویژگی‌های رفتار بازیگران سیاسی که منجر به منازعه و جنگ می‌شود و آسیب‌پذیری‌های فناوری اطلاعات که باعث اختلال در عملکرد می‌شوند. در این مقاله به این سؤال اساسی پرداخته می‌شود: با توجه به منابع اصلی ناامنی سایبری در منطقه دولت‌ها چگونه به این چالش پاسخ داده‌اند؟ این مقاله در ابتدا طیفی از عوامل تهدید سایبری را در داخل و خارج از منطقه و همچنین عوامل ساختاری که باعث ناامنی سایبری می‌شوند را برجسته می‌کند. در ادامه به پاسخ‌های دولتی پرداخته می‌شود که به نوبه خود طیفی از واکنش‌ها را در بر می‌گیرد. این نوشتار با تکیه بر رویکرد واقع‌گرایی و روش توصیفی-تحلیلی به دنبال اثبات این فرضیه است که دولت‌های منطقه به عنوان بازیگران اصلی، پاسخ‌های متفاوتی به ناامنی سایبری داده‌اند. در سطح ملی، برخی دولت‌ها به دنبال افزایش ظرفیت امنیت سایبری بوده‌اند و تغییرات مهم نهادی و اداری همچون دفاع دیجیتالی و ادغام در قابلیت‌های نظامی را در اولویت خود قرار داده‌اند. در سطح بین‌الملل نیز برخی از کشورهای منطقه در مذاکرات پیرامون هنجارهای سایبری بین‌الملل شرکت کرده‌اند، در حالی که برخی دیگر از بازیگران منطقه‌ای خارج از این روند هستند. نتایج این مقاله مبتنی بر چند توصیه در سطح سیاست‌گذاری ملی و نیز بر اساس تغییرات سایبری در منطقه استوار است.

**کلمات کلیدی:** امنیت سایبری، واقع‌گرایی، خاورمیانه، تهدید، دولت.

### ۱ مقدمه

ما در عصری از فناوری‌های پیچیده‌تر و پشتیبانی از تغییرات گسترده‌تر زندگی می‌کنیم. انقلاب صنعتی چهارم فرصت‌های اقتصادی و اجتماعی عظیمی را برای مردم، سازمان‌ها و دولت‌ها به ارمغان آورده است. افزایش قابل توجه اتصال به اینترنت، رشد بالای تعداد دستگاه‌های متصل به شبکه و استفاده سریع از فناوری‌هایی مانند محاسبات ابری، روباتیک پیشرفته و هوش مصنوعی اساساً زندگی مردم را تغییر داده است. آن‌ها همچنین شیوه تجارت سازمان‌ها و نحوه ارائه خدمات دولتی و تعامل با شهروندان را تغییر می‌دهند.

در عین حال، با هر سیستم یا دستگاه جدیدی که به اینترنت متصل است، دامنه آسیب‌های سایبری و پیامدهای حملات موفقیت‌آمیز افزایش می‌یابد. همان‌طور که مهاجمان سایبری در عملیات خود پیچیده‌تر می‌شوند، سیاست‌گذاران نیز در تلاش‌اند تا واکنش‌های مناسب را ارائه دهند.

فضای سایبری به‌عنوان محیطی برای تعامل دولت‌ها، پیامدهای عمیقی برای امنیت بین‌المللی ایجاد کرده است. از یک‌سو، فضای سایبری فرصت‌هایی را برای کشورها فراهم کرده است تا در زمینه همکاری‌های نظامی و اطلاعاتی همکاری مؤثرتری داشته باشند. از سوی دیگر، رواج فضای سایبری باعث ایجاد تهدیدات منحصربه‌فردی شده است که نیازمند پاسخ‌های مستقیم سیاست‌گذارانه از سوی تصمیم‌گیرندگان است. در حالی که این فعل‌و‌انفعالات همچنان بر رفتار دولت‌ها تأثیر می‌گذارد، اما پیشرفت اندکی در مطالعه این موضوعات حیاتی حاصل شده است زیرا مشخص نیست که آیا نظریه‌ها و توضیحات موجود قادر به تفسیر پدیده‌های سایبری هستند یا خیر (Kello, 2013). امنیت سایبری ذاتاً بین‌رشته‌ای است و بیشتر فعالیت‌ها در یک حوزه بلافاصله بر سایر حوزه‌ها تأثیر می‌گذارد. فن‌آوری‌ها و تکنیک‌ها، استراتژی‌ها و تاکتیک‌ها، انگیزه‌ها و ایدئولوژی‌ها، قوانین، نهادها و صنایع، قدرت و پول و در یک کلام همه این موضوعات در امنیت سایبری نقش دارند و همه این‌ها به‌شدت درهم‌تنیده شده‌اند. مسائل مربوط به امنیت سایبری هم‌جهانی هستند، به این دلیل که به زیرساخت‌های فراملی بستگی دارند و پارادایم‌های جغرافیایی سیاست بین‌الملل را تغییر می‌دهند؛ و نیز موضوعی هستند، زیرا در زمینه‌های مختلف اجتماعی، ملی و منطقه‌ای متفاوت ظاهر می‌شوند؛ بنابراین امنیت سایبری از جمله در خاورمیانه و شمال آفریقا<sup>۱</sup> یک مسئله چندوجهی است و چگونگی پاسخ دولت‌ها به این ناامنی‌های سایبری مطمح نظر هست.

این تحقیق در پی آن است تا از امنیت سایبری به‌عنوان یک هدف برای تمرکز بر مواجهه با ناامنی سایبری بهره‌گیری کند. یکی از واضح‌ترین جنبه‌های ناامنی سایبری در منطقه خاورمیانه، طیف وسیع تهدیدها است که از عملیات هکرها تا نگرانی‌های مربوط به باندهای جنایتکار و جاسوسان که در فضای مجازی عمل می‌کنند را در بر می‌گیرد. این مقاله استدلال می‌کند که منابع ساختاری و عوامل کلیدی ناامنی سایبری در سراسر منطقه خاورمیانه مشترک است و زمینه‌ای برای اقدامات مشترک را فراهم می‌کند. بعد دیگر تحقیق بر دولت‌ها به‌عنوان محلی برای پاسخ به این منابع ناامنی متمرکز است. در بسیاری از موارد، اقدامات دولتی برای رفع چنین ناامنی‌های سایبری بدون همکاری گسترده‌تر بخش‌های اقتصادی یا تغییرات اجتماعی، ناکافی یا حتی نامناسب است. با این وجود، دولت‌ها کلید پاسخ‌های امنیت سایبری هستند زیرا تجربیات در سراسر جهان نشان داده است که رویکردهای مناسب، چه در مقررات رسانه‌های اجتماعی علیه شبکه‌های نفوذ و چه تشویق شرکت‌ها به رفع نقص داده‌ها، بدون حمایت یا مداخله دولت پیشرفت چندانی ندارد. از سوی دیگر ادبیات مطالعات سایبری در دهه‌های گذشته به‌طور قابل توجهی افزایش یافته است. با این حال، تحقیقات در مورد منازعه سایبری و موضوعات مرتبط بسیار خاص، متمایل به سیاست‌گذاری است و لزوماً به ایجاد یا آزمایش تئوری‌های مرکزی برای مطالعه روابط بین‌الملل کمک نمی‌کند. در ادبیاتی که می‌توان آن را علمی در نظر گرفت، بیشتر مطالعات بر روی بازیگران قدرتمند، به‌ویژه رقابت بین چین، ایالات متحده و روسیه

<sup>۱</sup>MENA: the Middle East and North Africa

متمرکز شده است. علیرغم مشارکت فعال سایر دولت‌ها در فضای سایبری، ارتباط دولت‌های خاورمیانه در چالش‌های سایبری تا حد زیادی نادیده گرفته شده است.

استدلال مشخص مقاله این است که علیرغم ناامنی‌های مشترک در فضای سایبری، دولت‌های منطقه خاورمیانه با توجه به اولویت‌های سیاسی متفاوت، واکنش‌های قابل توجهی را اتخاذ کرده‌اند. برخی توسعه نهادی قوی و متمرکز را برای امنیت موثر سایبری مهم می‌دانند، در حالی که برخی دیگر مسئولیت و توانایی را بین سازمان‌های بین دولتی تقسیم کرده‌اند. به‌طور مشابه، در سطح بین‌المللی، برخی از دولت‌ها به‌طور گسترده در مذاکرات حکمرانی امنیت سایبری مشارکت داشته‌اند، در حالی که برخی دیگر از این مسیر جدا شده‌اند و فاصله گرفتن از این فرایندها را بهترین راه خود برای اطمینان از انعطاف‌پذیری و حفظ حاکمیت می‌دانند. این مقاله پیرامون دو مسئله تحقیق سازمان یافته است. بخش اول منابع ناامنی سایبری در منطقه خاورمیانه را مورد بررسی قرار می‌دهد و سپس عوامل ساختاری را بررسی می‌کند. بخش دوم به پاسخ‌های دولتی می‌پردازد و به‌نوبه خود به پاسخ‌های بین‌المللی نیز می‌پردازد. این مقاله با چندین توصیه در عرصه سیاست‌گذاری بر اساس تغییرات اخیر در همسویی سیاسی در منطقه به پایان می‌رسد.

## ۲ منابع ناامنی سایبری مبتنی بر بازیگران

منابع امنیت سایبری مبتنی بر بازیگران در منطقه خاورمیانه را می‌توان در سه نوع اصلی طبقه‌بندی کرد: رقابت و درگیری بین دولتی، زمینه‌های حملات و جنگ‌های داخلی و جرائم سایبری که به ترتیب توضیح داده خواهند شد. اول، منطقه خاورمیانه از وضعیت جاسوسی سایبری به‌عنوان ابزاری برای پیشبرد منافع منطقه‌ای مستثنا نیست. شرکت‌های امنیت سایبری، کمپین‌های جاسوسی سایبری را با هدف قرار دادن نهادهای دولتی و خصوصی در تعدادی از کشورهای خاورمیانه و همچنین عملیات جاسوسی سایبری قدرتمند از سوی قدرت‌های بزرگ و فرامنطقه نسبت داده‌اند.

به‌عنوان نمونه، پس از افشای عملیات خرابکارانه موسوم به استاکس نت<sup>۲</sup> در سال ۲۰۱۰ علیه برنامه هسته‌ای ایران، عملیات سایبری مختل‌کننده دولتی به دلیل تنش‌ها در خلیج فارس شروع شد؛ از جمله عملیات علیه زیرساخت‌های حیاتی در عربستان از سال ۲۰۱۲ (از جمله بدافزار "Shamoon"). حملات سایبری ایالات متحده در پاسخ به تحرکات ایران در سال ۲۰۱۹ و گزارش حملات سایبری مستمر بین اسرائیل و ایران در سال ۲۰۲۰ (Harknett, 2020). خلیج فارس همچنین بر کمپین‌های نفوذ دولتی تمرکز کرده است زیرا بحران خلیج فارس در سال ۲۰۱۷ با ایجاد فضای رسانه‌ای تفرقه‌انگیزی تشدید شد به‌ویژه با دست‌کاری رسانه‌های اجتماعی تحت حمایت دولت‌ها علیه قطر و ترکیه. همچنین کشته شدن جمال خاشقچی در کنسولگری عربستان در استانبول در سال ۲۰۱۸ به تامین کنندگان خصوصی نرم‌افزارهای نظارتی هدفمند و همچنین تأثیرگذاری بر کمپین‌های رسانه‌های اجتماعی مرتبط بود (Timberg, 2021). دوم، گذشته از این اختلافات بین دولتی، فعالیت‌های مشابهی نیز در زمینه جنگ داخلی توسعه پیدا کرده است. ابزارهای جاسوسی سایبری به بسیاری از بازیگران در جنگ داخلی سوریه نسبت داده شده است

<sup>2</sup>Stuxnet

که مهم‌ترین آن‌ها ارتش الکترونیکی سوریه<sup>۳</sup> وابسته به حکومت اسد است (Baezner, 2017). اعضای ائتلاف بین‌المللی در سوریه ادعا کرده‌اند که عملیات سایبری علیه داعش<sup>۴</sup>، هم برای برهم زدن تبلیغات و هم برای حمایت از اقدامات نظامی انجام شده است.

در جنگ داخلی لیبی اطلاعات غلط فراوانی وجود داشته است؛ بسیاری از طرفین درگیری تبلیغات رسانه‌های اجتماعی را انجام می‌دهند و همچنین کمپین‌های رسانه‌های اجتماعی از طرف شرکت‌های رسانه‌ای مرتبط با کشورهای خارجی مانند روسیه، مصر و امارات تغذیه می‌شوند. گزارش شده است که برخی از شرکت‌های نظامی خصوصی درگیر در این درگیری قابلیت‌های حمله سایبری را نیز ارائه می‌دهند (Grossman, 2020). به‌طور کلی، هم جنگ داخلی و هم اختلافات سیاسی طولانی‌مدت، بستر مستمری را برای حملات سایبری در منطقه فراهم کرده‌اند، زیرا بازیگران غیردولتی از طریق تخریب و هک و نشت به دنبال بالا بردن تنش در موضوعات مختلف سیاسی مانند درگیری اسرائیل/فلسطین و تنش‌های عربستان و ایران بوده‌اند.

سوم، طیف وسیعی از بازیگران مخرب از ابزارهای سایبری برای سود مالی نامشروع استفاده می‌کنند. در حالی که این بازیگران در سراسر جهان فعالیت می‌کنند، اتفاقات قابل توجهی توسط بازیگران منطقه رخ داده است و همچنین اثرات دامنه‌داری از این حملات در سراسر جهان وجود دارد. به‌عنوان نمونه، دو مورد مجزا از سرقت اطلاعات کارت اعتباری مشتریان بانک مسقط عمان و RAKBank امارات در دسامبر ۲۰۱۲ و فوریه ۲۰۱۳ وجود داشت. این اطلاعات در اختیار یک شبکه جنایی فراملی قرار گرفته بود که ۴۵ میلیون دلار پول نقد از دستگاه‌های خودپرداز در سراسر جهان با استفاده از اطلاعات کارت برداشت کرده است. در سال‌های بعد، چندین نوع بدافزار برنامه‌های بانکداری تلفن همراه در امارات را نیز هدف قرار دادند (Sun, 2017). جرائم مالی آنلاین همچنین افراد را هدف قرار می‌دهند و دارای سوگیری جنسیتی قابل توجهی است. به‌عنوان مثال، باج‌خواهی به دنبال به اشتراک‌گذاری تصاویر خصوصی، جنبه مهم اما ناشناخته‌ای از امنیت سایبری در سطح شخصی و خانوادگی است تا عرصه دولتی.

### ۳ منابع ساختاری ناامنی سایبری

ما همچنین می‌توانیم منابع ساختاری ناامنی سایبری را به سه نوع اصلی طبقه‌بندی کنیم. اولین مورد از نظر شرایط ژئوپلیتیکی است زیرا منطقه خاورمیانه تحت تأثیر متغیر رقابت تجاری و فناوری ایالات متحده و چین قرار گرفته است. از یک سو، بسیاری از کشورهای خاورمیانه از جمله ترکیه، اسرائیل و بازیگران حوزه خلیج فارس روابط نزدیک امنیتی و دفاعی با آمریکا و متحدانش دارند؛ از سوی دیگر، سرمایه‌گذاری‌های چین در زیرساخت‌ها، مشارکت‌ها در بخش انرژی و تحقیقات در زمینه‌های مرتبط با فناوری 5G و هوش مصنوعی (AI)<sup>۵</sup> برای این کشورها بسیار جذاب است؛ بدین لحاظ، آن‌ها به دنبال ایجاد تعادل بین همکاری اقتصادی چین و الزامات امنیتی ایالات متحده بوده‌اند (Hakme, 2020).

<sup>3</sup>SEA: Syrian Electronic Army

<sup>4</sup>ISIS: the Islamic State of Iraq and Syria

<sup>5</sup>Artificial Intelligence

تحولات ژئوپلیتیک از جهات دیگر بر امنیت سایبری خاورمیانه تأثیر می‌گذارد. به‌عنوان مثال، تقویت قوانین حفاظت از داده‌های اتحادیه اروپا از طریق مقررات عمومی حفاظت از داده‌ها (GDPR)<sup>۶</sup> باعث شده است که شرکت‌ها و اشخاص حقوق مشابهی را در جاهای دیگر مورد پی‌جویی قرار دهند و همچنین الزامات محلی سازی داده‌ها و مقررات محاسبات ابری<sup>۷</sup> را در سراسر منطقه، به‌ویژه در خلیج فارس، منعکس کنند (Ali, 2016). سرانجام، شکاف‌های ژئوپلیتیکی از طریق توسعه زیرساخت‌های واقعی اینترنت در منطقه به شکل فیزیکی خود را نشان می‌دهد. بازسازی زیرساخت‌های دیجیتالی پس از جنگ‌های داخلی در سوریه، لیبی و یمن و همچنین ایمن‌سازی پروژه‌های جدید شهری مانند Neom در عربستان سعودی، پیچیدگی را بر رقابت موجود و بهره‌برداری مداوم از پروتکل‌های مسیریابی و کابل‌کشی در منطقه می‌افزاید.

دومین منبع ساختاری ناامنی سایبری مبتنی بر بازار است. مشکلات مهمی در ایجاد ظرفیت‌های امنیت سایبری در منطقه خاورمیانه وجود دارد که ناشی از انگیزه‌های نامطلوب برای بخش خصوصی به‌ویژه در زیرساخت‌های حیاتی است تا اولویت امنیت شبکه‌های دیجیتالی خود را بر سودهای کوتاه‌مدت و قابل اعتماد بیشتر قرار دهد. علاوه بر این، امنیت سایبری از نظر ساختاری به شیوه‌های امنیتی کلیدی مانند آزمایش نفوذ به تحقیقات آسیب‌پذیر وابسته است؛ اما این شیوه‌های امنیتی غیرنظامی می‌تواند برای بهره‌برداری از بخش‌های امنیتی و اطلاعاتی نیز مورد استفاده قرار گیرد و تعدادی از بازیگران در منطقه چنین تحقیقات مشکوکی انجام می‌دهند (DeSombre, 2021). این ویژگی ساختاری پیوندهای تنگاتنگ بین بسیاری از این شرکت‌ها و سازمان‌های نظامی و اطلاعاتی در کشورشان را نمایان می‌کند، بدین معنا که بازار ابزارهای سایبری با تلاش هم‌زمان دولت‌ها برای توانایی‌های امنیتی و جاسوسی خود همپوشانی شده و از آن‌ها پشتیبانی می‌کند.

سومین منبع ساختاری ناامنی سایبری در توسعه رسانه‌های اجتماعی در منطقه خاورمیانه نهفته است. تقریباً همه پلتفرم‌های بزرگ رسانه‌های اجتماعی از ایالات متحده سرچشمه گرفته و مقر آن‌ها در ایالات متحده است، بدین معنی که قوانین تعدیل محتوا و استانداردهای جامع و وسیع‌تری از سوی ایالات متحده یا بازارهای کلیدی مانند اروپا و نه منطقه خاورمیانه ایجاد و اعمال می‌شوند. کشورهایی مانند عربستان سعودی برای دور زدن این محدودیت‌ها از روش‌های غیرمعارف استفاده کرده‌اند، مانند استخدام افراد داخلی در دفاتر توییتر در کالیفرنیا برای ارائه اطلاعات در مورد حساب‌های خاص (Kantrowitz, 2020). به‌طور گسترده‌تر، اکثر بازیگران منطقه‌ای بر معماری‌های نظارتی در سطح ملی، با حمایت از قوانین گسترده جرائم سایبری، برای نظارت بر رسانه‌های اجتماعی منطبق بر هنجارهای فرهنگی و همچنین محدود کردن بحث سیاسی آزاد، تکیه کرده‌اند. البته شبکه‌های اجتماعی جایگزین توسط جمهوری اسلامی ایران، عربستان سعودی و امارات متحده عربی پیشنهاد و راه‌اندازی شده اما موفقیت چندانی نداشته‌اند.

<sup>6</sup>the General Data Protection Regulation

<sup>7</sup>cloud computing

## ۴ پاسخ‌های متنوع

این بخش با تمرکز بر اقدامات دولت‌های خاورمیانه در سطح ملی و دوجانبه و سپس مشارکت منطقه در مدیریت امنیت بین‌الملل سایبری در مجامع بین‌المللی و در مورد انواع واکنش‌های دولت به منابع ناامنی سایبری منطقه، اعم از ساختاری یا غیر ساختاری، بحث خواهد کرد. در سراسر منطقه خاورمیانه و فراتر از آن باید تأکید کرد که واکنش‌های دولت اشکال مختلفی دارد، از جمله ابتکارات سیاسی، قانونی و نظارتی. در سطح استراتژیک، ما همچنین می‌توانیم پاسخ‌های دولت را به‌عنوان چندین هدف متمایز، از جمله بازدارندگی (منصرف کردن عوامل تهدیدکننده از هدف قرار دادن آن دولت)، دفاع (بهبود حفاظت و آگاهی از امنیت سایبری، به‌ویژه از طریق ظرفیت‌سازی) و تاب‌آوری (اطمینان از تداوم عملکردهای اصلی دولت با وجود اختلال سایبری) مورد نظر و تقسیم‌بندی قرار دهیم؛ اما در عرصه عمل، تمام این استراتژی‌ها و سیاست‌های دولتی در یک مجموعه مرتبط به هم به این اهداف می‌رسند و بنابراین کاملاً متمایز نیستند.

### ۱.۴ پاسخ‌های ملی و دوجانبه

بر اساس شاخص جهانی امنیت سایبری ITU که در سال ۲۰۱۸ انجام شد، عربستان سعودی، عمان و قطر در زمینه امنیت سایبری سه کشور برتر جهان عرب و در رتبه‌های بعدی مصر، امارات، کویت و بحرین قرار گرفتند (ITU, 2018). این دولت‌ها گام‌های مهمی در جهت ایمن‌سازی دیجیتالی خدمات دولتی برداشته‌اند و امارات متحده عربی از بسیاری جهات از سایر کشورها جلوتر است در حالی که سایر دولت‌های خاورمیانه نمرات ضعیف‌تری دارند. بر اساس مطالعه ۲۰۱۹ توسط Google و Bain & Company، بازار تجارت الکترونیک در سال ۲۰۱۷ در منطقه خاورمیانه به‌طور کلی ۳.۸ میلیارد دلار ارزش داشت و در شرایط قبل از همه‌گیری کرونا ۲۵ درصد رشد کرد (Bain&Company and Google, 2019).

این مطالعه، مصر و کشورهای حوزه خلیج را با هم به‌عنوان مرکز سایبری منطقه در نظر گرفته است؛ با توجه به اینکه این کشورها ۸۰ درصد از بازار تجارت الکترونیکی منطقه را به‌طور کلی (به‌استثنا اسرائیل) تشکیل می‌دهند. بر اساس تحقیقات گارتنر در حوزه امنیت سایبری، ارزش فروش تجهیزات امنیت سایبری بین سال‌های ۲۰۱۴ تا ۲۰۱۸ دو برابر شده و به حدود ۲ میلیارد دلار رسیده است (Shetty, 2018). سایر آمار ارقام بالاتری را ارائه می‌دهند که نشان می‌دهد بازار امنیت سایبری خاورمیانه در سال ۲۰۲۰ به ارزش حدوداً ۱۶ میلیارد دلار رسیده است (Markets and Markets, 2020).

یک عنصر کلیدی در ایجاد ظرفیت امنیت سایبری، استراتژی امنیت سایبری ملی است. اکثر دولت‌ها در منطقه خاورمیانه، حداقل یک‌بار چنین استراتژی را منتشر کرده‌اند و بسیاری از آن‌ها چندین بار استراتژی‌های خود را به‌روز کرده‌اند. بسیاری از دولت‌های منطقه تلاش‌های گسترده‌ای را در زمینه آموزش امنیت سایبری با ارائه مدارک در زمینه‌های فنی و سازمانی انجام داده‌اند و همچنین راه‌های عملی‌تر برای نقش‌های حرفه‌ای امنیت سایبری و افزایش آگاهی عمومی را بر عهده گرفته‌اند. این دوره‌ها به‌ویژه توسط زنان پذیرفته شده است و جنبه‌های جنسیتی هویت‌های حرفه‌ای و شخصی امنیت سایبری و عوامل ساختار بخش قوی برای ظرفیت‌سازی امنیت سایبری در منطقه خاورمیانه صورت پذیرفته است.



از نظر نهادی، برخی دولت‌های منطقه مسئولیت‌های امنیت سایبری را در یک سازمان ملی امنیت سایبری متمرکز کرده‌اند. کشورهایی که در سال گذشته این کار را انجام داده‌اند عبارت‌اند از عمان، بحرین و قطر؛ در حالی که سایر کشورها چندین ترتیبات نهادی مانند شورای عالی امنیت سایبری مصر<sup>۸</sup> یا آژانس ملی امنیت الکترونیکی امارات<sup>۹</sup> (NESAs) را تأسیس کرده‌اند. چنین سازمان‌هایی برای ادغام عملکردهای مجازی قبلی که در وزارتخانه‌های ارتباطات و کشور و غیره ادغام شده‌اند، طراحی شده است. حساس‌ترین جنبه این سیاست بوروکراتیک، برای دولت‌های خاورمیانه و هم‌تایان خود در ایالات متحده و اروپا، رابطه بین چنین سازمان‌هایی با سازمان‌های نظامی و اطلاعاتی است. ارزیابی‌ها نشان داده‌اند که چگونه مثلاً در ترکیه، این رقابت نهادی منجر به نقش امنیتی غالب در چنین تحولاتی شده است، در حالی که دیگران پتانسیل چنین موسساتی را در فضاهای مورد مناقشه مانند فلسطین و اسرائیل نقد کرده‌اند (Unver, 2018).

دولت‌های دیگر مانند تونس، شامل ترتیبات چند ذی‌نفع را که شامل بخش‌های دولتی و خصوصی و نمایندگان جامعه مدنی می‌شود، مطابق با ترتیبات گسترده‌تر چندجانبه در مدیریت جهانی اینترنت دنبال کرده‌اند. به طور کلی، به استثنای اسرائیل و ایران، سایر دولت‌های منطقه به دلیل عدم وجود ساختارهای سایبری نظامی عمومی و عدم ایجاد دستورات سایبری جداگانه، قابل توجه هستند. این ممکن است به دلیل عدم توانایی به طور کلی یا به این دلیل باشد که منبع قدرت سایبری در جای دیگری مانند سازمان‌های اطلاعاتی قرار دارد، یا این که این کشورها ترجیح می‌دهند با ایجاد برنامه‌های سایبری تهاجمی، سیگنال‌های جداگانه‌ای را ارسال نکنند (Raymond, 2015).

علاوه بر این، دولت‌ها مشارکت‌های دوجانبه جدید یا تقویت‌شده‌ای را دنبال کرده‌اند که پاسخ‌های امنیت سایبری را در برابر طیف وسیعی از تهدیدات درک شده از مخالفت‌های سیاسی شدید در داخل و خارج تا پیامدهای بالقوه عملیات سایبری علیه زیرساخت‌های حیاتی تسهیل می‌کند. پویایی چنین مشارکت‌هایی عموماً از اتحاد‌های دیپلماتیک وسیع‌تری پیروی می‌کند، اگرچه شکاف شورای همکاری خلیج فارس و سکون نهادی اتحادیه کشورهای عرب چالش‌های پیروی از خطوط سازمانی ایجادشده را آشکار می‌کند. نمونه این مشارکت در تولید امنیت سایبری مثالی بین امارات و عربستان است. اگرچه به طور کامل در مورد یمن و دیگر نقاط نبرد سازگار نیست، اما روابط آن‌ها نمونه‌ای چابک برای امنیت سایبری و کنترل اطلاعات است. همکاری امنیت سایبری همچنین می‌تواند به ایجاد ارتباط در خطوط طولانی سایبری کمک کند. به عنوان مثال، امضای اخیر توافقنامه ابراهیم و عادی‌سازی روابط اسرائیل با بحرین، سودان، امارات متحده عربی و مراکش به این معناست که بخش قوی امنیت سایبری اسرائیل می‌تواند علیرغم تنش‌ها در زمینه ارزش‌های دموکراتیک، علناً تجربیات خود را به کشورهای خلیج فارس صادر کند (Fakro, 2020). با این حال، سردی کنونی در روابط بین برخی بازیگران ممکن است اتحادها را در جهت دیگری تغییر دهد و این مسئله مانعی برای مشارکت گسترده‌تر است. بدیهی است که همکاری در حوزه امنیت سایبری می‌تواند یک کارت دیپلماتیک مفید برای همه طرف‌ها باشد.

بخشی از دلایل تغییر مسیرهای فوق، به‌ویژه حرکات اسرائیل، مقابله با موفقیت ایران در شیوه بسیار

<sup>8</sup>Egypt's Supreme Cybersecurity Council

<sup>9</sup>the UAE's National Electronic Security Agency

متفاوت همکاری‌های سایبری است. برخلاف بازیگران فوق، ایران در پی برخی ناآرامی‌ها فضای سیاسی و اجتماعی خود طی سال‌های ۲۰۱۷ تا ۲۰۱۹ دست به تعدیل معماری اینترنت داخلی خود در جهت کنترل متمرکز بر آمد تا خودمختاری فنی خود را از زیرساخت اینترنت سایر دولت‌های منطقه افزایش دهد. در عین حال، ایران صحنه سایبری قابل توجهی را پرورش داده است، به طوری که افراد با استعداد در نهادهایی که وظیفه نظامی و اطلاعاتی را بر عهده دارند به کار گرفته است (Anderson, 2018). اگرچه این ممکن است با توجه به منابع محدود ایران راه حلی کارآمد باشد، اما محدودیت بر روی چنین نهادها و سازوکارهایی منجر به برخی افشای قابلیت‌های کلیدی و گزارش هک و نشت در چنین نهادهایی شده است. گزارش شده است که ایران همچنین بر روی جمع‌آوری اطلاعات دیجیتالی از طریق بازوهای نیابتی خود در مناطق مختلف درگیری کار کرده است که احتمالاً یکی از این مناطق عرصه جنگ داخلی سوریه بوده است (Scott-Railton, 2016). همچنین، حملات اسرائیل به گروه‌های سایبری حماس نشان‌دهنده تلاقی بین مبارزات آفلاین و آنلاین بین دو دشمن در سراسر سوریه و لبنان است (Chesney, 2019).

## ۲.۴ پاسخ‌های منطقه‌ای و بین‌المللی

این بخش از پاسخ‌های ملی و دوجانبه فوق به منظور در نظر گرفتن تحولات امنیت سایبری که منطقه خاورمیانه را به سایر مناطق و فرآیندهای بین‌المللی متصل می‌کند، حرکت کرده است. در گام اول، چندین طرح توسعه ظرفیت‌های امنیت سایبری فراملی با محوریت خاورمیانه وجود دارد (Kshetri, 2016). یکی از اولین تلاش‌ها، پیشنهاد ایجاد یک مرکز نظارتی پان عربی در سال ۲۰۰۹ بود که در لبنان مستقر باشد و اعضای همه کشورهای عربی را پوشش می‌داد. این پیشنهاد شامل چند وزارتخانه لبنان (کشور و دادگستری) و همچنین انجمن‌ها و دانشگاه‌های فناوری اطلاعات (IT) در لبنان و اتحادیه کشورهای عربی بود. این ایده اولیه چند سال بعد، در مارس ۲۰۲۰، با راه‌اندازی دستورالعمل‌های امنیت زیرساخت اینترنت برای کشورهای عربی توسط انجمن اینترنتی، یک سازمان غیرانتفاعی فراملی با اعضاء دولتی و شرکت‌ها، به ثمر رسید (Internet Society, 2020). این ابتکار، از جمله یک مرکز نظارتی جدید، نشان می‌دهد که فرآیندهای چندجانبه در منطقه خاورمیانه مفید هستند، زیرا گام‌های عملی را برای سازمان‌ها در مسیر ایمن‌سازی مکانیسم‌های مسیریابی و بهبود شیوه‌های امنیت سایبری ارائه می‌دهند. بدین اعتبار، کشورهای خاورمیانه در فرآیندهای بین‌المللی حاکمیت امنیت سایبری از جمله (GGE<sup>10</sup>) و (OEWG<sup>11</sup>) در سازمان ملل شرکت کرده‌اند.

این فرآیندهای بین‌المللی وسیع‌تر از مذاکرات گسترده بین‌المللی درباره جرائم سایبری است. اصلی‌ترین متن حقوقی بین‌المللی درباره جرائم سایبری، کنوانسیون بوداپست در مورد جرائم سایبری است که توسط شورای اروپا در سال ۲۰۰۱ به توافق رسید. به دنبال کنوانسیون بوداپست که دارای ۶۶ عضو پیوسته و ناظر است و تنها چهار دولت در منطقه خاورمیانه (ترکیه، اسرائیل، مراکش و تونس که عضو ناظر است) حضور دارند. به موازات این روند، اتحادیه کشورهای عربی کنوانسیون مبارزه با تخلفات فناوری اطلاعات را پیشنهاد داد. این کنوانسیون ابتدا در سال ۲۰۰۴ به عنوان قانون الگوی پان عربی برای مبارزه با تخلفات فناوری

<sup>10</sup>Group of Governmental Experts

<sup>11</sup>Open Ended Working Group

اطلاعات تصور شد و سرانجام در دسامبر ۲۰۱۰ امضا شد. این کنوانسیون عربی و رویدادهای هم‌زمان بهار عربی منجر به توسعه قوانین بحث‌انگیز جرائم سایبری شد و در سرتاسر منطقه، بسیاری از آن‌ها به‌عنوان بندهای مبهم مورد استفاده برای سرکوب انتقادات تعبیر شدند (Shires, n.d.). مذاکرات بین‌المللی فعلی در سازمان ملل متحد در حال بازبینی ایده یک معاهده جهانی جرائم سایبری است. با قطعنامه سال ۲۰۱۹ روسیه که به سرعت تقریباً از سوی همه دولت‌های خاورمیانه تأیید شد، اما تأثیر این مذاکرات بر قوانین داخلی تا چند سال ظاهر نخواهد شد. در مقایسه با جرائم سایبری، یک حوزه مذاکره‌کننده به همان اندازه کاربرد قوانین بین‌المللی درگیری‌های مسلحانه در عملیات سایبری از یک سو و اجرای دقیق‌تر هنجارهای رفتار مسئولانه دولت در فضای مجازی از سوی دیگر است که در GGE در سال ۲۰۱۵ و متعاقباً در چندین فرآیند چندجانبه هر چند با نمایندگی محدود از منطقه مورد توافق قرار گرفت. چنین هنجارهایی شامل حفاظت از زیرساخت‌های حیاتی است که به‌وضوح توسط برخی از عملیات دولتی نقض شده و همچنین حفاظت از عرصه عمومی اینترنت نیز رعایت نشده است (Broeders, 2020). سایر ابتکارات مرتبط، مانند اقدامات ایجاد اعتماد (CBM<sup>12</sup>) برای کاهش خطر تشدید عملیات سایبری، به‌تازگی در حال پیشرفت در منطقه خاورمیانه است. به‌طور عملی، گنجاندن نهادهای فنی مانند گروه‌های واکنش اضطراری رایانه‌ای (CERTs<sup>13</sup>) در مکانیسم‌های تبادل اطلاعات و گفتگوی بین‌المللی، عملاً به ارائه کانال‌های ارتباطی می‌پردازند که ممکن است در سناریوهای بحرانی مفید باشد (Tanczer, 2018).

## ۵ نتیجه‌گیری

واقع‌گرایی به‌عنوان نظریه‌ای که بیشتر به مسائل امنیت ملی و قدرت مربوط می‌شود، به نظر می‌رسد دیدگاه غریزی روابط بین‌الملل برای درک فضای سایبری باشد. تحلیل مقاله به ما نشان داد که واقع‌گرایی یک چارچوب مرتبط برای شناسایی مسائل مهم مرتبط با امنیت در حوزه سایبری باقی می‌ماند و گاهی اوقات می‌تواند بینش مفیدی در مورد برخی از ویژگی‌های پایدار روابط بین‌الملل ارائه دهد. از بسیاری جهات، حوزه سایبری با ماهیت آنارشیک و فقدان حکومت نهادی، به دنیایی واقع‌گرا شباهت دارد که در آن دولت‌ها از یکدیگر می‌ترسند و توانایی‌های خود را در پاسخ به آن توسعه می‌دهند. با این حال، مشخص نیست که آیا رقابت‌های تسلیحاتی سایبری احتمالاً به درگیری سایبری تبدیل می‌شود یا خیر. واقع‌گرایی همچنین سوالات جالبی را در مورد توان سایبری، در مورد اینکه چه کسی آن را در اختیار دارد و چگونه با ثبات منطقه‌ای و بین‌المللی مرتبط است، مطرح می‌کند. از نظر اینکه آیا توان سایبری پویایی قدرت سنتی را تغییر می‌دهد، شواهد نشان می‌دهد که این‌طور نیست. روندی که تاکنون دیده‌ایم از جنگ سایبری تمام‌عیار به نفع اشکال کمتر مخرب تعاملات و نیز همکاری‌های سایبری خودداری شده است.

با توجه به امکان‌پذیری در مورد استفاده از فناوری سایبری به‌عنوان یک سلاح تهاجمی، دولت‌های منطقه باید با احتیاط در حوزه سایبری عمل کنند و بر ایجاد دفاع انعطاف‌پذیر تمرکز کنند. در واقع، با خودداری از

<sup>12</sup> Confidence-Building Measures

<sup>13</sup> Computer Emergency Response Teams

جنگ سایبری آشکار، بسیاری از دولت‌ها تاکنون نسبتاً محتاطانه رفتار خود را در فضای سایبری حفظ کرده‌اند و این نتیجه‌ای است که نظریه پردازان واقع‌گرا آن را جذاب می‌دانند و زمینه‌ای برای تشریح نظری بیشتر است. با تحقیقات تجربی بیشتر، می‌توانیم به درک دقیق‌تری از مسائل کلیدی مانند تأثیر رقابت‌های تسلیحاتی سایبری بر روابط بین دولت‌های منطقه خاورمیانه، توزیع قابلیت‌های سایبری بین بازیگران دولتی و غیردولتی و دلایل خویشتن‌داری با وجود رقابت شدید امنیتی و تصور مزیت تهاجمی دست یابیم. پاسخ‌های دقیق‌تر به این سؤالات می‌تواند به ما در تدوین راهنمایی‌های بهتر سیاست‌گذارانه برای دولت‌ها و نیز سازمان‌های بین دولتی کمک کند.

دولت‌های خاورمیانه به شدت از چشم‌انداز تهدید جدید مرتبط با دیجیتالی شدن آگاه هستند. بسیاری از آن‌ها برای تقویت قابلیت‌های امنیت سایبری ملی خود و ارتقای سطح حفاظت از زیرساخت‌های اطلاعاتی مهم ملی خود، فعالیت‌های امنیت سایبری خود را در سال‌های اخیر افزایش داده‌اند. دولت‌های خاورمیانه تنها دینفعانی هستند که از قدرت، دسترسی و منابع لازم برای توسعه و هدایت یک دستور کار واقعا ملی امنیت سایبری، اطمینان از همسویی تلاش‌ها و پیشبرد همکاری و بهبود مستمر از طریق بخش‌های خاص، ملی و در نهایت نهادهای حاکمیت منطقه‌ای برخوردار هستند. به همین دلیل است که دولت باید یک برنامه ملی امنیت سایبری را تعریف کند و مسئولیت آن را در بالاترین سطح تصمیم‌گیری تعیین کند. در پایان، چهار توصیه در عرصه سیاست‌گذاری دولتی را بر اساس مباحث فوق ارائه داده و با تأمل بر درک مضاعف ناامنی سایبری در پی پیاده‌سازی این موارد بر آمد:

- اول: دولت، بخش خصوصی و نهادهای جامعه مدنی باید برای افزایش تاب‌آوری سایبری همکاری کنند. آن‌ها باید با هم نقاط قوت و ضعف نسبی هر یک از ذینفعان را شناسایی کرده و به دنبال جبران این نقاط ضعف از طریق نقاط قوت مختلف باشند.
- دوم: دولت‌ها باید آموزش و پرورش را به‌عنوان پایه‌ای برای امنیت سایبری ملی و منطقه‌ای توسعه دهند. ابتکارات آموزشی باید در سراسر منطقه هماهنگ شده و برابری جنسیتی و بین بخشی را در اولویت قرار دهند.
- سوم: دولت‌ها باید بر اعتبار و قابلیت اطمینان بلندمدت در اقدامات و ارتباطات امنیت سایبری سرمایه‌گذاری کنند. این به معنای تدوین سیاست و مقررات مربوط به امنیت سایبری است که هم از نظر ماهیت و هم از نظر کاربرد قابل دسترسی باشد و به‌طور مداوم تفسیر و اجرا شود.
- چهارم: دولت‌ها باید در سطح بین‌المللی برای بالا بردن سطح امنیت سایبری در منطقه تلاش کنند. دولت‌ها می‌توانند از مفاهیم رفتار مسئولانه دولتی مسئول و عرصه عمومی اینترنت به‌عنوان مبنایی برای سرمایه‌گذاری در فرایندهای وسیع‌تر بین‌المللی مدیریت امنیت سایبری، توسعه حقوق بین‌الملل و مشارکت در گروه‌های کاری مرتبط در سازمان ملل استفاده کنند.
- در نهایت، این مقاله بر حس دوگانه ناامنی سایبری رایج در منطقه سایبری تأکید کرده است. ناامنی‌های سایبری، اعم از سطح بازیگران و نیز سطح ساختاری، خطرات روشنی را برای عملکردهای

اصلی دولت به همراه دارد: ثبات اقتصادهای دیجیتالی، عملکرد روان زیرساخت‌های حیاتی ملی و فراملی و حفاظت از افراد آسیب‌پذیر به صورت آنلاین و آفلاین.

اما ناامنی‌های سایبری همچنین در ناامنی‌های سیاسی وسیع‌تری گنجانده شده است، به‌ویژه در دولت‌ها و گستره‌هایی که حاکمان فعلی درگیر جنگ‌های منطقه‌ای و بین‌المللی هستند یا صداهای مخالف داخلی را برای جلوگیری از اعتراضات مردمی مسدود می‌کنند. به این ترتیب، ناامنی‌های سایبری - هم نفوذ به شبکه‌های دیجیتالی و هم دست‌کاری بسترهای رسانه‌های اجتماعی - تهدیدی برای قدرت سیاسی داخلی و منطقه‌ای و همچنین عملکردهای دولتی در راهبرد کلان است. در نتیجه، برخی دولت‌ها نه با هدف بهبود امنیت سایبری برای شهروندان و سازمان‌های تجاری در منطقه، بلکه برای حفظ موقعیت و موقعیت‌نخبگان همسو سرمایه‌گذاری کرده‌اند، در حالی که موقعیت مخالفان خود را کاهش داده یا بی‌ثبات می‌کنند. با دیجیتالی شدن منطقه خاورمیانه، افزایش جمعیت جوان و سرعت در حال رشد درصد کاربران آنلاین، ناامنی‌های سایبری نه تنها به ناامنی سیاسی تبدیل می‌شود، بلکه به‌طور فزاینده‌ای رسانه اصلی مشارکت سیاسی، اعتراض و رقابت بر سر روندهای آینده خواهد بود.

## مراجع

- [1] Ali, R. A., 2016. Cloud Computing in Arab States: Legal Aspect, Facts and Horizons, s.l.: ITU Arab Regional Office.
- [2] Anderson, C., 2018. Iran's Cyber Threat: Espionage, Sabotage, and Revenge, s.l.: Carnegie Endowment for International Peace.
- [3] Baezner, M., 2017. The Use of Cybertools in an Internationalized Civil War Context: Cyber Activities in the Syrian Conflict, Zurich: Center for Security Studies.
- [4] Bain & Company and Google, 2019. E-Commerce in MENA: Opportunity beyond the Hype, s.l.: s.n.
- [5] Broeders, D., 2020. Governing Cyberspace: Behavior, Power and Diplomacy, Lanham: Rowman & Littlefield.
- [6] Cyber resilience in the GCC , 2021, Chatham House, <https://www.chathamhouse.org/events/all/members-event/cyber-resilience-gcc>.
- [7] Chesney, R., 2019. Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility, s.l.: Lawfare.
- [8] Craig, A. & Valeriano, B., 2018. Realism and Cyber Conflict: Security in the Digital Age, s.l.: E-International Relations Publishing.
- [9] DeSombre, W., 2021. Countering Cyber Proliferation: Zeroing in on Access-as-a-Service, Washington D.C: Atlantic Council Cyber Statecraft Initiative.
- [10] Fakro, E., 2020. What the Abraham Accords Reveal About the United Arab Emirates, s.l.: War on the Rocks.



- [11] Grossman, S., 2020. Blurring the Lines of Media Authenticity: Prigozhin-Linked Group Funding Libyan Broadcast Media, s.l.: The Stanford Internet Observatory Cyber Policy Center.
- [12] Hakmeh, J., 2020. Is the GCC Cyber Resilient?, London: Chatham House Royal Institute for International Affairs.
- [13] Harknett, R., 2020. Troubled Vision: Understanding Recent Israeli-Iranian Offensive Cyber Exchanges, Washington D.C: Atlantic Council.
- [14] Internet Society, 2020. Internet Infrastructure Security Guidelines for the Arab State, s.l.: s.n.
- [15] ITU, 2018. Global Cybersecurity Index (GCI), s.l.: ITU Publications.
- [16] Kantrowitz, A., 2020. How Saudi Arabia Infiltrated Twitter. [Online] Available at: <https://www.buzzfeednews.com/article/alexkantrowitz/how-saudi-arabia-infiltrated-twitter>.
- [17] Kello, L., 2013. The Meaning of the Cyber Revolution Perils to Theory and Statecraft. *International Security*, 38(2), pp. 7-40.
- [18] Kshetri, N., 2016. *Cybersecurity in the Gulf Cooperation Council Economies*. New York: Springer.
- [19] Markets and Markets, 2020. Middle East Cybersecurity Market Worth \$29.9 Billion by 2025, s.l.: PRNewswire.
- [20] Möller, D., 2016. *Guide to Computing Fundamentals in Cyber-Physical Systems—Concepts, Design Methods, and Applications*. s.l.: Springer.
- [21] Raymond, M., 2015. Multistakeholderism: Anatomy of an Inchoate Global Institution. *International Theory*, 7(3), p. 572–616.
- [22] Scott-Railton, J., 2016. Group5: Syria and the Iranian Connection, s.l.: Citizen Lab.
- [23] Shetty, S., 2018. Gartner Says Middle East and North Africa Enterprise Information Security Spending Will Grow 9.8 Percent in 2019, s.l.: Gartner.
- [24] Shires, J., n.d. *Ambiguity and Appropriation: Cybercrime in Egypt and the Gulf*, London: Rowman & Littlefield Publishers.
- [25] Sun, K., 2017. BankBot Seen on Google Play, Targets New UAE Bank Apps, s.l.: Trend Micro.
- [26] Tanczer, L. M., 2018. CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*, 9(3), pp. 60-66.
- [27] Timberg, C., 2021. When U.S. Blamed Saudi Crown Prince for Role in Khashoggi Killing, s.l.: Washington Post.
- [28] Unver, A., 2018. The Logic of Secrecy: Digital Surveillance in Turkey and Russia. *Turkish Policy Quarterly*, 17(2).



## حریم شخصی در فضای سایبر

محمد جعفری<sup>۱</sup>

<sup>۱</sup> کارشناسی ارشد مدیریت فناوری اطلاعات گرایش کسب و کار الکترونیکی، دانشکده مدیریت و حسابداری  
دانشکدگان فارابی دانشگاه تهران  
jafarim584@gmail.com

### چکیده

در عصر فناوری اطلاعات و ارتباطات تمام جنبه‌های زندگی جوامع بشری خواسته یا ناخواسته تحت تأثیر قرار گرفته‌اند. با گسترش روزافزون فضای سایبری، نگرانی‌های زیادی هم در این خصوص ایجاد می‌شود که یکی از آنها مربوط به حریم خصوصی افراد حقیقی و حقوقی می‌باشد. با افزایش کاربران فضای مجازی موضوعی که بیش از پیش اهمیت پیدا می‌کند مسأله حریم خصوصی افراد در این فضا می‌باشد. امروز نقض حریم افراد و مؤسسات با توجه به امکانات عصر فناوری اطلاعات و ارتباطات بصورت گسترده و آن هم در محدوده‌ای به وسعت جهان هستی فراهم شده است ما در این پژوهش ضمن بررسی مفهوم حریم خصوصی در فضای سایبری، کوشیده‌ایم تا مهمترین مصادیقی که حریم خصوصی در فضای سایبری را نقض می‌کند بیان کنیم. ضمن آن که باید بیان کنیم فضای سایبری همچون دیگر بسترهایی که بشر امروزی در آن به فعالیت می‌پردازد برای مصون ماندن از آسیب‌های مختلف نیازمند تدوین پروتکل‌ها و دستورالعمل‌های خاصی است.

**کلمات کلیدی:** فضای سایبری، حریم شخصی، تهدید.

### ۱ مقدمه

به لطف پیشرفت‌های فناوری ما وارد عصری شده‌ایم که آن را عصر اطلاعات می‌نامند. جامعه بشری روزگار ما، جامعه‌ای اطلاعات محور است؛ بدین معنی که اطلاعات نقش محوری در آن ایفا می‌کند [۱]. پیشرفت سریع فناوری اطلاعات و انتقال تجربیات بشری منجر به تشکیل دنیای جدیدی به نام دنیای مجازی یا همان فضای سایبری شده است؛ دنیایی که در آن محدودیت‌های مرتبط با زمان و مکان بی‌اثر می‌شوند. این ویژگی‌های جدید به حریم شخصی و امنیت افراد خدشه وارد می‌کنند [۲].

امنیت همواره به عنوان یکی از اصلی‌ترین نیازهای بشر مورد توجه بوده است؛ به گونه‌ای که آدمی برای رسیدن به یک محیط مطلوب برای زیستن به تنهایی در آن تمایل دارد و این میلی است به مصون ماندن از دسترسی و اطلاع سایرین که مطلوب نوع بشری است؛ چنین حیطه‌ای از زندگی انسان را حریم خصوصی نامیده‌اند.

عصر اطلاعات جوامع بشری را با تاثیرات ارادی و غیرارادی مواجه کرده است. با گسترش روزافزون فضای سایبری، نگرانی‌های زیادی هم در این خصوص ایجاد می‌شود و در کنار آثار مثبتی که در بهبود زیست جهانی دارد، برخی ابعاد منفی و قابل توجه دیگری نیز دارد که حتی ممکن است آثار آن مخرب‌تر از جنگ‌های نظامی بوده و امنیت و ساختارهای یک جامعه را به چالش بکشاند. فضای سایبر امکانات جدیدی در اختیار بشر قرار می‌دهد: جغرافیا را از بین می‌برد؛ انسان را از موثر بودن در محیط اجتماعی، به تاثیرپذیر بودن در محیط مجازی سوق می‌دهد؛ ایده‌ها را گسترش می‌دهد؛ کنترل پذیری را کم‌رنگ می‌سازد و دولت را به عنوان نهاد ناظر بر روابط سیاسی، اجتماعی، فرهنگی و ... خلع سلاح می‌کند.

توسعه فضای سایبر همانند همه‌ی پیشرفت‌های دیگر در زندگی بشر با پیامدهای منفی و مثبت همراه بوده است که یکی از پیامدهای منفی، به خطر انداختن حریم خصوصی افراد و یکی از پیامدهای مثبت تسهیل و تسریع ارتباطات و تبادل اطلاعات است [۳]. در عصر فناوری اطلاعات و ارتباطات نقض حریم خصوصی و امنیت افراد حقیقی و حقوقی با استفاده از امکانات این عصر به راحتی امکان پذیر شده است. سیستم‌های رایانه‌ای و فضای سایبری این امکان را فراهم آورده‌اند که در گستره‌ی جهانی، اطلاعات افراد بدون اینکه خودشان مطلع شوند سرقت شود و ارزش ذاتی آن از بین برود [۴].

حریم خصوصی، یکی از بدیهی‌ترین حقوق افراد در جوامع بشری و یک جامعه دموکراتیک است. حریم خصوصی از منظر اسناد بین المللی و منطقه‌ای و نظام حقوقی داخلی کشورها مورد توجه قرار گرفته و در همه این اسناد حیثیت و محرمانگی افراد در جامعه مورد حمایت قرار گرفته است. این قوانین در راستای حفظ حیثیت افراد وضع شده‌اند و می‌توانند حریم خصوصی فضای مجازی افراد را نیز در بر گیرند.

حریم خصوصی و محرمانگی اطلاعات شخصی، مهم‌ترین و جنجالی‌ترین بحثی است که در حوزه فناوری اطلاعات وجود دارد. این موضوع قدمتی به بلندای زمانی دارد که اینترنت و شبکه‌های اجتماعی فراگیر شده است؛ در واقع همچنان که هیچکس در فضای واقعی نمی‌پذیرد که اطلاعات شخصی و خانوادگی خود را در اختیار دیگران قرار دهد، در این فضای جدید نیز کسی به این فکر نمی‌افتد که خود داده‌های شخصی خویش را افشا کند. در ادامه این پژوهش به بررسی دو مفهوم فضای سایبر و حریم خصوصی می‌پردازیم سپس رابطه آن‌ها را مورد کنکاش قرار داده و در پایان مهم‌ترین مصادیق نقض حریم خصوصی در فضای سایبری را بیان می‌کنیم.

## ۲ فضای سایبری

فضای سایبر، جدیدترین و در عین حال پیچیده‌ترین پدیده‌ای است که زندگی بشر را به خود مشغول کرده است. رایانه‌ها، قبل از ورود به حوزه شبکه، دستگاه‌های پردازشگری بودند که دورنمای سرعت و دقت را برای شرکت‌ها و نهادهای دولتی و غیردولتی فراهم کرده بودند. اما زمانی که این پردازشگرها برای اولین بار به صورت شبکه‌ای در یکی از اتاق‌های وزارت دفاع آمریکا در آمدند، اولین بنیان تشکیل فضای سایبری را بنا نهادند.

فضای سایبر به عنوان مجموعه تعامل‌های انسان‌ها از طریق رایانه و فناوری‌های نوین ارتباطات، بدون در

نظر گرفتن زمان و مکان توسط ویلیان گیسیون نویسنده داستان علمی تخیلی در کتاب «نوروموتسر» در سال ۱۹۸۴ به کار برده شد. او فضای سایبر را بازنمایی گرافیکی از داده‌ها از نظام‌های رایانه می‌داند [۵]. کلمه فضای مجازی (سایبر اسپیس) از درون کلمه سایبرنتیکس که بوسیله نوربرت وینر ابداع شده بود پدید آمد. سایبرنتیکس علم نظریه کنترل است و در مورد سیستم‌های پیچیده به کار می‌رود. فضای سایبر یا فضای مجازی در تعریف برخی نویسندگان عبارت است از: «مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و وسائل 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 شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص، خود؛ در آن، زنده و مستقیم روی می‌دهد. قید (واقعی)، مانع از این است که تصور شود مجازی بودن این فضا به معنای غیر واقعی بودن آن است؛ چرا که در این فضا نیز همان ویژگی‌های تعاملات انسانی در دنیای خارج همچون مسئولیت وجود دارد. ضمن این که فضای سایبر در واقع یک «محیط» است که ارتباطات در آن انجام می‌شوند؛ نه صرف مجموعه‌ای از ارتباطات. از سوی دیگر، این ارتباطات گرچه ممکن است در همه حال بر خط نباشد، ولی زنده، واقعی و مستقیم است. از این رو، تأثیر و تأثر بالایی در این روابط رخ می‌دهد.

فضای سایبری یک دامنه سراسری در محیط اطلاعاتی است که شامل شبکه‌های مرتبط به هم از زیرساخت‌های فناوری اطلاعات، شامل اینترنت، شبکه‌های مخابراتی، سامانه‌های کامپیوتری، پردازنده‌ها و کنترل‌های توکار است. این تعریف از این نظر قابل توجه است که تنها به مولفه فناوری سخت افزاری اشاره می‌کند، با وجودی که نرم‌افزار و داده‌ها هم ممکن است از واژه‌های به کار برده شده استنباط شود. مورد قابل ذکر دیگر در تعریف فوق، فقدان مولفه انسانی است، در حالی که جزء مهمی در تعاریف وینر و گیسیون است [۶].

فضای سایبر در سند راهبردی امنیت فضای تبادل اطلاعات (افتا): به فضای سایبری، فضای تبادل اطلاعات گفته می‌شود و به صورت زیر تعریف می‌شود:

در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات، مدیریت و کنترل و ارتباطات از طریق ساز و کارهای الکترونیکی و مجازی انجام می‌پذیرد. از این فضا با نام فتا یاد می‌شود.

نگرش فناورانه به فضای سایبر به مؤلفه‌هایی چون سخت افزار، نرم افزار، کیفیت و کمیت انتقال داده‌ها و تعامل در شبکه می‌پردازد. در حالی که رویکرد روانشناسانه مقوله‌هایی چون فضای ذهنی، الگوی رفتاری انسان و رایانه، تخیل، هویت و شخصیت، به مرز بین واقعیت و خیال و مانند آن توجه می‌کند. دیدگاه جامعه‌شناسانه درباره‌ی فضای سایبر نیز به دلیل پرداختن به جماعت‌های برخط، شبکه‌های اجتماعی سایبر، و آثار اجتماعی تعامل انسان و رایانه حائز اهمیت است.

با شکل‌گیری فضای سایبر، مرزها کمرنگ‌تر شده‌اند و جهانی شدن در کلیه امور اجتماعی به وضوح دیده می‌شود. سرعت، ارزانی، بالا بودن کیفیت، نزدیکی و در دسترس بودن، شفافیت و تنوع از ویژگی‌های فضای سایبر است. همچنین فضای سایبر باعث شکل‌گیری حجم انبوهی از داده‌ها و اطلاعات شده است؛ که خود نیازمند ایجاد پروتکل‌های امنیتی خاصی می‌باشد [۷].

## ۳ حریم خصوصی

حریم خصوصی یک مفهوم سیال است که معانی مختلفی از جمله آزادی اندیشه، کنترل بر جسم خود، کنترل بر اطلاعات راجع به خود، آزادی از نظارت‌های دیگران، خلوت و تنهایی، حمایت از حیثیت و اعتیاد و حمایت در برابر تفتیش‌ها و تجسس‌ها را شامل می‌شود. حریم خصوصی حق افراد برای برخورداری از حمایت در برابر مداخله بی‌اجازه دیگران، در امور زندگی خود و خانواده‌شان است؛ خواه این عمل با ابزار مستقیم فیزیکی صورت پذیرد یا به وسیله نشر اطلاعات.

در لایحه حریم خصوصی که در زمان دولت هفتم از سوی کمیسیون لوایح دولت تهیه و به مجلس ارائه شد در بند اول ماده ۲ در تعریف حریم خصوصی قید شده بود: «حریم خصوصی قلمروی از زندگی هر شخصی است که آن شخص عرفاً یا با اعلان قبلی در چارچوب قانون، انتظار دارد دیگران بدون رضایت وی بدان وارد نشوند یا بر آن نظارت نکنند، یا به اطلاعات راجع به آن دسترسی نداشته باشند، یا آن قلمرو را مورد تعرض قرار ندهند».

### ۱.۳ حریم خصوصی در فضای سایبر

بحث حریم خصوصی در فضای مجازی به حفظ داده‌ها از دسترسی افراد غیر مجاز تعریف می‌شود. منظور از داده‌ها در بحث حریم خصوصی نیز داده‌های شخصی است که همانا مشخصات، ممیزات و اطلاعات مربوط به یک شخص معین یا قابل تمایز که موجب تمایز او از سایر افراد گروه می‌باشد. در فضای سایبر حریم خصوصی اطلاعات و داده‌ها عبارت از اموری هستند که انسان تلاش می‌کند فاش نشوند؛ زیرا این حریم با شخصیت او در ارتباط است. برخی معتقدند حریم خصوصی مختص اشخاص حقیقی است؛ ولی واقعیت این است که اشخاص حقوقی هم نوعی حریم خصوصی داده دارند [۸].

دو اصطلاح حریم خصوصی و داده بیشتر مواقع در کنار هم به کار می‌روند در حالی که کاملاً برابر نیستند. حریم قلمرو است، حتی اگر تهی باشد و کافی است تعلق آن به شخص ثابت شود که می‌بایست مورد حمایت واقع شود؛ به همین دلیل دسترسی غیر مجاز به داده‌های عمومی در حریم خصوصی جرم انگاشته شده است. مبنای ترسیم حریم، قانون و مقررات و قرارداد یا عرف است اما داده، پیکرده و مفهوم دارد و باید ارتباطش به شخص ثابت شود.

### ۲.۳ فضای سایبر از لحاظ حقوقی

فضای سایبر از دو جهت وجود و ماهیت قابل بررسی است. از نظر وجودی (فنی) عبارت است از شبکه‌های عنکبوتی و غیر ملموس الکترونیکی که با در هم تنیده شدن، این شبکه سراسری و جهانی را شکل داده‌اند. از نظر فنی، این شبکه جهانی سایبر از خود استقلال ندارد و حاصل در هم تنیده شدن و ادغام بخش‌های مختلف است که در نهایت یک قلمرو نامحدود سایبر را در فضای خلأ شکل داده است. فضای سایبر را از نظر وجودی می‌توان ظرف نامحدودی دانست که هر کس با دسترسی به آن، امکان وارد کردن یا تخلیه مظروف (محتوا) را در آن دارد؛ بدون اینکه قدر آن اشباع شده یا محدودیتی برای سایرین ایجاد شود.

اما اینکه ماهیت حقوقی فضای سایبر، با تعریف ارائه شده چگونه است، نظریه‌های مختلفی بیان شده است که در ذیل بیان می‌کنیم:

#### الف) ماهیت ملی

برخی معتقدند، فضای سایبر در هر کشوری، همانند قلمرو مادی و فیزیکی آن تلقی می‌شود و جزو خاک آن کشور به حساب می‌آید، بنابراین در حاکمیت و کنترل کامل آن کشور است و هرگونه که خواست، می‌تواند برای کنترل آن، اقدام به وضع مقررات کند. یعنی اگر چه فضای سایبر، قلمروی سراسری در همه نقاط جهان دارد، اما از نظر حاکمیت، در کنترل دولت کشوری است که در آن مورد استفاده قرار می‌گیرد و از این نظر تفاوتی با خاک آن کشور ندارد.

#### ب) ماهیت غیر ملی

به نظر این گروه، ذات فضای سایبر، به گونه‌ای است که ماهیت فراملی دارد و هیچ کشوری نمی‌تواند آن را کنترل و مدیریت کند، ادعای تشابه و محدودیت قلمرو سایبر به مرزهای واقعی یک کشور، قابلیت تحقق و امکان ندارد. بنابراین، دولت‌ها نمی‌توانند و نباید بر فضای سایبر کنترل و نظارتی داشته باشند، چون در اصل، فضای سایبر در قلمرو حاکمیت ایشان شکل نگرفته است.

#### ج) ماهیت عام جهانی

این گروه معتقدند، اگرچه فضای سایبر در قلمرو حاکمیت دولت و کشور خاصی نیست و هیچ دولتی نمی‌تواند ادعای حاکمیت مطلق بر آن را داشته باشد، اما نهایتاً در حاکمیت جامعه جهانی است و دولت‌ها، به اتفاق، صاحب صلاحیت‌اند که در مورد آن تصمیم‌گیری کنند. به عبارت دیگر، فضای سایبر، همچون قلمرو دریاهای آزاد است که اگرچه هیچ کشوری توان وضع قانون و اعمال حاکمیت در خصوص آن را ندارد، اما جامعه جهانی برای انتظام بخشی به آن، چاره‌ای جز وضع مقررات از طریق کنوانسیون‌ها و پروتکل‌های مختلف ندارد.

### ۳.۳ مصادیق نقض حریم خصوصی در فضای سایبر

در ادامه ۱۳ مصداق قانونی درباره نقض حریم خصوصی را مورد بررسی قرار می‌دهیم:

- دسترسی غیر مجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا حساب کاربری.
- شنود غیر مجاز محتوای در حال انتقال در سیستم‌های رایانه‌ای و چت‌های اینترنتی.
- دسترسی غیر مجاز به داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای.
- در دسترس قرار دادن داده‌های سری در حال انتقال در سیستم‌های رایانه‌ای برای اشخاص فاقد صلاحیت.

- نقض تدابیر امنیتی سیستم‌های رایانه‌ای و مخابراتی به قصد دسترسی به داده‌های سری.
- حذف، تخریب و یا غیر قابل پردازش کردن داده‌های دیگری از سیستم‌های رایانه‌ای به طور غیرمجاز.
- انتشار هرزنامه (Spam) و ارسال بدافزار از طریق پست الکترونیک که مدتی است توسط کلاهبرداران سایبر متداول شده را می‌توانیم مصداق این موضوع بدانیم.
- از کار انداختن سیستم‌های رایانه‌ای به طور غیر مجاز و ممانعت از دسترسی اشخاص به پورتال‌ها.
- ممانعت از دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای به طور غیرمجاز.
- ربودن داده‌های متعلق به دیگری به طور غیرمجاز.
- هتک حیثیت از طریق انتشار صوت و فیلم تحریف شده دیگری توسط سیستم‌های رایانه‌ای و مخابراتی.
- نشر اکاذیب از طریق سیستم‌های رایانه‌ای یا مخابراتی به قصد تشویش اذهان عمومی.
- فروش، انتشار و یا در دسترس قرار دادن رمز عبور یا هر داده‌ای که امکان دسترسی غیر مجاز به داده‌ها یا سیستم‌های رایانه‌ای دیگران را فراهم کند.
- آموزش نحوه ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی. یکی از آشکارترین مصداق‌های نقض حریم خصوصی کاربران در اینترنت به ویژه در شبکه‌های اجتماعی، تبلیغ شیوه‌های هک تلگرام، اینستاگرام و نصب نرم‌افزارهای مربوطه است.

۱۳ موردی که در بالا به آن اشاره کردیم، مصادیق آشکار نقض حریم خصوصی کاربران در فضای سایبری هستند. شما باید در صورت برخورد با چنین مواردی، مراتب را به پلیس سایبر اطلاع دهید. برای حضوری فعال و استفاده فرصت آفرین از شبکه‌های اجتماعی داخلی و بین‌المللی، همانطور که بارها تاکید شده است، باید به حریم خصوصی خود و دیگران احترام گذاشت.

## ۴ نتیجه‌گیری

حریم خصوصی محدوده‌ای است که فرد تمایل دارد از نظارت، کنترل، مشاهده و زیر نظر داشتن توسط سایرین محفوظ بماند. این سایرین دربردارنده‌ی افراد حقیقی و حقوقی می‌باشد. فضای سایبری با توجه به ویژگی‌های ذاتی خود همانند دسترسی بالا، ناشناس بودن و نداشتن محدودیت زمان و مکان امکان نقض حریم خصوصی افراد و شرکت‌ها را فراهم می‌کند، که این امر نیازمند تدوین قوانین و رعایت پروتکل‌های خاصی می‌باشد. در این پژوهش سعی شد تا مفهوم حریم خصوصی در فضای سایبری مورد بررسی قرار گیرد و مهم‌ترین مصادیق نقض آن هم بیان گردد. با توجه به رشد فزاینده‌ی فضای سایبری در کشور، ما نیازمند تدوین قوانین و



پروتکل‌های مختص این فضای جدید می‌باشیم تا بتوانیم حریم خصوصی افراد حقیقی و حقوقی را محترم شماریم و از نقض آن جلوگیری کنیم.

## مراجع

- [1] Seyyed Ahmad Khalili Juo Lorestani, (2017). Revisiting the Challenges and Threats of Cyberspace on Sustainable Security, , 14(42), 147-176. [magiran.com/p1809682](http://magiran.com/p1809682)
- [2] Ali Sadeghi, Zeinab Ameri, (2017). Social Networks and Social Damage Case Study: Public Safety., Journal of survey in teaching humanities, 2(5), 51-65. [magiran.com/p2146143](http://magiran.com/p2146143).
- [3] M. Janparvar, T. Heidari Moselo, (2011). Pathology of cyberspace on social security, Order & Security Research Journal, 4(3), 141. [magiran.com/p1055026](http://magiran.com/p1055026).
- [4] Yunes Fathi , Kheyrollah Shahmoradi, (2017). Area and territory of privacy in virtual space, The Judiciary Law Journal, 81(99), 227-250. [magiran.com/p1791388](http://magiran.com/p1791388).
- [5] Zanettin, F. and C. Rundle (2022). The Routledge Handbook of Translation and Methodology.
- [6] Ottis, R; Lorents, P. (2010). Cyberspace: Definition and Implications. Proceedings of the 5th International Conference on Information Warfare and Security: 5th International Conference on Information Warfare and Security, Dayton, Ohio, USA, 08-09.04.2010. Ed. Dr Leigh Armistead. Reading, UK: Academic Conferences Limited, 267-270.
- [7] Jafari, Mohammad and Hashmati, Hamed, 2018, Investigating the impact of the Internet of Things, big data and artificial intelligence on the development of a smart city, the 8th International Conference on Information Technology, Computer and Telecommunications, <https://civilica.com/doc/1010129M>.
- [8] Hamidreza Afshar, Seyyed Shamsoddin Hoseini, Mohammadreza Movahedisefat, (2020). Investigating Opportunities and Threats of Adoption and Development of Blockchain Technology in I.R.of Iran, National Security, 10(36), 307-348. [magiran.com/p2158554](http://magiran.com/p2158554).



## بررسی قابلیت‌های فناوری بلاک‌چین در مدیریت اسناد و آرشیوهای الکترونیکی

فاطمه ترکاشوند<sup>۱</sup>، محمدرضا وصفی<sup>۲</sup>، مژگان رستگار<sup>۳</sup>

<sup>۱</sup> فارغ‌التحصیل کارشناسی ارشد، گروه علم اطلاعات و دانش‌شناسی، دانشکده مدیریت، دانشگاه تهران  
torkashvand.f@ut.ac.ir

<sup>۲</sup> نویسنده مسئول، استادیار، گروه علم اطلاعات و دانش‌شناسی، دانشکده مدیریت، دانشگاه تهران  
mvasfi@ut.ac.ir

<sup>۳</sup> دانشجوی کارشناسی ارشد، گروه علم اطلاعات و دانش‌شناسی، دانشکده مدیریت، دانشگاه تهران  
mozghanrastgar@ut.ac.ir

### چکیده

در دنیای کنونی، تراکم داده‌ها رو به فزونی یافته و پرواضح است که، مبادله و مدیریت اسناد دیجیتال مستلزم ظهور ابزارهای جدید مدیریتی در حوزه اسناد و آرشیو است. از این رو، پژوهش حاضر به دنبال سنجش امکان استفاده از فناوری بلاک‌چین در مدیریت این حوزه، از منظر کارشناسان ایرانی است. این پژوهش از نظر هدف کاربردی و از نظر گردآوری داده‌ها از نوع آمیخته است. برای جمع‌آوری داده‌ها ترکیبی از روش‌های کمی و کیفی بکار گرفته شد. به عنوان جامعه آماری، از طریق نمونه‌گیری هدفمند، بیست نفر از متخصصان بلاک‌چین، انتخاب شدند. ابزار جمع‌آوری داده‌ها علاوه بر مصاحبه‌های نیمه ساختاریافته، پرسشنامه محقق ساخته است. به دنبال آن، به منظور تأیید اعتبار و پایایی نتایج، کارشناسان این حوزه تشویق شدند تا پاسخ‌های قبلی خود را با توجه به پاسخ سایر اعضا، مرور و اصلاح کنند. سپس به منظور تجزیه و تحلیل داده‌ها از آمار توصیفی و تحلیل استنباطی، شامل تکنیک‌های دلفی و دلفی فازی استفاده شد. یافته‌ها نشان می‌دهد که کارشناسان مفید بودن استفاده از بلاک‌چین در زنجیره مدیریت اسناد و آرشیو را تضمین حفظ حریم خصوصی، محرمانه بودن اطلاعات و ایجاد سپرهای مجازی از حملات سایبری می‌دانند. نتایج این مطالعه نشان می‌دهد فناوری بلاک‌چین می‌تواند راه حلی بسیار مناسب برای مدیریت زنجیره اسناد و فایل‌های الکترونیکی و نیز ایجاد اعتماد در ذخیره‌سازی بلندمدت آنها در فضایی مجازی و ایمن به شمار رود.

**کلمات کلیدی:** بلاک‌چین، مدیریت اسناد و آرشیو، حریم خصوصی، محرمانگی، حملات سایبری.

## ۱ مقدمه

مدیریت اسناد و آرشیو و زنجیره‌ی حیات آن، امروزه به عنوان یک علم در حال توسعه مورد توجه است. بازیابی اطلاعات پرونده‌ها و اسناد، جهت انجام وظایف گوناگون و پاسخگویی به نیازها اهمیت بسزایی دارد. رعایت اصول اساسی این دانش، امکان بهره‌وری را بالا برده و از امکان بروز خلل در نظام ادارات، سازمان‌ها، موسسات و بنگاه‌ها کاسته و مبادله اسناد و آرشیوها را در مسیری ایمن قرار می‌دهد. از این رو انجام وظایف قانونی و اجرای مسئولیت در قبال آرشیو و ضرورت ایجاد تشکیلات منسجم مدیریت اسناد در هر سازمان موضوعی اجتناب‌ناپذیر است (لیانگ<sup>۱</sup> و همکاران، ۲۰۱۷).

با توجه به گسترش استفاده از راه‌حل‌های مبتنی بر ابزار بلاک‌چین و افزایش استفاده از آن در نحوه تولید، نگهداری و توزیع پرونده‌ها و اسناد، امروزه نیاز به شناخت و درک درست از آن از سوی متخصصان با هدف مدیریت زنجیره حیات و نگهداری طولانی‌مدت آن‌ها احساس می‌شود (لیمیکس<sup>۲</sup>، ۲۰۱۷). تاکنون توجه به این فناوری به میزان زیادی بر خدمات مالی متمرکز بوده و یا اینکه چگونه این فناوری می‌تواند بر سازمان‌ها، مدل‌های تجاری و نحوه خلق و مبادله ارزش، تأثیر بگذارد (مورکانوس<sup>۳</sup>، ۲۰۱۹).

با پدیداری آرشیوهای دیجیتال و الکترونیکی، امنیت و یکپارچگی داده‌ها و قابل اعتماد و استناد بودن آن‌ها، به دغدغه‌ای بسیار مهم تبدیل شده است. مسئله‌ای که باید در روند مدیریت آرشیوها لحاظ شود. امروزه فعالان این حوزه و مراکز آرشیوی در تلاش هستند تا از بهترین شیوه‌ها برای ارائه خدمات ایمن با ماندگاری بالا بهره‌گیرند. بنابراین، باید نیازها و چالش‌ها به خوبی شناسایی و پیش‌بینی شوند تا اسناد در خدمت بهره‌وری بالا قرار گیرند و از معرض هرگونه آسیب در امان باشند و توانایی‌هایی مدیریتی این حوزه در پاسخ به خواسته‌های مخاطبان اطلاعات آرشیوی و اسنادی افزایش یابند.

بلاک‌چین نوع جدیدی از فناوری است که از رمزنگاری با استفاده از الگوریتم‌ها برای محافظت از سوابق و آرشیوهای اطلاعاتی هنگام ایجاد و ذخیره‌سازی و انتقال استفاده می‌کند. در ابتدا، این فناوری در رمزارزها مورد استفاده قرار گرفته است (ناکاموتو<sup>۴</sup>، ۲۰۰۹)؛ اما امروزه از این فناوری در زمینه‌های مختلف همچون پزشکی، زنجیره‌ی تأمین، اینترنت اشیا و غیره نیز استفاده می‌شود. لذا بسیاری از پژوهشگران، استفاده از این فناوری را فراتر از ارزهای دیجیتال و در سطحی گسترده پیش‌بینی می‌کنند (ژانگ<sup>۵</sup> و همکاران، ۲۰۱۷). با توجه به مشکلات در نبود سیستمی یکپارچه و کامل مخصوص آرشیوهای دیجیتال و نیاز عصر حال حاضر به بهبود و بالا بردن سطح کیفی آرشیوها در تمامی مراکز و سازمان‌ها که به اسناد در فرایند عملیات خود احتیاج دارند، اعم از خصوصی و دولتی، و نیز با توجه به خلا ادبیاتی و نظری با موضوع استفاده از بلاک‌چین در آرشیو، این پژوهش همچنین به دنبال آن است تا در کامل شدن مبانی نظری کاربست آن، ایفای نقش نماید.

<sup>1</sup>Liang

<sup>2</sup>Lemieux

<sup>3</sup>Morkunas

<sup>4</sup>Nakamoto

<sup>5</sup>Zheng

پژوهش حاضر به منظور بررسی اهداف خود، از خبرگان انجمن بلاک چین<sup>۶</sup> به عنوان جامعه آماری استفاده کرده است.

## ۲ مروری بر کارهای دیگران

ایزدی و شریف خطیبی (۱۳۹۹)، در مطالعه‌ای به معرفی بلاک چین و کاربرد آن در ذخیره اطلاعات به عنوان پایگاه داده توزیع شده‌ی امن پرداخته‌اند. آن‌ها در این مطالعه نشان دادند که میزان پردازش تراکنش‌ها یا توان عملیاتی سیستم‌های بلاک چین نسبت به پایگاه‌های داده‌ای دیگر، نسبتاً پایین و از طرف دیگر تاخیر تراکنش یا زمان پاسخ در این فناوری نسبتاً بالا است.

شهبازی و همکاران (۱۳۹۹) در مطالعه‌ای به بررسی کاربردی الگوریتم‌های اجماع استفاده‌شده در شبکه‌های بلاک چین پرداخته‌اند. نتایج آن‌ها نشان داده است که الگوریتم‌ها و اجماع به کار رفته در بلاک چین به دو گروه تقسیم می‌شوند. گروه نخست، الگوریتم‌های اثبات‌محور است. با این الگوریتم‌ها، اعضا و عوامل مشارکت‌کننده در شبکه صحت‌گذاری، نشان می‌دهند که برای افزودن بلوک جدید، شرایط و توان بهتری به نسبت سایر وجود دارد. گروه دوم الگوریتم‌های رأی‌محور است. در این الگوریتم‌ها، اعضای شبکه پیش از تصمیم نهایی، باید نتایج خود را در خصوص صحت تراکنش یا بلوک جدید با یکدیگر در میان بگذارند. رضائی و طائی‌زاده (۱۳۹۸) در مطالعه‌ای به بررسی ظرفیت ساختاری بلاک چین در بستر اینترنت اشیا برای ارتقای اعتماد و دسترس‌پذیری ذینفعان زنجیره‌ی تأمین به اطلاعات و دانش تبادل‌ی پرداخته‌اند. نتایج آن‌ها نشان داده است که بلاک چین ظرفیت پاسخ به چالش‌های جدی مدیریت اطلاعات در زنجیره تأمین را دارد.

بجاری و نجفی (۱۳۹۷) در مطالعه‌ای به بررسی کاربردهای فناوری بلاک چین در صنعت حمل و نقل دریایی پرداخته‌اند. یافته‌های آن‌ها نشان داده است که سیستم بلاک چین توانایی قراردادن اسناد کشتیرانی در یک دفتر کل یا لیست مشترک را فراهم می‌کند و طرف‌های درگیر در فرایند حمل و نقل مانند صادرکننده، واردکننده، فورواردرها، کشتی، بنادر و ادارات گمرک را قادر می‌سازد تا جزئیات فرایند ارسال یک محموله از مبدأ تا مقصد را مشاهده کنند. علاوه بر این، غیرقابل‌تغییر بودن ذاتی بلاک چین به تبادل اسناد در شکلی واقعی و اطمینان از خدشه‌ناپذیر بودن آن‌ها، کمک می‌کند.

بنویدی و همکاران (۱۳۹۷) در مطالعه‌ای به بررسی نقش بلاک چین بر صنعت بیمه بر رویکرد بهبود فرایندها پرداخته‌اند. یافته‌های آن‌ها نشان می‌دهد که بکارگیری این فناوری، فرآیندهای پذیرش، صدور و تعیین میزان خسارت را می‌تواند در این صنعت با دقت و سرعت قابل توجهی افزایش دهد. در رابطه با حاکمیت، حفظ حریم خصوصی، مقیاس‌پذیری، هویت و مدیریت دسترسی، امنیت و قابلیت اطمینان بودن، بیش از پیش نمایان می‌سازد.

<sup>۶</sup> انجمن فناوریان زنجیره بلوک فعالیت خود را ذیل قوانین رسمی جمهوری اسلامی در تاریخ ۹ تیر ۱۳۹۶ با نام «انجمن بلاکچین ایران» آغاز و رسماً اعلام موجودیت کرده است. اعضای این انجمن از متخصصان این حوزه تشکیل شده و در حوزه اجرا و محافل آکادمیک حضور دارند.

میشف و کارافیلوسکی (۲۰۱۷)، کاربرد بلاکچین را برای حل چالش‌های کلان داده، در حوزه‌های مدیریت غیر متمرکز داده‌های شخصی، شفافیت ویژگی‌های دیجیتال و ارتباطات اینترنت اشیا بررسی کرده‌اند.

دیوید و همکاران (۲۰۲۱) در مطالعه‌ای به بررسی بلاکچین برای مدیریت و امنیت سیستم‌های اطلاعاتی پرداخته‌اند. یافته‌های آن‌ها نشان داده است که ساختار بلاکچین و توسعه این فناوری برای افراد جدید در بازار پر جنب و جوش جهان امروز بی‌سابقه است.

انتان و همکاران (۲۰۲۰) در مطالعه‌ای به پیاده‌سازی فناوری بلاکچین برای تأیید صحت بایگانی در آرشیوهای الکترونیکی پرداخته‌اند. یافته‌های آن‌ها نشان داده است که پیشرفت‌های انجام‌شده در سیستم بلاکچین امنیت سیستم را از نظر جلوگیری از جعل بسیار بهبود بخشیده است.

## ۳ روش پژوهش

روش پژوهش در این مطالعه، از لحاظ هدف، کاربردی است و نتایج آن می‌تواند در برنامه‌ریزی‌ها و سیاست‌گذاری‌های این حوزه مورد استفاده قرار بگیرد. همچنین از لحاظ گردآوری داده‌ها، این مطالعه از نوع آمیخته است زیرا در آن از ترکیبی از روش‌های کمی و کیفی به صورت همزمان استفاده شده است. برای گردآوری آمار و اطلاعات پژوهش از دو روش استفاده شده است. نخست، به منظور جمع‌آوری اطلاعات مورد نیاز درباره ادبیات و پیشینه‌ی پژوهش از کتب، مقالات، پایان‌نامه‌ها در داخل و خارج از کشور، از روش کتابخانه‌ای استفاده شد. سپس مصاحبه با خبرگان این حوزه در ایران در دستور کار قرار گرفت و در انتها، با استفاده از پرسشنامه، آمار و اطلاعات لازم جمع‌آوری و به منظور بررسی فرضیه‌ها مورد بررسی قرار گرفت. جامعه آماری منتخب در این پژوهش عبارت بودند از اعضای انجمن بلاکچین ایران. دلیل این انتخاب آن بود که اعضای آن، اطلاعات کافی و مناسبی در خصوص قابلیت‌ها و پتانسیل‌های فناوری بلاکچین داشته و از نزدیک با این پدیده طی سال‌ها در حال کنش بوده‌اند. علاوه بر آن غالب اعضای این انجمن از جایگاه علمی در کشور برخوردار بوده و می‌توانستند سریع با اهداف پژوهش ارتباط فکری برقرار کنند. با این حال، در فرآیند انتخاب اعضا از روش نمونه‌گیری غیر احتمالی، گلوله برفی، استفاده شد.

در این جستار، پس از بررسی‌های اولیه، ابتدا ده تن از متخصصین به عنوان نامزد به منظور مشارکت و مصاحبه نیمه‌ساختاریافته انتخاب شدند. به منظور جلب مشارکت نامزدها به صورت جداگانه و حضوری با آن‌ها موضوع و اهمیت پژوهش به بحث گذاشته شد. پس از آن، چارچوب اولیه استخراج و مصاحبه‌ها انجام پذیرفت. به دنبال آن با تجزیه و تحلیل مصاحبه‌ها، پرسشنامه محقق ساخته طراحی و میان بیست نفر از افرادی که دارای تخصص در دو حوزه آرشیو و بلاکچین بودند، توزیع شد.

به منظور تعیین شاخص نسبت روایی محتوا و پایایی، از تعدادی از خبرگان و کارشناسان منتخب خواسته شد که در مورد هر یک از مؤلفه‌ها با استفاده از سه طیف ضروری، غیر ضروری و بی‌تفاوت پاسخ دهند که به ترتیب شامل پنج تن از اساتید دانشگاهی و چهار تن از اعضای انجمن بلاکچین ایران می‌شد. بدین ترتیب، ایده نهایی پرسشنامه پس از چند نوبت ویرایش تدوین و میان سایر متخصصین توزیع گردید. در نهایت داده‌ها



مورد تحلیل و نتایج قرار گرفت و مجدد نتایج اخذ شده جهت بازخورد و تایید میان متخصصین منتخب به منظور تعیین پایایی درونی عرضه و از روش آلفای کرونباخ استفاده گردیده و عدد (۰/۸۱۲) بدست آمد. همچنین در این پژوهش به منظور تجزیه و تحلیل داده‌ها و آزمون فرضیات از روش آمار توصیفی و آمار استنباطی بهره گرفته شد. مهم‌ترین آمار توصیفی به کار رفته در این پژوهش جدول توزیع فراوانی و شاخص‌های پراکندگی بود. آمار و اطلاعات گردآوری شده با استفاده از تکنیک دلفی و دلفی فازی نیز مورد تجزیه و تحلیل قرار گرفت.

### ۱.۳ یافته‌های پژوهش

در پژوهش حاضر فرضیات زیر مدنظر قرار گرفته است:

- استفاده از فناوری بلاک‌چین در آرشيو الكترونيكي موجب ارتقاء سطح محرمانگي اطلاعات مي‌شود.
- استفاده از فناوری بلاک‌چین در آرشيو الكترونيكي موجب ارتقا سطح دسترسي به اطلاعات مي‌شود.
- استفاده از فناوری بلاک‌چین در آرشيو الكترونيكي داراي قابليت عدم تغيير اطلاعات و جلوگيري از جعل اسناد مي‌شود.
- استفاده از فناوری بلاک‌چین در آرشيو الكترونيكي موجب ارتقا سطح امنيت اطلاعات مي‌شود.

نتایج بدست آمده نشان داد که همه‌ی مؤلفه‌های مندرج به عنوان شاخص‌های اساسی موثر بر قابلیت‌های فناوری بلاک‌چین برای استفاده در مدیریت چرخه اسناد و آرشیوهای الکترونیکی مورد تایید جامعه کارشناسی پژوهش بوده است.

بر اساس نتایج گزارش شده، بیشترین میزان موافقت خبرگان مربوط به حفظ حریم خصوصی افراد با ضریب کندال ۰/۳۶ است. همچنین، کمترین میزان موافقت خبرگان مربوط به اثربخشی تغییرناپذیری فناوری بلاک‌چین با ضریب کندال ۰/۲۷ است.

در الگوریتم اجرای تکنیک دلفی فازی برای غربالگری، نخست باید طیف فازی مناسبی برای فازی‌سازی عبارات کلامی پاسخ‌دهندگان توسعه داده می‌شود. به این منظور از روش‌های توسعه طیف فازی استفاده شد. برای نمونه طیف فازی مثلثی برای مقیاس پنج درجه لیکرت در بیان اهمیت شاخص‌ها به شرح این جدول طراحی گردید.

جدول ۱ میانگین دیدگاه‌های خبرگان حاصل از نظرسنجی نخست را برای معیارها نشان می‌دهد. در این جدول، عبارات کلامی به اعداد فازی تبدیل و نظرات خبرگان تجمیع گردید. بر همین اساس، میانگین قطعی بدست آمده، نشان‌دهنده‌ی شدت موافقت خبرگان با هرکدام از مؤلفه‌های پژوهش است. مطابق نتایج جدول، بیشترین میزان موافقت خبرگان با حفظ حریم خصوصی افراد ( $S = 0.76$ ) و محرمانه بودن اطلاعات کاربران ( $S = 0.70$ ) است. همچنین کمترین میزان موافقت با مؤلفه‌های زمینه‌ساز توانایی شرکتکنندگان در شبکه برای دستیابی به اطلاعات ( $S = 0.44$ ) و زمینه‌ساز توانایی تأیید وضعیت سیستم در داخل شبکه ( $S = 0.41$ ) است.

## ۲.۳ تکنیک دلفی فازی

در این مرحله، میزان اختلاف نظر هر خبره با میانگین نظرات اعضا نمونه خبرگان محاسبه شد. سپس پرسشنامه‌ی دیگری به همراه نظر قبلی هر خبره و میزان اختلاف نظر آن‌ها با میانگین نظرات اعضای پانل در اختیار آنها قرار گرفت. چنانچه نظرات ارائه شده در مرحله اول و مقایسه آن با نتایج مرحله دوم اختلاف نظر خبرگان در دو مرحله از حد آستانه ۲/۰ کمتر باشد، فرایند نظرسنجی متوقف می‌شود. لذا در این فرایند، با توجه به آنکه میزان اختلاف نظر خبرگان، بین دو مرحله اول و دوم اجرای دلفی، کمتر از حد آستانه خیلی کم (۲/۰) بدست آمد، نظرسنجی در مرحله دوم متوقف شد.

بر اساس نتایج به دست آمده جدول ۱، بیشترین توافق خبرگان در خصوص اقداماتی که باید در زمینه قابلیت‌های فناوری بلاک‌چین در آرشیوهای الکترونیکی و اسناد صورت گیرد، عبارت است از مؤلفه‌ی حفظ حریم خصوصی افراد ( $S = ۰/۸۷$ ) و مانع از حملات سایبری و هکرها با استفاده از الگوریتم‌های رمزنگاری ( $S = ۰/۸۳$ ) و کمترین متوافق خبرگان برای مؤلفه‌های زمینه‌ساز توانایی شرکت‌کنندگان در شبکه برای دستیابی به اطلاعات، اثربخشی رمزهای رمزگذاری شده‌ی فناوری بلاک‌چین و توانایی ایجاد امنیت در زمینه پرداخت‌ها و انجام تراکنش‌های مالی ( $S = ۰/۴۶$ ) بود.

## ۴ نتیجه‌گیری

نتایج حاصل از یافته‌ها، بر اساس نظرات خبرگان، نشان می‌دهد که حریم خصوصی، محرمانگی اطلاعات، و حملات سایبری و هکرها، از چالش‌های اصلی مدیریت چرخه‌ی آرشیوهای الکترونیکی و اسناد به شمار می‌روند. نتایج به خوبی نشان می‌دهند که می‌توان از ظرفیت‌های بلاک‌چین برای مدیریت بهینه در یافتن پاسخ به این چالش‌ها و گام نهادن به سوی بهره‌وری بالا استفاده کرد. فعال شدن زنجیره‌ی بلاک‌چین می‌تواند در محفوظ ماندن سند الکترونیکی ایفای نقش کند.

در حالت کلی، اصلی‌ترین هدف در استفاده از فناوری بلاک‌چین، امکان به اشتراک گذاری داده‌ها به روشی ایمن و غیر قابل دستکاری است؛ به‌ویژه زمانی که اعتماد کامل بین افراد وجود ندارد؛ برای محقق شدن این هدف بلاک‌چین داده‌ها را با استفاده از ابزارهای الگوریتمی ذخیره می‌کند. بدین وسیله هکرها و مهاجمان کار راحتی برای دستکاری و یا از بین بردن داده‌ها نخواهند داشت. بلاک‌چین به عنوان یک سیستم غیر متمرکز به یک شخص ثالث مورد اعتماد برای تایید نیاز ندارد. در مقابل، برای اطمینان، تضمین و انطباق داده‌ها از مکانیزم اجماع غیرمتمرکز استفاده می‌کند.

نتایج مربوط به مقایسه دلفی و دلفی فازی نیز نشان می‌دهد که بیشترین میزان موافقت، مربوط به حفظ حریم خصوصی است و مشخص گردید که در دو تکنیک فازی و دلفی فازی نتایج یکسانی حاصل شده است؛ زیرا هنگام استفاده از بلاک‌چین، کلید خصوصی کاربر به عنوان شناسه هویت و امنیت او در نظر گرفته می‌شود و شخص ثالثی در تولید و نگهداری وجود ندارد. به عبارت دیگر می‌توان گفت نقش امنیت در فناوری بلاک‌چین بر عهده هَش است. هَش هر یک از بلوک‌ها، بر اساس اطلاعات موجود درون هر بلوک و هَش تولید شده برای بلوک قبلی تولید می‌شود. در این شناسه، هَش‌ها، نقش بسیار مهمی در اطمینان از امنیت و تغییرناپذیری ایفا

جدول ۱: میانگین دیدگاه‌های خبرگان حاصل از نظرسنجی دوم معیارها

معیارها	میانگین فازی مثلثی				میانگین فازی زدایی شده	$ S_1 - S_2 $		
قابلیت محرمانه بودن اطلاعات	(	۰/۷۴	،	۰/۶۲	،	۰/۴۱	)	۰/۱۱
زمینه‌ساز توانایی پنهان نگه‌داشتن اطلاعات	(	۰/۹۸	،	۰/۵۲	،	۰/۳۴	)	۰/۰۵
محرمانه بودن اطلاعات کاربران	(	۰/۸۶	،	۰/۶۴	،	۰/۴۹	)	۰/۰۳
حفظ حریم خصوصی افراد	(	۰/۹۱	،	۰/۷۳	،	۰/۵۹	)	۰/۰۲
قابلیت اصلاح اطلاعات	(	۰/۸۰	،	۰/۵۱	،	۰/۳۷	)	۰/۰۲
قابلیت در دسترس بودن اطلاعات را در زمینه‌های مختلف	(	۱/۰۷	،	۰/۸۴	،	۰/۷۱	)	۰/۰۲
جلوگیری از جعل اسناد	(	۰/۸۵	،	۰/۴۷	،	۰/۳۸	)	۰/۰۲
قابلیت امنیت اطلاعاتی	(	۰/۹۰	،	۰/۶۴	،	۰/۴۶	)	۰/۰۸
محافظت از داده‌ها از دسترسی‌های غیرمجاز	(	۰/۸۲	،	۰/۴۳	،	۰/۳۶	)	۰/۰۶
مانع از دسترسی سایر افراد به اطلاعات دیگر کاربران از طریق احراز هویت	(	۰/۸۳	،	۰/۳۳	،	۰/۳۵	)	۰/۰۲
کنترل و ثبت ورود و خروج کاربران	(	۰/۷۵	،	۰/۴۳	،	۰/۳۲	)	۰/۰۱
زمینه‌ساز توانایی شرکت‌کنندگان در شبکه برای دستیابی به اطلاعات	(	۰/۶۷	،	۰/۴۰	،	۰/۳۰	)	۰/۰۲
زمینه‌ساز توانایی تأیید وضعیت سیستم در داخل شبکه	(	۰/۸۸	،	۰/۶۰	،	۰/۴۸	)	۰/۰۲
دارای توانایی ذخیره چندین کپی یکسان از پرونده برای داشتن نسخه پشتیبان	(	۰/۷۰	،	۰/۴۲	،	۰/۳۶	)	۰/۰۵
اعطا و لغو حقوق دسترسی	(	۰/۷۸	،	۰/۵۰	،	۰/۴۰	)	۰/۰۸
دارای توانایی دسترسی کاربران مختلف به داده‌های مشترک	(	۰/۷۳	،	۰/۴۶	،	۰/۳۸	)	۰/۰۴
مانع از حملات سایبری و هکرها با استفاده از الگوریتم‌های رمزنگاری	(	۱/۰۲	،	۰/۷۸	،	۰/۶۹	)	۰/۰۳
اثربخشی تمرکززدایی فناوری بلاکچین	(	۰/۸۱	،	۰/۳۵	،	۰/۳۹	)	۰/۰۰۵
اثربخشی قابلیت ردیابی فناوری بلاکچین	(	۰/۸۹	،	۰/۶۲	،	۰/۴۷	)	۰/۰۹
اثربخشی امنیت فناوری بلاکچین	(	۰/۷۷	،	۰/۳۷	،	۰/۲۸	)	۰/۰۲
اثربخشی تغییرناپذیری فناوری بلاکچین	(	۰/۸۴	،	۰/۳۱	،	۰/۳۱	)	۰/۰۰۲
اثربخشی رمزهای رمزگذاری شده فناوری بلاکچین	(	۰/۸۴	،	۰/۳۳	،	۰/۲۲	)	۰/۱۵
اثربخشی ایجاد اعتماد در بین احزاب ناشناخته فناوری بلاکچین	(	۰/۸۳	،	۰/۳۷	،	۰/۲۱	)	۰/۰۰۴
اثربخشی علامت‌گذاری دارایی‌ها فناوری بلاکچین	(	۰/۸۵	،	۰/۵۹	،	۰/۵۲	)	۰/۰۲
عملیات اشتراک‌گذاری اسناد و اطلاعات با توجه به تفاوت‌های فنی و تکنولوژیکی	(	۰/۸۹	،	۰/۶۲	،	۰/۴۷	)	۰/۰۹
نقش فناوری بلاکچین در توانایی دسترسی افراد به سوابق	(	۰/۷۷	،	۰/۳۷	،	۰/۲۸	)	۰/۰۲
توانایی حفاظت از اطلاعات شخصی و منابع مالی کارتهای اعتباری	(	۰/۸۴	،	۰/۳۱	،	۰/۳۱	)	۰/۰۰۲
توانایی ایجاد امنیت در زمینه پرداخت‌ها و انجام تراکنش‌های مالی	(	۰/۸۴	،	۰/۳۳	،	۰/۲۲	)	۰/۱۵
نقش فناوری بلاکچین در شفافیت و مدیریت	(	۰/۸۳	،	۰/۳۷	،	۰/۲۱	)	۰/۰۰۴
نقش فناوری بلاکچین در جلوگیری از حملات سایبری و امنیتی	(	۰/۸۵	،	۰/۵۹	،	۰/۵۲	)	۰/۰۲

می‌کنند. همچنین از هشینگ به عنوان اهرمی در الگوریتم‌های اجماع به منظور اعتبارسنجی تبادل اطلاعات استفاده می‌شود و از نگرانی‌ها در حفظ حریم خصوصی هنگام انتقال داده می‌کاهد. همچنین از این فناوری می‌توان در راستای مدیریت آرشیوهای الکترونیکی و حرکت دولت در راستای تبدیل شدن به یک دولت الکترونیکی پایدار استفاده کرد. لذا یافته‌های پژوهش، در تطبیق با مطالعات کتابخانه‌ای انجام شده، نشان می‌دهد که چنانچه کشورمان بخواهد از این فناوری در آرشیوهای الکترونیکی و اسناد استفاده کند، می‌تواند از تجربیات کشوری مانند سوئیس الگوبرداری کند؛ مانند رای‌گیری الکترونیکی، ثبت املاک، شناسایی دیجیتال، اعطاء و ابطال گواهینامه‌های رانندگی، رسیدگی به داده‌های پزشکی، بانکداری، بیمه‌ها و غیره. ارزش عملیاتی بکار بردن این فناوری، کاهش از هزینه‌های اقتصادی، صرفه‌جویی در وقت و کاستن از پیچیدگی در مبادلات اطلاعات مابین سازمان‌های دولتی و همچنین مابین سازمان‌های عمومی - خصوصی است.

به‌کارگیری این فناوری، به دلیل استفاده از دفاتر توزیع‌شده و قراردادهای هوشمند الکترونیکی، به کاهش بوروکراسی، کاهش دخالت‌ها و اختیارات فردی، و کاهش فساد می‌انجامد. خودکارسازی در این فناوری، شفافیت، قابلیت ممیزی و پاسخگویی اطلاعات در مراجع ثبت دولتی و غیره را به نفع شهروندان فراهم می‌کند و در نهایت به گسترش اعتماد عمومی میان شهروندان می‌انجامد.

## مراجع

- [۱] ایزدی، سید کامیار، شریف‌خطیبی، زهرا (۱۳۹۹). بلاک‌چین و کاربرد آن در ذخیره اطلاعات به عنوان پایگاه داده توزیع شده امن. نشریه فناوری اطلاعات و ارتباطات انتظامی (فاوا)، دوره ۱، شماره ۲.
- [۲] بچاری، محمدرضا، نجفی، منصور (۱۳۹۷). بررسی کاربردهای فناوری بلاک‌چین در صنعت حمل و نقل دریایی. دومین همایش بین‌المللی مهندسی برق، علوم کامپیوتر و فناوری اطلاعات. تهران.
- [۳] بنویدی، مجید، ولی‌نیا، سید آرشد، سلمانی، یونس (۱۳۹۷). نقش بلاک‌چین بر صنعت بیمه با رویکرد بهبود فرایندها. بیست و پنجمین همایش ملی بیمه و توسعه، تهران، پژوهشکده بیمه.
- [۴] رضائی، مهدی، طائی‌زاده، علی (۱۳۹۸). تاثیر بلاک‌چین بر گردش اطلاعات زنجیره تامین. مدیریت اطلاعات، دوره ۵، شماره ۱.
- [۵] شهبازی، محمد، پوریان، سید کاظم، تقوا، محمدرضا (۱۳۹۹). بررسی کاربردی الگوریتم‌های اجماع استفاده شده در شبکه‌های بلاک‌چین. سیاست نامه علم و فناوری، دوره ۱۰، شماره ۳.
- [6] Abeyratne, S. A. (2016). Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*, 5(9), 1–10. <https://doi.org/10.15623/ijret.2016.0509001>
- [7] David, B. , Safa, O. , Nikolas, S. , Dylan, P. , Yaser, J. (2021). A Survey on Blockchain for Information Systems Management and Security. *Information Processing and Management*, 58 (2021), 102397.
- [8] Ghamari F, Mohammadbeigi A, Mohammadsalehi N, Hashiani A. (2011). Internet addiction and modeling its risk factors in medical students, Iran. *Indian J Psychol Med* 2011 ;33: 1562-68.

- [9] Intan, P. , Essaid, M. Kim, H. and Ju, H. 2020. Blockchain Implementation to Verify Archives Integrity on Cilegon E-Archive. Appl. Sci. 2020, 10, 2621; doi: 10.3390/app10072621.
- [10] Karafiloski, E. , Mishev, A. , (2017). "Blockchain solutions for big data challenges: A literature review," in IEEE EUROCON 2017 -17th International Conference on Smart Technologies, pp. 763–768, 2017.
- [11] Klomp, Laurens. (2018). The impact of blockchain technology on insurance business models, Master thesis submitted to Delft University of Technology.
- [12] Lemieux, V. L. (2017). A Typology of Blockchain Recordkeeping Solutions and Some Reflections on their Implications for the Future of Archival Preservation, 2017 IEEE International Conference on Big Data, Boston, MA, 2017, pp. 2271–2278.
- [13] Lemieux, V. L. (2017). A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. Proceedings of the 2017 IEEE International Conference on Big Data, Boston, MA, USA, 2271–2278. <https://doi.org/10.1109/BigData.2017.8258180>
- [14] Liang, X. , Shetty, S. , Tosh, D. , Kamhoua, C. , Kwiat, K. , Njilla, L. , 2017. "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," in (2017) 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 468–477, 2017.
- [15] Wynd CA, Schmidt B, Schaefer MA. 2003. Two quantitative approaches for estimating content validity. West J Nurs Res 2003; 25(5): 508-18. Zheng, Z. S. Xie, H. Dai, X. Chen, and H. Wang An. 2017. Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 2017 IEEE 6th International Congress on Big Data, Honolulu, HI, 2017, pp. 557–564.





## مشروعیت آورده‌های اقتصادی بازی‌های دیجیتال

مهدی اخلاصی<sup>۱</sup>، جهانگیر رخسندگان<sup>۲</sup>، علی رستمی<sup>۳</sup>

<sup>۱</sup> دانش‌آموخته مرکز فقهی ائمه اطهار علیه‌السلام، قم، ایران  
ekhlasi.m97@gmail.com

<sup>۲</sup> دانش‌پژوه مرکز فقهی ائمه اطهار علیه‌السلام، قم، ایران  
rakhshandegan73@gmail.com

<sup>۳</sup> استاد سطوح عالی حوزه علمیه و دانش‌پژوه مرکز فقهی ائمه اطهار علیه‌السلام، قم، ایران  
alirostami14555@gmail.com

### چکیده

بازی‌های دیجیتال به‌عنوان بخشی از فناوری‌های نوین به یکی از پرطرفدارترین روش‌های تفریحی - اقتصادی تبدیل شده است که اکثر مخاطبین آن را جوانان تشکیل می‌دهند و با گسترش و توسعه شبکه اینترنت، این حضور رشد بیشتری خواهد یافت. هیجان، دستیابی به مبالغ زیاد آن هم در زمان کم، از مهم‌ترین عوامل جذب در این نوع از بازی‌ها به شمار می‌روند؛ بنابراین واکاوی حکم شرعی آورده‌های اقتصادی بازی‌های دیجیتال امری ضروری است. در این میان، مجازی بودن، آنلاین بودن، نبود قوانین مشخص و تهیه بازی‌ها توسط شرکت‌های خارجی همگی از مسائلی است که تحقیق در این زمینه را با چالش مواجه می‌سازد. از همین رهگذر، نوشتار حاضر کوشیده است تا آورده‌های اقتصادی بازی‌های دیجیتال را در قالب دو گروه ارائه‌کنندگان و کاربران بازی‌های دیجیتال مورد تحلیل قرار دهد. نتایج به دست آمده که بر مدار روش تحلیلی - توصیفی سامان یافته، حاکی از آن است که آورده‌های اقتصادی ارائه بازی‌های دیجیتال در صورتی مشروع قلمداد می‌شوند که از موانعی همانند: تقویت کفر، گمراه‌کننده بودن، اهانت به مقدسات و ابزار قمار بودن، خالی باشند. درآمدهای مالی کاربران نیز اگر از راه شرط‌بندی و برد و باخت به دست آمده باشد، حرام است. نسبت به جوایز مسابقات در قالب بازی‌های دیجیتال نیز اگر منبع تأمین جایزه از پرداختی‌های شرکت‌کنندگان باشد، قمار بوده و دریافت آن حرام و برنده مالک آن نخواهد بود و در غیر این صورت، دریافت آن بی‌اشکال است.

**کلمات کلیدی:** بازی دیجیتال، قمار، مسابقه، برد و باخت، استریم، تستر.

## ۱ مقدمه

بازی‌های دیجیتال به‌عنوان بخشی از فناوری‌های نوین به یکی از پرطرفدارترین روش‌های تفریحی - اقتصادی تبدیل شده است؛ به طوری که شاهد حضور طولانی اشخاص در سایت‌های بازی‌های آنلاین هستیم که اکثر مخاطبین آن را جوانان تشکیل می‌دهند و با گسترش و توسعه شبکه اینترنت، این حضور رشد بیشتری خواهد

یافت. جلوه‌های ویژه، دستیابی به مبالغ زیاد آن هم در زمان کم به همراه هیجان، از مهم‌ترین عوامل جذب در این نوع از بازی‌ها به شمار می‌رود. از این رو، یکی از مسائل مهمی که می‌بایست مورد بررسی قرار گیرد، حکم شرعی اموال به دست آمده در خلال این بازی‌ها است. بازی‌های دیجیتال از جهات مختلفی می‌توانند موجب درآمدزایی شوند که در این نوشتار از منظر ارائه‌کنندگان و کاربران مورد تبیین قرار می‌گیرد. درآمدهای ناشی از برد و باخت (مراهنه)، شرکت در مسابقات بازی‌های الکترونیک از جمله درآمدهای کاربران است که نیازمند بحث و بررسی است؛ چرا که این معاملات در بستر فضای مجازی و آنلاین صورت می‌پذیرد و لازم است که شرایط صحت و موانع آن‌ها تحلیل شود. همچنین تحلیل شرایط لازم در ارائه و فروش بازی‌ها از دیگر نکاتی است که نیازمند نگرش فقهی است. در زمینه پژوهش‌های صورت‌گرفته در بازی‌های دیجیتال، اگرچه احکام درآمد بازی‌ها به صورت سنتی در بیشتر کتب فقهی وجود دارد، اما تبیین این بحث در فضای مجازی با تفاوت‌هایی روبه‌رو است. از میان مقالات انتشار یافته نیز «موضوع‌شناسی قمار در پرداخت‌های پس از باخت در بازی‌های رایانه‌ای» اثر محمدعلی خادمی کوشا و محمود عبداللہی به موضوع‌شناسی پرداخت‌ها در بازی پرداخته است. «ابعاد فقهی و حقوقی بازی‌های مجازی» نوشته‌ی ابراهیم عبدی‌پور فرد و مرتضی وصالی ناصح از دیگر آثار است که در این زمینه به رشته تحریر در آمده است. «وضعیت حقوقی معاملات درون بازی‌های مجازی» اثر دیگری از همین نویسندگان است. با تمامی این آثار همچنان عرصه درآمدزایی از طریق بازی‌های مجازی نیازمند پژوهش‌های فراوان است، زیرا روز به روز بر پیچیدگی و گستردگی ابعاد صنعت بازی افزوده می‌شود. بدین منظور، در پژوهش پیش رو که با تکیه بر گردآوری اطلاعات به صورت کتابخانه‌ای و روش توصیفی، تحلیلی سامان یافته است؛ به بررسی آورده‌های اقتصادی بازی‌های دیجیتال از نظرگاه فقه پرداخته شده است.

## ۲ اقسام آورده‌های اقتصادی بازی‌های دیجیتال و احکام آن

با نگرشی بر جنبه‌های اقتصادی بازی‌های دیجیتال می‌توان آورده‌های آن را در دو محور مورد واکاوی قرار داد.

### ۱.۲ درآمدهای مالی کاربران بازی‌های دیجیتال

برخی از بازی‌های دیجیتال به گونه‌ای طراحی شده‌اند که قابلیت درآمدزایی بالایی را برای کاربران فراهم می‌نمایند. در ادامه به اقسام این قابلیت‌ها و حکم شرعی آن‌ها می‌پردازیم:

#### ۱.۱.۲ درآمد مالی حاصل از شرط‌بندی (مراهنه)

در بسیاری از مواقع روال بازی‌ها به این شکل است که گیمرها و کاربران پول یا کالای ارزشمندی را گرو گذاشته و اقدام به بازی و غلبه بر دیگری می‌نمایند و فرد برنده در نهایت صاحب جایزه مذکور می‌شود. از منظر فقهی چنین درآمدی باطل بوده و هیچ‌یک از افراد مالک پول نمی‌باشند (شیخ انصاری، ۱۴۱۵ ق، ج ۱، ص ۳۷۲). شایان ذکر است که در فرایند مذکور آنچه از نقشی بنیادین برخوردار است، مالی است که به

عنوان گرو و رهن قرار داده شده است. بنابراین در باطل بودن درآمد حاصل شده، تفاوتی میان ابزار بازی از لحاظ ساختار ماهوی آن (مانند مختص قمار بودن) وجود ندارد. بر همین اساس همان گونه که حکم به حرمت درآمد مذکور در بستر ابزار مختص برد و باخت و قمار مطرح گردیده (نجفی، بی تا، ج ۲۲، ص ۱۰۹)، در ابزار با قابلیت قمار (نه مختص قمار) (خویی، بی تا، ج ۱، ص ۳۷۷) و ابزار بیگانه با برد و باخت، مانند گردو یا تخم مرغ (کلینی، ۱۴۰۷ ق، ج ۵، ص ۱۲۴) نیز همین حکم جاری است. در بیان مستند نامشروع بودن درآمد ناشی از همراهی از سوی طرفین بازی می توان به روایت علاء بن سیابه تمسک کرد. در این روایت آمده است: «از امام صادق علیه السلام درباره اعتبار گواهی کسی که کبوتر باز است، پرسش نمودم. امام علیه السلام فرمودند: اشکال ندارد در صورتی که به فسق شناخته نشود. گفتم برخی می گویند عمر آن را شیطانی دانسته است؛ امام علیه السلام فرمودند: سبحان الله، آیا نمی دانی رسول خدا صلی الله علیه و آله می فرماید: همانا فرشتگان به هنگام گروگذاری و شرط بندی بیزاری می جویند و صاحب گرو را لعن می کنند؛ مگر در مسابقه حافر (اسب و استرسواری)، خف (شترسواری)، ریش (تیراندازی) و نصل (پرتاب نیزه) که فرشتگان در این موارد حاضر می شوند. همانا رسول خدا صلی الله علیه و آله با اسامه مسابقه دادند و مسابقه اسب سواری برگزار کردند» (شیخ صدوق، ۱۴۱۳ ق، ج ۳، ص ۴۸). این روایت حکایت گر بغض ملائکه نسبت به بازی رهنی است و لعن بازیکنان نیز حرمت این عمل را در پی خواهد داشت (شیخ انصاری، ۱۴۱۵ ق، ج ۱، ص ۳۷۷)؛ زیرا لعن اگر چه در موارد کراهت نیز استعمال می شود، اما کاربرد این واژه بدون قرینه گویای حرمت فعل است، بلکه استعمال بیشتر این واژه در خصوص محرمات است؛ بنابراین شبهه ای در ظهور حرمت نیست (امام خمینی، ۱۴۱۵ ق، ج ۲، ص ۳۳). در این میان با توجه به آن که این عقد فاسد است، نمی توان آثار ملکیت را در مورد آن جاری دانست زیرا سبب تملک در آن وجود ندارد؛ در نتیجه وضعاً نیز حکم به فساد می شود (شیخ انصاری، ۱۴۱۵ ق، ج ۱، ص ۳۷۷) و از آن جایی که لازم است که اموال و درآمدهای حاصل شده از راه حرام به صاحبان آن عودت داده شود (شهید ثانی، ۱۴۱۳ ق، ج ۳، ص ۱۲۹) و تصرف در آن «تصرف در مال غیر» بوده و عمل حرامی به شمار می رود؛ در مورد مال به دست آمده از طریق برد و باخت نیز همین حکم جاری است. از این رو، شیخ انصاری می نگارد: «در صورت فساد معامله نسبت به عوض دریافتی لازم است که عین آن در صورت موجود بودن به مالکش بازگردانده شود و اگر تلف شده، بدل (مثل یا قیمت) جایگزین می شود» (ر.ک: انصاری، ۱۴۱۵ ق، ج ۱، ص ۳۷۹؛ خویی، بی تا، ج ۱، ص ۳۷۸).

## ۲.۱.۲ درآمد های مالی حاصل از شرکت در مسابقات رقابتی بازی های دیجیتال

مسابقات بازی های کامپیوتری که اصطلاحاً به آن ها «ESport» گفته می شود، جایزه های بسیار پرارزشی دارند. از این رو، یکی از مهم ترین منابع درآمد در دنیای بازی های دیجیتال، شرکت در مسابقات است. ساختار مسابقات با در نظر گرفتن منابع درآمد آن متفاوت است؛ به طوری که در برخی از مسابقات از شرکت کنندگان پولی دریافت شده و مجموع آن در پایان بازی به فرد برنده به عنوان جایزه پرداخت می شود و گاهی نیز منبع جایزه از سوی دیگران (ناظران و مجریان) تهیه می شود که در حکم شرعی تأثیرگذار است. در ادامه به بررسی حکم هر یک از این بازی ها و جوایز پرداخت شده می پردازیم.

**تأمین منبع پرداختی از سوی شرکت‌کنندگان.** در مسابقاتی که در بستر فضای مجازی و در قالب بازی‌های دیجیتال برگزار می‌شود و ساختار آن بر اعطای جایزه مبتنی شده و تأمین‌کننده‌ی منابع آن نیز اعضای شرکت‌کننده هستند، فرد برنده مجاز به دریافت جایزه نبوده و نمی‌تواند در جایزه تصرف نماید. به دیگر سخن، اگر مالی که به عنوان جایزه تعیین می‌شود از سوی شرکت‌کنندگان تأمین شود، نامشروع است (ر.ک: علامه حلی، بی‌تا، ص ۳۵۴؛ حائری طباطبایی، ۱۴۱۸ ق، ج ۱۰، ص ۲۳۷)؛ همان‌گونه که در پاسخ آیت‌الله صافی نیز آمده است: «حرمت دایر مدار این است که کسانی که پول می‌دهند در این کار برنده یا بازنده شوند» (صافی گلپایگانی، ۱۴۱۷ ق، ج ۱، ص ۳۰۴، سؤال ۱۰۴۷). در مقام مستندسازی این حکم می‌توان از روایت عبدالله بن سنان بهره برد که در آن آمده است: «عَنْ أَبِي عَبْدِ اللَّهِ عَلَيْهِ السَّلَامُ قَالَ سَمِعْتُهُ يَقُولُ لَا سَبَقَ إِلَّا فِي خُفٍّ أَوْ حَافِرٍ أَوْ نَضَلٍ يَعْني النَّضَالُ؛ جز در این سه مورد نمی‌توان مسابقه برگزار کرد: شترسواری، اسبسواری و تیراندازی» (کلینی، ۱۴۰۷ ق، ج ۵، ص ۴۸). در این روایت واژه «سبق» به دو نحو (سبق) به فتح باء و (سبق) به سکون باء قرائت شده است. حال با در نظر گرفتن قرائت (سبق) به سکون باء، مفاد روایت عدم مشروعیت مسابقه و در نتیجه حرمت انجام آن خواهد بود (کرکی، ۱۴۱۴ ق، ج ۸، ص ۳۲۶) و در صورت پذیرش قرائت (سبق) به فتح باء نیز مقتضای روایت نامشروع بودن عوضی است که از راه مسابقه تحصیل شده است (شیخ طوسی، ۱۳۸۷ ق، ج ۶، ص ۲۸۹). شهید ثانی معتقد است که قرائت روایت فتح از شهرت بیشتری در میان محدثین برخوردار است (شهید ثانی، ۱۴۱۳ ق، ج ۶، ص ۷۰). با عنایت به هر دو قرائت، درآمد مالی حاصل از مسابقات امری نامشروع است زیرا در صورت قرائت فتح که روشن است و نسبت به قرائت سکون نیز در صورتی که معنا عدم مشروعیت مطلق مسابقات (غیر موارد مستثنا) باشد، انجام و دریافت عوض در مقابل آن نیز امری نامشروع خواهد بود.

**تأمین منبع پرداختی از سوی سایرین.** در بسیاری از محافل برای ترویج یا تشویق به انجام عملی، مسابقاتی را برگزار می‌نمایند که به دلایل مختلف: همچون مخاطبین جوان و جذابیت بازی‌های پویانمایی، این مسابقات در بستر بازی‌های رایانه‌ای شکل می‌گیرد و فرد برنده نیز از سوی ناظران و یا عاملان برگزارکننده جوایزی را دریافت می‌نماید. در برخی موارد نیز باهدف جذب کاربر برای بازی‌های جدید، جوایزی را در آن پیش‌بینی می‌نمایند. از منظر فقیهان شرکت در چنین مسابقاتی و دریافت جایزه برای اشخاص منعی نداشته و فرد برنده می‌تواند در جایزه دریافتی تصرف نماید. آیت‌الله تبریزی می‌نگارد: «برای مسابقات علمی، می‌شود جایزه تعیین کرد و جایزه آن است که شخص یا مؤسسه‌ای غیر از مسابقه‌دهندگان، آن را می‌پردازند» (تبریزی، بی‌تا، ج ۱، ص ۲۰۴، سؤال ۹۸۰). مستند این حکم نیز انحصار حرمت در درآمد مالی میان شرکت‌کنندگان دانسته شده است؛ زیرا چیزی که دریافت جایزه را توسط فرد برنده با مخاطره مواجه می‌کند، تأمین آن از ناحیه شرکت‌کنندگان در مسابقه بود که عنوان رهن بر آن اطلاق می‌شد. از این رو، اگر جایزه مذکور از ناحیه فرد دیگری پرداخت شود، منعی ندارد، زیرا در کتب لغت، رهن (گرو) را به بردو باختی معنا کرده‌اند که در میان شرکت‌کنندگان جریان داشته باشد (ر.ک: ابن‌منظور، ۱۴۱۴ ق، ج ۱۳، ص ۱۸۹؛ طریحی، ۱۳۷۵ ش، ج ۶، ص ۲۵۹).

## ۲.۲ درآمدهای مالی سازندگان و ارائه‌کنندگان بازی‌های دیجیتال

ارائه بازی‌های دیجیتال در قالب‌های مختلفی همانند: فروش نسخه اصلی بازی، فروش اکانت یا کاراکترهای بازی صورت می‌پذیرد. برای بیان حکم این معاملات لازم است که شرایط بیان شده در معاملات مورد توجه قرار گیرد که در صورت تمامیت آن‌ها و نبود موانع، حکم به صحت این معاملات خواهد شد. بر این اساس، بحث را در دو محور پی می‌گیریم.

### ۱.۲.۲ محور اول: بررسی شرایط صحت در قراردادهای ارائه بازی

بازی‌ها عمدتاً به دو نحو فروش یا اجازه بهره بردن از بازی در دسترس مشتریان قرار می‌گیرند که نیازمند تحلیل است.

#### ۱. درآمدهای ناشی از ارائه نسخه و کاراکترهای بازی دیجیتال

نسبت به صحت معاملات در ارائه نسخه و کاراکترهای بازی دیجیتال لازم است که پارامترها و شرایط لازم در مبيع واقع شدن بازی‌ها مورد بررسی قرار گیرد.

(آ) **مالیت بازی‌ها.** یکی از شرایط اساسی در کالاها و مبادلات تجاری و شرعی، مالیت داشتن کالا و جنس مورد نظر است، به طوری که برخی از فقیهان وجود مالیت را به عنوان اولین شرط در معاملات مطرح نموده‌اند. تعاریف مختلفی از سوی فقیهان در تبیین و تحلیل مالیت صورت پذیرفته است. از کلمات علامه حلی چنین برداشت می‌شود که مال عبارت است از آنچه در آن منفعت مقصوده وجود داشته و شارع مقدس نیز آن را حلال دانسته باشد، از این رو هر آنچه دارای منفعت مقصوده نبوده و یا شارع منفعت آن را ساقط کرده است، به عنوان مال اعتبار نمی‌شود (حلی، بی تا، ج ۱۰، ص ۳۵). شهید اول نیز مال را آن چیزی می‌داند که قابلیت انتفاع داشته باشد (بی تا، ج ۲، ص ۲۳۹). از منظر شیخ انصاری مال چیزی است که در نزد عقلاء دارای منفعت مقصوده باشد و این منفعت نیز از نظر شارع مجاز دانسته شده باشد (۱۴۱۵ ق، ج ۴، ص ۹). به دیگر سخن مال چیزی است که وجود منفعت و رغبت ناشی از دست یافتن به آن و رفع نیاز از این راه باعث شده است که عقلاء برای تهیه آن هزینه نمایند (امام خمینی، بی تا، ج ۱، ص ۳۷). با عنایت به آنچه بیان شد، نسخه بازی‌های دیجیتال و نیز اکانت آن‌ها و همچنین کالاها و اجناسی که در حین بازی برای بالا بردن کیفیت و تنوع بازی مورد معامله قرار می‌گیرند، دارای وصف مالیت هستند، چون کاربران باهدف تجهیز منابع و ارتقاء وضعیت خود در بازی، اقدام به خرید آن‌ها می‌کنند. بنابراین در این گونه معاملات یک منفعت عقلایی و عرفی متصور است و همین امر برای آن‌ها ارزش اقتصادی به همراه داشته و سبب می‌شود قابلیت دادوستد را پیدا کنند.

(ب) **عینیت.** از قیود اساسی معاملات، مسئله «عینیت» است (شیخ طوسی، ۱۳۸۷ ق، ج ۲، ص ۷۶؛ خوبی، بی تا، ج ۲، ص ۱۰) و این در حالی است که بستر بازی‌های مجازی و دادوستدهای

درون آن، همه در محیط اینترنت اتفاق می‌افتد، بنابراین آنچه مورد خرید و فروش قرار می‌گیرد، مجازی یا به عبارتی غیرواقعی است. در متون فقهی معنایی که از «عین» اراده شده، جسمی است که وجود خارجی دارد (مروج، ۱۴۱۶، ق، ج ۱، ص ۳۳). محقق خویی در تعریف عین می‌نگارد: مراد از عین چیزی است که اگر در عالم خارج ایجاد شود به صورت یک جسم سه‌بعدی نمایان می‌گردد (خویی، بی‌تا، ج ۲، ص ۱۶). سید صادق حسینی روحانی در تعریف عین می‌نویسد: مراد از عین همان موجود متعین خارجی است و یا این‌که اگر در بیرون و عالم خارج موجود شود، از امور متعین خواهد بود (بی‌تا، ص ۳۰۱). نکته‌ای که در این میان وجود دارد آن است که این قید برای خارج کردن منافع است (شیخ انصاری، ۱۴۱۵، ق، ج ۳، ص ۷)، بنابراین نمی‌توان منافع یک کالا را فروخت. از این رو، مستندات امضای معادله بیع تنها نقل اعیان را در برمی‌گیرد (خویی، بی‌تا، ج ۲، ص ۱۰). نسبت به عینیت بازی و آیکن های داخلی آن به نظر می‌رسد که تعریفی که از عین بیان شد، مشکلی را برای دادوستد در بازی‌های دیجیتال ایجاد نمی‌کند؛ چراکه در بستر فضای مجازی می‌توان شاهد عینیت برای این‌گونه از بازی‌ها بود، مخصوصاً با توجه به این نکته که عین مدنظر در مقابل منفعت معنا شده است. بر این اساس، در فضای مجازی می‌توان یک بازی را خرید و نصب کرد و یا آیکنی را برای ارتقاء بازی به آن افزود و در تمامی این موارد عین بودن محفوظ است. شایان ذکر است که این عینیت می‌بایست با توجه به فضای مجازی و بازی تعریف گردد.

## ۲. درآمدهای ناشی از اجازه استفاده از بازی دیجیتال

از دیگر راه‌های درآمد در بازی‌های دیجیتال، دریافت مال در ازای حق بازی است؛ به دیگر سخن شرکت سازنده کاربرهای خود را مالک بازی نمی‌کند، بلکه تنها به آن‌ها اجازه دسترسی می‌دهد، بنابراین گیمرها تنها حق انتفاع از بازی را دارند. سؤالی که در میان مطرح می‌شود آن که آیا می‌توان در مقابل این حق انتفاع، مالی دریافت کرد؟ پاسخ آن که حق از اموری است که مورد توجه عقلا بوده و دادوستد می‌شود. امام خمینی در این باره می‌نویسد: حق در منظر عرف مال به حساب می‌آید، چراکه عقلاء به آن رغبت داشته و در ازای آن مال پرداخت می‌نمایند و این اعتبار در نزد عقلاء کاشف از مالیت عرفی است (۱۴۲۸، ق، ص ۶۵). آیت‌الله میلانی نیز می‌نگارد: اطلاق مال بر یک شیء با دلیلی مانند توجه نفوس و پرداخت ازای در مقابل آن است و یا این‌که میل به زوال دارد (از دسترس عموم خارج می‌شد) و با این اوصاف حق از مصادیق مال خواهد بود (میلانی، ۱۳۹۵، ق، ص ۳۵). آیت‌الله سید صادق خویی نیز از مدافعان مالیت عرفی حقوق به شمار می‌رود (بی‌تا، ج ۲، ص ۴۳). آیت‌الله سید صادق حسینی روحانی نیز به مالیت حقوق از همین منظر تصریح می‌نماید (روحانی، بی‌تا، ج ۱۵، ص ۲۰۸). با عنایت به آنچه گذشت، ارائه این حق و دریافت پول در مقابل آن بی‌اشکال است؛ بنابراین دریافت پول در بازی‌های آنلاین که در عوض بهره‌بری از بازی دریافت می‌شود، امری مشروع است. همین‌طور در صورتی که بازی‌ساز نسبت به برنده شدن پولی دریافت نکرده و آن را به‌عنوان تشویق برای ادامه بازی در نظر می‌گیرد، اما در صورت باخت گیمر پولی را که از حساب وی کسر نماید و یا اقدام به



دریافت پول کند، اگر بر اساس حق بازی صورت گیرد، به نظر می‌رسد بی‌اشکال باشد.

### ۳. درآمدهای ناشی از استریم

کاربرهای فراوانی وقت خود را صرف تماشای بازی کردن دیگران از طریق پخش زنده اینترنتی در سرویس‌هایی مانند توییچ می‌کنند که از آن به‌عنوان استریم (stream) یاد می‌شود. «استریم کردن» یا «اشتراک‌گذاری محتوا به صورت زنده» معمولاً به‌گونه‌ای از تولید و انتقال محتوا اطلاق می‌شود که هم‌زمان توسط گیرنده مصرف می‌شود و در مقابل «بارگیری» قرار می‌گیرد که در آن محتوای رسانه دریافت شده برای مصرف در آینده ذخیره می‌شود. به دیگر سخن استریم بدون دانلود پرونده، رسانه را پخش می‌کند، بنابراین فضای سخت‌افزاری برای دانلود یک برنامه را از بین نمی‌برد. در برخی موارد کاربران برای اشتراک در یک استریم خاص هزینه‌ای را به‌عنوان حق اشتراک پرداخت کنند که این اشتراک باید ماهانه تمدید شود تا مزایای آن حفظ شود. از منظر فقهی به نظر می‌رسد که دریافت هزینه در مقابل استریم به‌خودی‌خود مانعی نداشته باشد. از این‌رو، در صورتی که این عمل در بردارنده ضوابط شرعی باشد، بدین معنا که اصل بازی مجاز بوده، تبلیغ و ترویج امور باطل و حرام در آن صورت نپذیرد، دریافت پول از این طریق مشروع است.

### ۴. درآمد تسترهای بازی دیجیتال

از دیگر راه‌ها برای کسب درآمد با بازی‌های دیجیتال تستر بودن است. سازندگان بازی به آزمایش‌کنندگان بازی مبلغی را پرداخت می‌نمایند تا در محیطی که آن‌ها تعیین می‌کنند بازی‌ها را آزمایش کنند. هدف از این امر نیز آن است که اشکالات و نواقص احتمالی بازی از طریق یک گیمر، آن هم قبل از انتشار عمومی شناسایی و مرتفع گردد. در بررسی مشروعیت چنین درآمدی از سنجه فقه لازم است که محتوای این بازی‌ها مدنظر قرار گیرد؛ چراکه در اصل چنین عملی با توجه به رغبت سازندگان بازی و پرداخت هزینه اشکالی به ذهن نمی‌رسد، بنابراین در صورتی که بازی از عناوین ممنوعه‌ای که در بخش بعد مطرح باشد تهی باشد، درآمدهای مالی از این راه بی‌اشکال می‌نماید.

## ۲.۲.۲ محور دوم: بررسی موانع صحت در قرارداد ارائه بازی‌ها

در بهره‌بری از بازی‌های دیجیتال به‌عنوان عاملی برای تجارت و در نتیجه مشروع بودن درآمدهای آن، این نکته مهم است که کالاهای ارائه‌شده در صنعت بازی مجاز شناخته شده و نبایستی از کالاهای ممنوعه به شمار روند. در ادامه به برخی از عناوین ممنوع ساز اشاره می‌نماییم:

### ۱. ابزار قمار بودن

بخشی از بازی‌های ارائه‌شده در فضای دیجیتال تنها مصرف قمار داشته و بهره‌بری آن‌ها منحصر در حرام و فساد است. در چنین مواردی خرید و فروش این‌گونه از بازی‌ها ممنوع و درآمد مالی حاصل از آن امری فاسد قلمداد می‌شود (علامه حلی، ۱۴۲۰ ق، ج ۲، ص ۲۵۸). از مستندات می‌توان

در بیان حرمت تکلیفی و وضعی معاملات ابزار قمار بهره برد، روایت صحیحی است که بزنتی از امام صادق علیه السلام چنین نقل می‌نماید: «فروش شطرنج حرام و استفاده از بهای آن سحت و پلیداست» (حر عاملی، ۱۴۰۹، ق، ج ۱۷، ص ۳۲۳). این روایت بر حرمت وضعی و تکلیفی بیع شطرنج دلالت دارد (تقی طباطبایی، ۱۴۲۶، ق، ج ۷، ص ۲۰۱) و در این حکم، شطرنج خصوصیتی نداشته و شامل تمامی ابزار قمار می‌شود (حسینی روحانی، ۱۴۲۹، ق، ج ۱، ص ۱۷۷)؛ همان‌گونه که عموم تنزیل روایت صحیح معمر بن خلاد که در آن از امام رضا علیه السلام نقل می‌نماید که «بازی با تخته‌نرد، شطرنج و سه پرک به منزله یک چیزند» بیانگر تساوی در حکم است (امام خمینی، ۱۴۱۵، ق، ج ۱، ص ۱۷۳). شایان ذکر است که هرگونه انتفاع از ابزار قمار چه به‌طور مستقیم باعث درآمدزایی شود و چه غیرمستقیم مانند ارتقاء امتیاز سایت، نامشروع خواهد بود (نجفی، بی تا، ج ۲۲، ص ۲۵).

## ۲. گمراه‌کننده بودن

هرگونه کالایی که استفاده از آن در راستای تقویت کفر و شرک بوده و یا به‌واسطه آن حق موهن جلوه داده شود، خرید و فروش و حتی نگهداری آن نامشروع است (نراقی، ۱۴۱۵، ق، ج ۱۴، ص ۱۵۷). مستند این حکم فرازی از روایت تحف العقول است: «هر چه ممنوع شده از چیزهایی که به‌وسیله آن‌ها به غیر خدا تقرب جویند یا به هر وسیله گناه آمیزی که کفر و شرک در سایه آن قدرت پیدا نماید یا هر بایی از ابواب که گمراهی به آن قدرت یابد یا بایی از باب‌های باطل را تقویت نماید، یا بایی که حق به‌وسیله آن تضعیف گردد، همه این‌ها حرام است. خرید و فروش، نگه‌داشتن، مالک شدن، بخشیدن، عاریه دادن و هرگونه تصرف در آن‌ها حرام است» (حر عاملی، ۱۴۰۹، ق، ج ۱۷، ص ۸۴).

## ۳ نتیجه

یکی از راه‌های درآمدزا که در عصر حاضر با پیشرفت صنعت بازی‌سازی شاهد آن هستیم، درآمد از طریق بازی‌های دیجیتال است که روش‌های متعددی را به خود اختصاص داده است. در این نوشتار برخی از آن‌ها مورد واکاوی قرار گرفت. براین اساس؛ درآمدهای قمار گونه امری نامشروع قلمداد گردید. مسابقات رقابتی از دیگر طرق درآمد در این بازی‌ها است که بیان گردید جایزه دریافتی در صورتی مجاز است که از سوی غیر شرکت‌کنندگان تحصیل شده باشد چرا که در غیر این صورت ملحق به قمار خواهد بود. فروش و ارائه بازی‌های دیجیتال دیگر موضوعی بود که در این نوشتار با تأکید بر دو شرط مالیت و عینیت مورد تحلیل قرار گرفت و بیان شد که با توجه به وجود رغبت و منافع موجود در این کالاها و عدم ردع شارع مقدس، مالیت این کالا قابل پذیرش بوده و تفاوتی میان پرداخت هزینه برای خرید اصل بازی، کاراکترهای داخل بازی یا مراحل آن وجود ندارد. همچنین نسبت به شرط عینیت نیز علاوه بر اجماعی نبودن این شرط، عین بودن بازی‌ها در بستر فضای مجازی امری بی‌اشکال است. مشروعیت درآمدهای حاصل از طریق اشتراک‌گذاری محتوا به‌صورت زنده و همکاری در ساخت و رفع نقایص بازی‌ها نیز مبتنی بر اصل بازی است، بدان معنا که در صورت مشروع بودن اصل بازی، چنین فعالیت‌هایی نیز مجاز شناخته می‌شوند. در پایان بر این نکته بنیادین تأکید

شد که بازی‌های دیجیتالی نایستی به‌عنوان ابزار قمار شناخته شده و یا در این راستا قرار بگیرند که ابزاری گمراه‌کننده و موهن حق قلمداد شوند، زیرا در این صورت هرگونه دادوستد آن‌ها حرام خواهد بود.

## مراجع

- [۱] خادمی کوشا، محمدعلی و محمود عبداللهی، موضوع شناسی قمار در پرداخت‌های پس از باخت در بازی‌های رایانه‌ای، جستارهای فقهی و اصولی، ش ۲۷، ۱۴۰۱ ش.
- [۲] انصاری، مرتضی، کتاب الطهارة، کنگره جهانی بزرگداشت شیخ اعظم انصاری، قم - ایران، اول، ۱۴۱۵ ه.ق.
- [۳] نجفی، محمدحسن، جواهر الکلام فی شرح شرایع الاسلام، دار احیاء التراث العربی، بیروت - لبنان، هفتم. بی تا.
- [۴] خوبی، سید ابوالقاسم، مصباح الفقاهة، ۷ جلد. بی جا، بی تا.
- [۵] کلینی، محمد بن یعقوب، الکافی، ۸ جلد، دار الکتب الإسلامية، تهران، چهارم، ۱۴۰۷ ه.ق.
- [۶] صدوق، محمد بن علی بن بابویه، من لا یحضره الفقیه، ۴ جلد، دفتر انتشارات اسلامی، قم - ایران، دوم، ۱۴۱۳ ه.ق.
- [۷] امام خمینی، سید روح‌الله، مکاسب المحرمة، مؤسسه تنظیم و نشر آثار امام خمینی قدس سره، قم، اول، ۱۴۱۵ ه.ق.
- [۸] شهید ثانی، زین‌الدین بن علی، مسالك الأفهام إلى تنقیح شرایع الاسلام، مؤسسه المعارف الإسلامية، قم، اول، ۱۴۱۳ ه.ق.
- [۹] حلی، حسن بن یوسف بن مطهر، تذکرة الفقهاء، در یک جلد، مؤسسه آل‌البيت عليهم السلام، قم - ایران، اول، ه.ق.
- [۱۰] طباطبایی حائری، سید علی بن محمد، ریاض المسائل، مؤسسه آل‌البيت عليهم السلام، قم، اول، ۱۴۱۸ ه.ق.
- [۱۱] صافی گلپایگانی، لطف‌الله، جامع الأحكام، دو جلد، انتشارات حضرت معصومه سلام‌الله علیها، قم، چهارم، ۱۴۱۷ ه.ق.
- [۱۲] کرکی، علی بن حسین، جامع المقاصد فی شرح القواعد، مؤسسه آل‌البيت عليهم السلام، قم، دوم، ۱۴۱۴ ه.ق.
- [۱۳] شیخ طوسی، محمد بن حسن، المبسوط، المكتبة المرتضوية لإحياء الآثار الجعفرية، تهران، سوم، ۱۳۸۷ ه.ق.
- [۱۴] تبریزی، جواد بن علی، صراط النجاة، ۷ جلد، بی جا، بی تا.
- [۱۵] ابن منظور، محمد بن مکرم، لسان العرب، دار الفكر للطباعة و النشر و التوزيع - دار صادر، بیروت، سوم، ۱۴۱۴ ه.ق.
- [۱۶] طریحی، فخرالدین، مجمع البحرين، کتاب‌فروشی مرتضوی، تهران - ایران، سوم، ۱۴۱۶ ه.ق.
- [۱۷] شیخ طوسی، محمد بن حسن، الخلاف، دفتر انتشارات اسلامی، قم - ایران، اول، ۱۴۰۷ ه.ق.
- [۱۸] مروج جزایری، سید محمدجعفر، هدی الطالب فی شرح مکاسب، ۷ جلد، مؤسسه دارالکتاب، قم، اول، ۱۴۱۶ ه.ق.
- [۱۹] میلانی، سید محمدهادی، محاضرات فی فقه الإمامية - کتاب البیع، دانشگاه فردوسی، مشهد، اول، ۱۳۹۵ ه.ق.
- [۲۰] حسینی روحانی قمی، سید صادق، فقه الصادق علیه السلام، ۲۶ جلد، بی جا، بی تا.
- [۲۱] طباطبایی قمی، سید تقی، مبانی منهاج الصالحین، ۱۰ جلد، منشورات قلم الشرق، قم، اول، ۱۴۲۶ ه.ق.
- [۲۲] حرّ عاملی، محمد بن حسن، وسایل الشیعة، ۲۹ جلد، مؤسسه آل‌البيت عليهم السلام، قم، اول، ۱۴۰۹ ه.ق.
- [۲۳] نراقی، مولی احمد، مستند الشیعة فی أحكام الشریعة، مؤسسه آل‌البيت عليهم السلام، قم، اول، ۱۴۱۵ ه.ق.



## سئوی سایتهای فروش آنلاین کتاب و استفاده از فناوری واقعیت مجازی (مطالعه موردی)

مهشید التماسی<sup>۱</sup>

استادیار گروه علم اطلاعات و دانش‌شناسی، دانشکده مدیریت دانشگاه تهران  
eltemasi@ut.ac.ir

### چکیده

هدف این مطالعه بررسی میزان اثرگذاری استفاده از فناوری واقعیت مجازی در وبسایت فروشگاه اینترنتی کتاب تخصصی بر بهبود سئوی سایت است. رویکرد این تحقیق آمیخته است و در زمره تحقیقات کاربردی-توسعه‌ای قرار می‌گیرد. سؤال ۱، پیمایشی و پرسشنامه، سؤال ۲، پیمایشی تجربی، پیش‌آزمون و پس‌آزمون. از بین مؤلفه‌های سئوی سایت‌ها با تحلیل محتوای کمی متون ۱۱ مؤلفه به عنوان مؤلفه‌های اصلی سئوی سایت‌های فروش آنلاین استخراج شد. سپس بر اساس نظر متخصصان موضوعی ۷ مؤلفه اصلی تأثیرپذیر از محتوای واقعیت مجازی تعیین شد و سپس سایت فروش آنلاین کتاب سازمان مدیریت صنعتی برای آزمون میزان تأثیر محتوای واقعیت مجازی بر سئو، انتخاب شد. که نتیجه استفاده از واقعیت مجازی بر رؤیت‌پذیری آن نشان داد که رتبه سایت مذکور در بازبایی گوگل در مدت یک ماه بطور متوسط (بدون تبلیغ و اطلاع رسانی‌های عمده) ۴۵٪ بهبود داشته است، که می‌تواند بر اساس دو مؤلفه تعداد بازدیدکنندگان با افزایش تقریبی ۴۸٪ و مدت زمان حضور کاربران در سایت با افزایش تقریبی ۵۱٪ توجیه شود. بنا به نظر متخصصین حوزه سئو و واقعیت مجازی و فروشگاه‌های آنلاین استفاده از فناوری واقعیت مجازی در بهبود برخی آیتم‌های مرتبط با سئو می‌تواند تاثیرگذار باشد.

**کلمات کلیدی:** سئو، واقعیت مجازی، وبسایت کتابفروشی، فروش آنلاین، رتبه‌بندی گوگل.

### ۱ مقدمه

امروزه، اهمیت اینترنت و منابع اطلاعاتی موجود در آن به طور گسترده‌ای افزایش یافته که یکی از دلایل آن می‌تواند موتورهای جستجو و کارکردها و اهمیت آنها باشد (Manek et al, 2019). اینترنت از جمله فناوری‌های جدید است که در چارچوب رهیافت ارتباط توسعه‌ای می‌تواند روند توسعه کشورهای در حال توسعه را تسریع نماید. تاریخ این کشورها گواه براین مدعاست که انتقال فناوری بدون انطباق آن با شرایط اقتصادی، اجتماعی، فرهنگی و سیاسی کشور میزبان، به مثابه برهم زدن نظم داخلی و تعادل آن‌ها و نهایتاً سوق دادن آن‌ها به سمت کشوری نامتعادل است که بخش‌های مختلف آن زیر سیستم از یک فراسیستم ملی

نیستند. لذا به کارگیری و توسعه خدمات اینترنت در این کشورها نیازمند دقت، تخصص و مطالعه است تا ضمن در نظر گرفتن شرایط عمومی کشور میزبان و وقفه‌های تاثیرگذاری این فناوری جدید، فرایند علمی سازگاری و انطباق و نیز زمینه‌سازی و انطباق و نیز زمینه‌سازی در مورد آن صورت گیرد تا نهایتاً جامعه از منافع آن بهره‌مند شود و هدایت آن را بر عهده گیرد. اینترنت به بستری گسترده برای معاملات تجاری و رسانه‌ای قوی برای بازاریابی تبدیل شده است. آمارها نشان می‌دهند که تعداد کاربران اینترنت و تمایل به خرید و فروش از طریق اینترنت افزایش یافته‌اند [۵]. اینترنت، عامل تجاری مهمی است که سریع‌تر از هر فناوری ارتباطی دیگری رشد کرده و بازارهای جهانی را بیشتر از سایر فناوری‌های رسانه‌ای متحول کرده است [۳]. کسب و کارها به سوی الکترونیکی شدن پیش می‌روند و تجارت الکترونیک هر روز جلوه جدیدتری می‌یابد. یکی از جنبه‌های نوظهور در این عرصه پیدایش فروشگاه اینترنتی است [۵] و ارائه محصولات آنلاین مقدمه‌ای برای فروش محصولات و خدمات است و کسب درآمد از دیگر دستاوردهای اینترنت و محتویات آن تلقی می‌شود [۱۷]. در جهان، متوسط رشد استفاده از اینترنت بین سال‌های ۲۰۰۰ تا ۲۰۱۵ برابر با ۸.۹ درصد و در همان دوره زمانی در کشورهای خاورمیانه برابر با ۹.۸٪ بود. در ایران نیز چنین رشدی مشاهده می‌شود؛ بر همین اساس، شمار کاربران اینترنت در دسامبر ۲۰۱۴ در ایران، ۴۶ میلیون و ۸۰۰ هزار نفر بود؛ در حالیکه در ماه دسامبر سال ۲۰۰۰، تعداد کاربران حدود ۲۵۰ هزار نفر بوده است [۲]. شاید یکی از دلایل مهم در رشد این پدیده دسترسی به اطلاعات بیشتر برای انتخاب بهتر باشد؛ گسترش تجارت الکترونیک به مصرف‌کنندگان بیشتر و بهتر از خرید سنتی گزینه ارائه می‌دهد. بنابراین، توسعه خرید آنلاین می‌تواند اطلاعات موجود در محصولات را بهبود بخشد و هزینه‌های بررسی و تحقیق مصرف‌کنندگان را کاهش دهد.

در استفاده از اینترنت چه برای امور تحقیق و پژوهش و چه در خصوص خریدهای اینترنتی موتورهای جستجو با هدف یافتن موارد مورد نظر کاربران بطور گسترده استفاده می‌شود؛ که در ایران اغلب از موتور جستجوی گوگل استفاده می‌شود و لذا اینکه سایت‌ها، بتوانند در بازیابی‌های گوگل رتبه بالاتری داشته باشند و یا به عبارتی در صدر یافته‌ها باشند می‌تواند به آنها در افزایش دسترسی و دیده‌شدنشان کمک شایانی نماید. یکی از مواردی که همواره به عنوان راه حلی برای بهبود جایگاه وبسایت‌ها در رتبه‌بندی گوگل مطرح می‌شود مبحث سئو و رعایت مؤلفه‌های آن برای بهبود رویت‌پذیری سایت‌هاست؛ اما یکی از فناوری‌هایی که در حال حاضر به عنوان فناوری‌های برتر در حوزه کتاب و کتابخانه مطرح شده است فناوری واقعیت مجازی<sup>۱</sup> است؛ واقعیت افزوده، پُل میان جهان واقعی و مجازی است که با افزودن اطلاعات مجازی خلق شده توسط رایانه [۶، ۹، ۲۴] تعامل، دانش فردی و فهم کاربر را از جهان واقعی ارتقا می‌دهد [۸، ۹] در واقع، مفهوم ترکیب یا افزودن داده‌های مجازی مانند اطلاعات و رسانه‌های غنی به هر آنچه در دنیای واقعی می‌بینیم، با هدف افزایش اطلاعاتی است که می‌توانیم از طریق حواس خود درک نماییم [۱۴]. اما اینکه آیا استفاده از فناوری واقعیت مجازی در بهبود شاخص‌های سئو، به ویژه از نظر رتبه‌بندی در بازیابی موتور جستجوی گوگل موثر است یا خیر، یکی از کاربردهایی است که کمتر به آن توجه شده است. بنابراین هدف این مقاله بررسی میزان اثرگذاری استفاده از فناوری واقعیت مجازی در وبسایت فروش آنلاین کتاب بر بهبود سئوی سایت

<sup>۱</sup> Virtual Reality



این فروشگاه‌ها است. سئوالات اساسی که در این تحقیق مطرح هستند عبارتند از: فناوری واقعیت مجازی بر کدام یک از مؤلفه‌های سئوی وبسایت‌های فروش آنلاین موثر هستند؟ و آیا بین بهبود رتبه‌بندی گوگل و استفاده از فناوری واقعیت مجازی در وبسایت فروش آنلاین کتاب ارتباط وجود دارد؟

## ۲ مروری بر کارهای دیگران

دهدشتی و مبرهن (۱۳۹۱) پژوهشی با هدف بررسی تأثیر عوامل انگیزش فردی بر خرید اینترنتی انجام دادند. نتایج نشان داد که اگر مدیران بتوانند احتمال خرید مکرر را از طریق ارائه اطلاعات با کیفیت بالا در خریداران خود افزایش دهند، تمایل خریداران برای بازگشت به سایت افزایش خواهد یافت. در این راستا، می‌توان به مدیران فروشگاه‌های آنلاین پیشنهاد کرد که حس لذت‌جویی از زندگی را در خریداران تقویت کنند و افزون بر این، برای پاسخگویی به نیاز به برقراری روابط اجتماعی در افراد، امکانات چت و غیره را فراهم کنند. منتظری و همکاران (۱۳۹۳) عوامل موثر بر قصد خرید اینترنتی مشتریان را مطالعه کرده‌اند و نشان دادند که با ایجاد محیط امن و ارائه ضمانت‌های لازم تمایل به خرید آنلاین افزایش می‌یابد؛ چرا که ریسک درک‌شده مشتریان کاهش می‌یابد. این مهم با توجه به پیشامدهای شناختی، تجربی، شخصیتی و حالت عاطفی مشتریان نیز اتفاق می‌افتد. قنبریور (۱۳۹۳) نیز در پایان‌نامه ارشد خود با عنوان «نیازسنجی و امکان‌سنجی به کارگیری فناوری واقعیت افزوده در کتابخانه‌های دانشگاهی: دیدگاه متخصصان شاغل در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران» نشان داد که کتابخانه‌های مورد مطالعه دارای امکانات فنی اولیه مناسب و امکانات مالی در حد متوسط برای استفاده از فناوری واقعیت افزوده هستند و نیروی انسانی با مهارت‌های قابل قبول برای راه‌اندازی و پشتیبانی از این فناوری در کتابخانه‌های مورد مطالعه داشته‌اند. در مجموع چنین استنباط می‌شود که از دیدگاه مدیران و متخصصان شاغل در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران، استفاده از فناوری واقعیت افزوده در کتابخانه‌ها می‌تواند مزایای بسیار و کارایی بالایی داشته باشد.

دانگ می<sup>۲</sup> (۲۰۱۷) در مطالعه خود به دنبال تحلیل نگرش مشتریان نسبت به خرید آنلاین بود و نشان داد که چگونه عوامل اجتماعی و جمعیت‌شناختی مانند سن، درآمد، تحصیلات و شغل بر نگرش و وفاداری مصرف‌کنندگان خرید آنلاین تأثیر می‌گذارند. نتایج مطالعه وی نشان داد که بین ویژگی‌های وبسایت، عوامل محصول سرویس و عوامل انگیزشی با نگرش پاسخ‌دهندگان رابطه معناداری وجود دارد. همچنین، بین نگرش و وفاداری مشتریان نیز رابطه‌ای معنادار وجود دارد. هان<sup>۳</sup> (۲۰۱۲) در تحقیقی با هدف معرفی برنامه‌های کاربردی واقعیت مجازی تلفن همراه برای استفاده از کتابخانه و خدمات بعدی کتابخانه، نشان داد که از واقعیت مجازی تلفن همراه می‌توان برای افزودن اطلاعات به کتاب‌های سنتی، مرور و راهنمایی کتابخانه، تشخیص نوری، تشخیص چهره و نرم‌افزار موبایل شناسایی ساختمان و همچنین برای افزایش تجربیات جذاب کاربران کتابخانه، مثل تورهای کتابخانه و ... استفاده شود. چن و تسای<sup>۴</sup> (۲۰۱۲). در تحقیقی با عنوان واقعیت مجازی تعاملی سیستمی برای افزایش آموزش رسمی در مدارس ابتدایی، نشان دادند که واقعیت

<sup>2</sup>Dang mai

<sup>3</sup>Hahn

<sup>4</sup>Chen & Tsai.

مجازی می‌تواند نقش کتابدار را در آموزش استفاده‌کننده بازی کند، استفاده از آن می‌تواند تفاوت‌های مهارتی کتابداران را در آموزش کتابخانه‌ای از بین ببرد، یادگیری بهتر و بیشتر را فراهم کند، همچنین می‌تواند درک کاربران را از کتابخانه و خدمات آن افزایش دهند، و در نهایت عملکرد یادگیری شرکت‌کنندگان، تحت تأثیر واقعیت مجازی بهتر خواهد شد. ماسیس (۲۰۱۵)<sup>۵</sup> در تحقیق خود که با هدف توصیف زمینه‌های استفاده کتابخانه‌ها از مزایای واقعیت مجازی و افزوده انجام داد به این نتیجه رسید که فناوری‌های واقعیت مجازی و افزوده نه تنها به دلیل ایفای نقش مهمشان در افزایش رضایت و جلب مخاطب بلکه به دلیل نقش آن‌ها در آموزش مناسب و سواد اطلاعاتی و تقویت یادگیری نیز می‌توانند در کتابخانه‌ها به عنوان ابزاری مهم مطرح باشند. شات، هلدسورت و لی<sup>۶</sup> (۲۰۱۴) در تحقیقی عملیاتی با هدف طراحی و ارائه سیستم مدیریت کتابخانه بافت‌آگاه بر اساس واقعیت مجازی همراه، پس از طراحی این سیستم و آزمایش آن به این نتیجه رسیدند که ارائه سیستم بافت‌آگاه مبتنی بر تلفن همراه می‌تواند در بهبود مدیریت عملکرد و خدمات کتابخانه بسیار موثر باشد.

ایلود<sup>۷</sup> (۲۰۱۷) نیز در تحقیق خود با عنوان واقعیت مجازی و مجازی در کتابخانه‌ها و بخش آموزش، به تاثیر و نقش این فناوری‌ها در بهبود خدمات‌دهی کتابخانه‌ها و البته نقش آنها در بهبود آموزش و یادگیری مادام‌العمر پرداخته و نشان می‌دهد که میزان استفاده از این فناوری‌ها در غرب به شکل فزاینده‌ای به ویژه در این دو بخش رو به رشد است و دلیل آن هم می‌تواند هزینه مناسب آن و حتی رایگان بودن آن در برخی موارد باشد. اسکی و آرتلیش<sup>۸</sup> (۲۰۱۴)، استفاده وبگاه از پروتکل اچ‌تی‌تی‌پی‌اس به جای اچ‌تی‌تی‌پی را یکی از عوامل مؤثر بر سئو در موتور جستجوی گوگل دانسته‌اند و بیان کرده‌اند که کتابخانه‌ها نیز برای رشد خود باید این موضوع را رعایت نمایند تا در صفحات اولیه نتایج بازبایی‌شده‌ی موتور جستجوی گوگل بهتر دیده شوند. گنارو<sup>۹</sup> (۲۰۱۵)، در نوشتاری با عنوان «کوتاه و واضح: عنوان‌ها، کلمات کلیدی و بهینه‌سازی موتور جستجو»، معتقد است که در دنیای کتاب‌های چاپی، اگر نویسنده از عنوانی ناآشنا و غریب برای کتاب خودش، استفاده می‌کرد، مشکل خاصی نبود اما در دنیای دیجیتال کنونی، استفاده از عنوان مناسب برای جستجوی کاربر و به کار بردن کلمات کلیدی متناسب در همه متن نوشته بسیار مهم است زیرا باعث افزایش قابلیت بازدید و فهرست شدن در موتورهای جستجو خواهد شد.

کراباج و همکاران<sup>۱۰</sup> (۲۰۱۷)، یک وبسایت آموزشی را از منظر رعایت تکنیک‌های سئوی داخلی<sup>۱۱</sup> و سئوی خارجی<sup>۱۲</sup>، بررسی کرده‌اند و این تکنیک‌ها را موجب افزایش رتبه سایت در موتورهای جستجو دانسته‌اند. روش مورد استفاده آنها نیز روش مقایسه‌ای براساس چک‌لیست سئو بوده است. ساها و پال<sup>۱۳</sup> (۲۰۱۸)،

<sup>5</sup>Massis<sup>6</sup>Shatte, Holdsworth & Lee<sup>7</sup>Oyelude<sup>8</sup>Askey and Arlitsch<sup>9</sup>Gennaro<sup>10</sup>Krrabaj et al<sup>11</sup>Off-Page SEO<sup>12</sup>On-Page SEO<sup>13</sup>Saha and Paul

در پژوهشی بیان کرده‌اند که پژوهشگران بهتر است علاوه بر اینکه به موضوعاتی مانند انواع مدل‌های اقتصادی دسترسی آزاد مانند دسترسی آزاد سبز یا طلایی، در هنگام نوشتن و ارسال مقاله علمی خود، تسلط داشته باشند، و آن‌ها باید با تکنیک‌های سئو یا بهینه‌سازی موتور جستجو نیز آشنایی داشته باشند تا مقاله آن‌ها بیشتر دیده شود. مارکز و لی<sup>۱۴</sup> (۲۰۱۷)، در پژوهش خود با عنوان "افزایش رویت‌پذیری مقالات آنلاین" بیان کرده‌اند که عواملی مانند «اشتراک‌گذاری متن مقاله در چندین مکان»، «تبدیل متن مقاله از حالت پی‌دی‌اف بدون خوانش یا بدون فهرست‌شدن در موتورهای جستجو، به پی‌دی‌اف دارای قابلیت خوانش در موتورهای جستجو»، «استفاده از عنوان و چکیده و فراداده‌های مناسب»، منجر به ارتقای سئو و بازدید مقاله خواهد شد.

مروری اجمالی بر پیشینه‌های ارائه‌شده در بالا نشان می‌دهد که تقریباً تحقیقی با هدفی مشابه این نوشته پیش از این انجام نشده است و این مهم نشان می‌دهد که کمتر به تاثیر استفاده از فناوری واقعیت مجازی در ارتقای سئو و رتبه‌بندی سایت‌های مرتبط با کتاب توجه شده است و لذا با توجه به اهمیت رویت‌پذیری وبسایت‌ها در وب و ارتقای جایگاه وبسایت‌ها در موتورهای جستجو، به نظر می‌رسد انجام تحقیقی با هدف بررسی نقش استفاده از فناوری واقعیت مجازی در ارتقای سئوی این سایت‌ها می‌تواند در این راستا کمک‌کننده باشد.

### ۳ روش‌شناسی

با توجه به اهداف و سوالاتی که در این تحقیق مطرح است، رویکرد این تحقیق آمیخته بوده و در زمره تحقیقات کاربردی - توسعه‌ای قرار دارد. بنابراین برای بخش‌های مختلف آن از روش‌ها و ابزار مختلفی استفاده شده است و با توجه به اینکه تکنیک‌های کمی و کیفی را همزمان دارد، روش این تحقیق آمیخته می‌باشد:

**بخش اول:** با هدف پاسخ‌گویی به سؤال فناوری واقعیت مجازی بر کدام یک از مؤلفه‌های سئوی وبسایت‌های فروش آنلاین کتاب موثر هستند؟ بدین ترتیب انجام شد: ابتدا از روش مطالعات کتابخانه‌ای و مطالعه متون مؤلفه‌های اصلی سئوی سایت‌ها استخراج شدند. سپس برای تعیین مؤلفه‌های مهم سئو در وبسایت‌های فروش آنلاین کتاب، مجدداً با کلید واژه‌های: طراحی وبسایت فروش آنلاین، سئو، سئوی کتابخانه، مدیریت و طراحی وبسایت‌ها، بهینه‌سازی وبسایت در موتور جستجو، نمایه‌سازی در وب، نمایه‌سازی در گوگل، رتبه‌بندی گوگل، و ... در متون مرتبط موجود در بانک‌های اطلاعاتی ساینس دایرکت، دواچ، پروکوئست، لیزا، لیستا، گوگل اسکالر و بانک‌های فارسی گنج ایرانداک و آی.اس.سی جستجو انجام شد، از بین مقالات، کتب، پایان‌نامه‌ها و گزارشات بدست آمده متون مربوط به سال‌های ۲۰۱۴ الی ۲۰۱۹ بوده و در آنها به شاخص‌ها و مؤلفه‌های سئوی وبسایت‌ها بطور کلی و وبسایت‌های فروش آنلاین به طور خاص اشاره شده بود، به عنوان متون اصلی برای مطالعه اسنادی انتخاب شدند که در کل ۱۰۰ متن به عنوان نمونه انتخاب شدند و برای تحلیل داده‌ها، از تحلیل محتوای کمی و نرم افزار اطلس.تی.ای<sup>۱۵</sup> استفاده شده

<sup>14</sup>Marks and Le

<sup>15</sup>Atlas T.A

است. در ادامه از روش پیمایشی استفاده شده است (این پیمایش با هدف نظرسنجی از متخصصین استفاده شده است)، و برای این پیمایش از ابزار پرسشنامه محقق ساخته بر اساس مؤلفه‌های بدست آمده از بخش اول استفاده شده است، این پرسشنامه حاوی ۱۲ سوال ساختاریافته بر اساس مؤلفه‌های سئوی بازیابی شده از متون و یک ستون باز برای افزودن موارد دلخواه و البته ملاحظات نمونه مورد مطالعه بود. سوالات براساس طیف لیکرت امتیازدهی شده اند؛ ۱ کمترین امتیاز و ۵ بیشترین امتیاز.

جامعه مورد مطالعه در این بخش متخصصان حوزه‌های سئو و واقعیت مجازی بودند، البته برای نمونه‌گیری از روش هدفمند استفاده شده است؛ بدین ترتیب که متخصصان سئو باید حتما تجربه کاربردی واقعیت مجازی را داشته باشند و متخصصان واقعیت مجازی نیز باید با مؤلفه‌های سئو آشنایی می‌داشتند و لذا تعداد نمونه مورد مطالعه ۵۰ نفر بوده است. روایی صوری این پرسشنامه توسط ۳ نفر از متخصصین حوزه سئو و ۲ نفر از متخصصین واقعیت مجازی تایید شد، برای پایایی پرسشنامه نیز آلفای کرونباخ آن محاسبه شد. که عدد ۰/۸۱ را نشان داد؛ و با توجه به بزرگتر بودن آلفای محاسبه شده از ۰/۷، پایایی این پرسشنامه مناسب بوده است.

**بخش دوم:** آیا بین بهبود رتبه‌بندی گوگل و استفاده از فناوری واقعیت مجازی در وبسایت فروش آنلاین کتاب ارتباط وجود دارد؟ برای پاسخگویی به این پرسش از روش پیش‌آزمون و پس‌آزمون استفاده شده است؛ بدین ترتیب که رتبه بازیابی ۱ سایت کتاب‌فروشی آنلاین (سایت فروش اینترنتی کتاب سازمان مدیریت صنعتی) پیش از استفاده از فناوری واقعیت مجازی با توجه به مؤلفه‌های مهم در سئو و واقعیت مجازی مورد توجه قرار گرفت و مجدداً رتبه آنها بعد از گذشت یک ماه از استفاده فناوری واقعیت مجازی محاسبه شده و مقایسه این دو رتبه انجام شده است.

## ۴ یافته‌ها

برای تعیین عوامل موثر بر بهبود سئوی وبسایت‌های فروش آنلاین کتاب، از مطالعه کتابخانه‌ای و اسناد و براساس مؤلفه‌های ذکر شده در متون مرتبط استفاده شد و ۱۱ عامل به عنوان عوامل تاثیرگذارتر براساس بسامد آن‌ها در متون انتخاب شدند که در جدول ۱ آمده است. برای این بخش از تحلیل محتوای کمی و برای خوشه‌بندی و ارائه مؤلفه‌ها از نرم افزار اطلس تی.ای استفاده شده است:

با مرور داده‌های جدول ۱ به نظر می‌رسد در وبسایت‌های فروش آنلاین، عواملی که بیشتر به بخش تعامل سایت با کاربران اشاره دارند از بسامد بیشتری در میان متون مورد مطالعه برخوردار بوده‌اند.

فناوری واقعیت مجازی بر کدام یک از مؤلفه‌های سئوی وبسایت‌های فروش آنلاین کتاب موثر هستند؟

برای پاسخگویی به این سؤال از پرسشنامه‌ای ۱۲ سئوالی با طیف لیکرت و یک ستون آزاد برای بیان دیدگاه‌ها و ملاحظات متخصصین پاسخ‌دهنده استفاده شد. نتیجه مربوط به میانگین هر یک از سئوال‌ها در

جدول ۲ آمده است.

جدول ۱: مؤلفه‌های اصلی بهبود سئوی وب سایت‌های فروش آنلاین کتاب

تعداد تکرار در متون	مؤلفه
۸۴	مدت زمان حضور کاربران در وبگاه
۹۶	تعداد بک‌لینک‌ها یا استنادات وبی از سایر وبگاه‌ها
۸۸	بالا بودن سرعت بارگذاری مطالب برای کاربران
۸۰	تعداد بازدید کاربران
۵۳	تعداد صفحات نمایه‌شده وبسایت در موتور جستجوی گوگل
۹۱	کدنویسی‌های جاوای درست یا کم خطا
۴۵	محتوای چندرسانه‌ای و غنی
۶۵	ارتباط با رسانه‌های اجتماعی
۴۴	حجم مناسب مطالب و ساختار محتوا
۳۲	امکان بازبینی سایت در گوشی موبایل

جدول ۲: میانگین پاسخ‌های متخصصین به هریک از ۱۲ سؤال پرسشنامه

سؤال	میانگین امتیاز	ملاحظات
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر بر مدت زمان حضور کاربران در سایت موثر است.	۴/۳۲	با ارائه محتوا و اطلاعات جذاب و اضافی انگیزه کاربر برای ماندن در وب سایت افزایش می‌یابد.
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند بر تعداد بک‌لینک‌ها یا استنادات وبی از سایر سایت‌ها موثر باشد.	۳۴/۳	سایر وبسایت‌های مرتبط برای استفاده کاربران از اطلاعات افزوده در سایت به آن لینک می‌دهند.
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند بر بالا بودن سرعت بارگذاری مطالب برای کاربران موثر باشد.	۴/۵۱	با توجه به امکان استفاده از فضای ابری و یا سرور جدا (اصولا سرور مهمان) برای محتوای واقعیت مجازی می‌توان از حجم مطالب در وبسایت اصلی کاست.
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند بر کاهش نرخ پرش کاربران موثر باشد.	۳/۰۴	پرش کاربر به خارج از سایت یا انتقال به صفحه‌ای دیگر، بیشتر یک اشکال طراحی وبسایت است، اما فناوری واقعیت مجازی می‌تواند کاربر را در صفحه ابتدایی یا صفحه اصلی نگه دارد.
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند بر افزایش تعداد بازدید کاربران موثر باشد.	۴/۵۲	انگیزه‌ی بیشتری به کاربران می‌دهد.
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند بر افزایش تعداد صفحات نمایه‌شده وبسایت در موتور جستجوی گوگل امکان بازبینی بر روی موبایل موثر باشد.	۲/۸۳	
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند استفاده از برچسب یا فراداده‌ی «ویژگی» برای فایل‌های تصویری موثر باشد.	۱/۹۱	یک مهارت طراحی سایت است.

استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند بر نقشه‌ی سایت موثر باشد.	۲/۴۱	یک مهارت طراحی سایت است؛ البته امکان ارائه نقشه سایت بصورت واقعیت مجازی وجود دارد.
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند بر افزایش کد نویسی‌های درست جاوا موثر باشد.	۱/۰۰	یک مهارت طراحی سایت است.
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند بر ارائه محتوای چندرسانه‌ای و غنی موثر باشد.	۴/۸۱	اصول واقعیت مجازی ارائه محتوای غنی و تکمیلی است.
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند بر ارتباط با رسانه‌های اجتماعی موثر باشد.	۲/۷۳	یک مهارت طراحی سایت است.
استفاده از فناوری واقعیت مجازی در سایت فروش آنلاین کتاب چقدر می‌تواند بر حجم مناسب مطالب و ساختار محتوا موثر باشد.	۴/۳۷	حجم زیادی از محتوا بوسیله واقعیت مجازی می‌تواند بدون اشکال در حجم اصلی سایت ارائه شود.

با توجه به وزن‌دهی طیف لیکرت، مواردی که میانگین آنها ۳ و بالاتر هستند را می‌توان مورد پذیرش متخصصین نمونه دانست، میانگین طیف لیکرت تنها به عنوان یک شاخص ابتدایی برای انتخاب موارد و مؤلفه‌های مهم‌تر استفاده شده و برای سنجش میزان همخوانی نظرات متخصصان از ضریب کندال استفاده شده است و بنابراین هفت مورد از شانزده مؤلفه بهبود سئوی وبسایت‌های فروش آنلاین کتاب از نظر متخصصان با استفاده از فناوری واقعیت مجازی بهبود می‌یابند. برای اطمینان از صحت وزن‌دهی و نتایج بدست آمده ضریب هماهنگی کندال متخصصین بر پاسخ‌های ارائه‌شده به پرسشنامه محاسبه شد که ضریب کندال محاسبه‌شده عدد ۰/۹۳ بوده است که نشان‌دهنده‌ی توافق بالای پاسخ‌دهندگان به پرسشنامه است. ملاحظات ارائه‌شده در ستون سوم نیز بر اساس جمع‌بندی و تقلیل کیفی مطالب ارائه‌شده توسط نمونه مورد مطالعه ارائه شده است.

آیا بین بهبود رتبه‌بندی گوگل و استفاده از فناوری واقعیت مجازی در وبسایت فروش آنلاین کتاب ارتباط وجود دارد؟ برای پاسخگویی به این سوال وضعیت رتبه بازیابی سایت، تعداد بازدیدکنندگان، و مدت زمان حضور کاربران در سایت فروش آنلاین کتاب مورد نظر در مدت یک ماه رصد شد؛ سپس به مدت یک هفته محتوای سایت (فقط محتوای سایت و نه هیچ یک از بخش‌های دیگر مرتبط با طراحی و کدنویسی و ...) با محتوای حاوی فناوری واقعیت مجازی جایگذاری شد و باز هم به مدت یک ماه رتبه بازیابی صفحه فروش آنلاین کتاب در گوگل با کلیدواژه‌های یکسان، تعداد بازدیدکنندگان، و مدت زمان حضور کاربران در سایت فروش آنلاین کتاب مورد نظر، بصورت روزانه پایش شد. میانگین نتایج بدست آمده در جدول ۳ آمده است.

از داده‌های جدول ۳ برمی‌آید که رتبه سایت فروش آنلاین کتاب مذکور در بازیابی گوگل در مدت یک ماه به طور متوسط (بدون تبلیغ و اطلاع‌رسانی‌های عمده) ۴۵٪ کاهش رتبه داشته؛ به این معنی که بطور میانگین ۴۵٪ رتبه بهتری در نتایج بازیابی گوگل به دست آورده است. که می‌تواند براساس دو مؤلفه تعداد بازدیدکنندگان با افزایش تقریبی ۴۸٪ و مدت زمان حضور کاربران در سایت با افزایش تقریبی ۵۱٪ توجیه شود.



جدول ۳: میانگین مؤلفه‌های مرتبط با پیش‌آزمون و پس‌آزمون در فروش آنلاین کتاب مورد مطالعه

مؤلفه	پیش از واقعیت مجازی (متوسط یک ماه)	پس از واقعیت مجازی (متوسط یک ماه)
رتبه بازیابی در موتور جستجوی گوگل	۵	۲
تعداد بازدیدکنندگان	۵۷۲۳۴ نفر (تقریبی)	۸۴۷۰۶۴ نفر (تقریبی)
مدت زمان حضور کاربران در سایت	۱۱ دقیقه	۱۷ دقیقه

## ۵ نتیجه‌گیری

امروزه اغلب افراد حتی متخصصان موضوعی نیز از موتورهای جستجوی عمومی و به ویژه موتور جستجوی گوگل به عنوان اولین مجرای بازیابی اطلاعات خود استفاده می‌کنند؛ بنابراین، جایگاه و رتبه بازیابی وبسایت فروش آنلاین کتاب می‌تواند در افزایش دسترس‌پذیری بسیار حائز اهمیت باشد؛ و لذا، طراحان و مدیران وبسایت‌های فروش آنلاین کتاب همواره به بهبود و ارتقای رتبه بازیابی وبسایت خود می‌اندیشند. هدف این مقاله بررسی ارتباط بین سئوی وبسایت فروش آنلاین کتاب با محتوای حاوی واقعیت مجازی بوده است. نتایج تحلیل یافته‌های این پژوهش به شرح زیر است: مؤلفه‌های سئوی خاص وبسایت‌های فروش آنلاین کتاب از مطالعه متون بدست آمد، که شامل ۱۱ مؤلفه بود: مدت زمان حضور کاربران در وبگاه؛ تعداد بکلینک‌ها یا استنادات وبی از سایر وبگاه‌ها؛ بالا بودن سرعت بارگذاری مطالب برای کاربران، تعداد بازدید کاربران، تعداد صفحات نمایه‌شده وبسایت در موتور جستجوی گوگل، استفاده از برچسب یا فراداده «ویژگی» برای فایل‌های تصویری؛ کدنویسی‌های جاوای درست یا کم‌خطا، محتوای چندرسانه‌ای و غنی، ارتباط با رسانه‌های اجتماعی، حجم مناسب مطالب و ساختار محتوا، امکان بازیابی سایت در گوشی موبایل. این مؤلفه‌ها را می‌توان به سه دسته تقسیم کرد: مؤلفه‌هایی که به محتوای وبسایت مرتبط هستند، مؤلفه‌های کدنویسی و طراحی، و مؤلفه‌هایی که به پیوندها و فعالیت‌های سایر سایت‌ها وابسته هستند.

تحلیل یافته‌های مرتبط با سؤال دوم تحقیق نشان داد که از بین ۱۱ مؤلفه‌ای که در بخش اول بدست آمد، براساس نظر متخصصان حوزه‌های مرتبط، ۷ مؤلفه می‌توانستند با استفاده از محتوای حاوی واقعیت مجازی ارتقا یابند که عبارتند از: مدت زمان حضور کاربران در وبگاه، تعداد بکلینک‌ها یا استنادات وبی از سایر وبگاه‌ها، بالا بودن سرعت بارگذاری مطالب برای کاربران، نرخ پرش کاربران، تعداد بازدید کاربران، ارائه محتوای چندرسانه‌ای و غنی، حجم مناسب مطالب و ساختار محتوا. به نظر می‌رسد دلیل اصلی تاثیرگذاری این هفت مؤلفه ایجاد انگیزه بیشتر در کاربران با استفاده از محتوای واقعیت مجازی است که به تبع آن افزایش اطلاعات و دستیابی به اطلاعات و دانش فزاینده را با حداقل حجم ممکن و با سرعت و سهولت بسیار امکان‌پذیر می‌سازد و همین امر موجب استقبال بیشتر کاربران از سایت فروش آنلاین کتاب و در نتیجه ارتقای رتبه‌بندی وبسایت‌ها خواهد شد. نتایج حاصل از اجرای فناوری واقعیت مجازی بر روی وبسایت یک کتاب‌فروشی آنلاین نشان داد که محتوای غنی‌شده به وسیله واقعیت مجازی استقبال کاربران از خدمات و منابع موجود در وبسایت را ارتقا می‌دهد و همین امر موجب می‌شود که کاربران زمان بیشتری را در صفحات وبسایت سپری نموده و کمتر به سایت‌های مشابه مراجعه کنند که این مساله افزایش رتبه وبسایت را در نتایج موتور

جستجوی گوگل موجب شده است؛ بنابراین به نظر می‌رسد استفاده از فناوری واقعیت مجازی در محتوای وبسایت‌ها به طور کلی و وبسایت فروش آنلاین کتاب مورد مطالعه به طور خاص، می‌تواند موجب افزایش بازیابی وبسایت شده و بهبود جایگاه وبسایت را در رتبه‌بندی گوگل به همراه خواهد داشت. بنابر نظر متخصصین حوزه سئو و واقعیت مجازی، استفاده از فناوری واقعیت مجازی در بهبود برخی آیتم‌های مرتبط با سئو می‌تواند تاثیرگذار باشد، آزمایش استقرار محتوای مبتنی بر واقعیت مجازی نیز در وبسایت فروش آنلاین کتاب نشان داد که رتبه گوگل سایت به میزان ۴۵٪ بهبود پیدا کرد، اما این تغییر دو جنبه دارد: بهبود سئوی سایت و افزایش مراجعات و مدت زمان ماندگاری کاربران که البته دو مورد از موارد مهم در سئو هم به شمار می‌آیند؛ بنابراین می‌توان گفت که استفاده از فناوری واقعیت مجازی در سایت می‌تواند تا حدودی بر برخی مؤلفه‌های سئوی سایت نیز اثرگذار باشد. یافته‌های این تحقیق با توجه به هدف آن نسبتاً منحصر به فرد است؛ اما نزدیکی قابل قبولی با برخی نتایج حاصل از تحقیقات پیشین از جمله نوروزی (۲۰۰۵) و کار و همکارانش (۲۰۱۶) دارد؛ چرا که این تحقیقات نیز به ارتقای سئو و تاثیر آن در وبسایت‌ها پرداخته‌اند.

## مراجع

- [۱] دهدشتی شاهرخ، ز.، و مبرهن، س. بررسی عوامل انگیزشی فردی در خرید اینترنتی. مدیریت بازرگانی ایران، ۱۳۹۱، ۴(۱۲).
- [۲] رزاقی، م. ه.، محرابی، ق.، و جلالی فراهانی، م. ارزیابی بازاریابی اینترنتی (مدیریت ارتباط با مشتری) باشگاه‌های فوتبال ایران. فصلنامه مدیریت ارتباطات در رسانه‌های ورزشی، ۱۳۹۴، ۲(۷)، ۱۹-۲۸.
- [۳] قنبرپور، سولماز. نیازسنجی و امکان‌سنجی به‌کارگیری فناوری واقعیت مجازی در کتابخانه‌های دانشگاهی: دیدگاه متخصصان شاغل در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران، ۱۳۹۳. پایان نامه کارشناسی ارشد علوم اطلاعات، دانشکده علوم تربیتی و روانشناسی دانشگاه الزهرا.
- [۴] منتظری، م.، ابراهیمی، ع.، احمدی، ص.، و رهنما، ع. بررسی عوامل موثر بر قصد خرید در تجارت الکترونیک. مدیریت بازرگانی ایران، ۱۳۹۳، ۶(۲)، ۲۶-۲۰۷.
- [5] Ahlers, K. H., Kramer, A., Breen, D. E., Chevalier, P. Y., Crampton, C., Rose, E., & Greer, D. Distributed augmented reality for collaborative design applications. *Computer Graphics Forum*, 1995, 14(3), 3-14. doi.org/10.1111/j.1467-8659.1995.cgf143\_0003.x.
- [6] Askey, D., & Arlitsch, K. Heeding the signals: Applying web best practices when Google recommends. *Journal of Library Administration*, 2014, 55(1), 49-59.
- [7] Azuma, R., Bailiot, Y., Behringer, R., Feiner, S., Julier, S., & MacIntyre, B. Recent advances in augmented reality. 2001. Naval Research Lab Washington DC.
- [8] Carmigniani, J., & Furht, B. Augmented reality: An overview. 2011. In *Handbook of augmented reality*, Springer New York.
- [9] Chen, C. M., & Tsai, Y. N. Interactive augmented reality system for enhancing library instruction in elementary schools. *Computers & Education*, 2012, 59(2), 638-652. doi.org/10.1016/j.compedu.2012.03.001.

- [10] Dang, T. M. Study of Vietnamese customer's behavior in online shopping market study of Vietnamese customer's behavior in online shopping market. (Master's thesis). 2017. Ise University, Vietnam.
- [11] Genaro, S. Brevity and clarity: Titles, key words, and search engine optimization. *Journal of Nursing Scholarship*, 2015, 47(3), 195-196. <https://doi.org/10.1111/jnu.12129>.
- [12] Hahn, J. (2012), "Mobile augmented reality applications for library services," *New Library World*, Vol. 113 No. 9/10, pp. 429-438. [https://www.researchgate.net/publication/259761919\\_Search\\_engine\\_optimization\\_with\\_Google](https://www.researchgate.net/publication/259761919_Search_engine_optimization_with_Google).
- [13] Johnson, L., Smith, R., Levine, A., & Haywood, K., 2010 horizon report: K-12 edition. Austin, Texas: The New Media Consortium.
- [14] Kaur, S., Kaur, K., & Kaur, P. An empirical performance evaluation of universities website. *International Journal of Computer Applications*, 2016, 146(15), 10-16. <https://doi.org/10.5120/ijca2016910922>.
- [15] Krabaj, S., Baxhaku, F., & Sadrijaj, D. Investigating search engine optimization techniques for effective ranking: A case study of an educational site. 2017 6th Mediterranean Conference on Embedded Computing (MECO). <https://doi.org/10.1109/meco.2017.7977137>.
- [16] Kriemadis, T., Terzoudis, C., & Kartakoullis, N. Internet marketing in football clubs: A comparison between English and Greek websites. *Soccer & Society*, 2010, 11(3), 291-307.
- [17] Manek, F. S., Reddy, A. J., Panchal, V., & Pinjarkar, V. Hybrid crawling for time-based personalized web search ranking. 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA). <https://doi.org/10.1109/iceca.2017.8203681>
- [18] Marks, T., & Le, A. Increasing article Findability online: The four Cs of search engine optimization. *109 Law library Journal*, 2017, 83. <https://doi.org/10.2139/ssrn.3204550>
- [19] Massis, B. "Using virtual and augmented reality in the library," *New Library World*, 2015, Vol. 116 No. 11/12, pp. 796-799.
- [20] Noruzi, A. Web Impact Factors for Iranian Universities. *Webology*, 2(1). Retrieved July 5, 2020, from <http://www.webology.org/2005/v2n1/a11.html>.
- [21] Oyelude, A.A. "Virtual and augmented reality in libraries and the education sector," *Library Hi Tech News*, 2017, Vol. 34 No. 4, pp. 1-4.
- [22] Saha, I., & Paul, B. Research submission: Some technicalities and vital links. *Medical Journal Armed Forces India*, 2018. 74(2), 165-168. <https://doi.org/10.1016/j.mjafi.2017.10.006>
- [23] Shatte, A.; Holdsworth, J.; Lee, I. Mobile augmented reality based context-aware library management system. *Expert systems with Applications*, 2014, 41(5): 2174-2185.
- [24] Yuen, S., Yaoyuneyong, G., & Johnson, E. Augmented reality: An overview and five directions for AR in education. *Journal of Educational Technology Development and Exchange*, 2011, 4(1), 119-140. [doi.org/ 10.18785/je](https://doi.org/10.18785/je).



## هوش مصنوعی و کاربردهای نظامی در فضای سایبری

فریده محمدعلی پور<sup>۱</sup>، میرامیر پور موسوی<sup>۲</sup>

<sup>۱</sup> استادیار گروه روابط بین الملل دانشگاه خوارزمی  
fm.alipour@khu.ac.ir

<sup>۲</sup> دانش آموخته کارشناسی ارشد روابط بین الملل دانشگاه خوارزمی  
amir.p.m.7@gmail.com

### چکیده

مهمترین تغییرات در جنگ‌ها در پی تحولات فناوری رخ داده‌اند و سه واژه‌ی بقا، امنیت و منافع ملی توجیه‌گر استفاده و توسعه انواع تسلیحات نظامی در جنگ بوده‌اند. جهان، مستمراً با پدیده‌ها و جهش‌های خارق‌العاده فناوری‌های نوین روبه‌رو می‌شود که بر زندگی و زیست مردمان و جوامع بین‌المللی تأثیر بسیار داشته است. از مهم‌ترین دستاوردهای فناوری‌های بشر در طول تاریخ، هوش مصنوعی است. استفاده‌ی گسترده از هوش مصنوعی در جنگ سایبری از جنگ دوم خلیج فارس در قرن بیست و یکم آغاز و به صورت امری رقابتی موجب پیشرفت و توسعه نسل جدید تسلیحات و تجهیزات نظامی شده است. لذا در این پژوهش به این سؤال پاسخ داده شده است که کاربرد هوش مصنوعی در سامانه‌های نظامی چیست. یافته‌های پژوهش نشان می‌دهند هوش مصنوعی از طریق جنگ سایبری و تغییر اشکال پدافند نوین بر سامانه‌های نظامی تأثیر گذاشته و نسل جدیدی از آن‌ها ایجاد کرده است. سامانه‌های هوش مصنوعی می‌توانند با بهره‌گیری از سامانه‌های خبره و یادگیری ماشینی و بیگ دیتا باعث افزایش سرعت و دقت و هوشمندی پدافند شوند لذا با هوشمندتر و سریع‌تر شدن جنگ‌افزارها، فناوری پدافند نیاز روزافزونی به تشخیص‌دهنده و عوامل هوشمند دارد تا قبل از بروز هرگونه مخاطره‌ای، اقدامات پیشگیرانه صورت پذیرد.

**کلمات کلیدی:** هوش مصنوعی، فضای سایبری، جنگ سایبری، تسلیحات نظامی نوین، جنگ نامتقارن.

## ۱ مقدمه

استفاده کشورها از قدرت اقتصادی، سیاسی، فرهنگی و اجتماعی و رسانه‌ای در کنار قدرت امنیتی و نظامی برای پیشبرد اهداف و تأمین منافع ملی موجب گردیده که واژه‌ی «جنگ» صرفاً نظامی‌گری را به اذهان متبادر نسازد. در قرن حاضر با پیچیده شدن نظام بین الملل، جنگ ابعاد مختلفی تحت عنوان جنگ ترکیبی به خود گرفته و در این میان، جنگ سایبری با استفاده از هوش مصنوعی جایگاه ویژه‌ای دارد. این نوع از جنگ در چارچوب جنگ نامتقارن قرار می‌گیرد. جنگ نامتقارن به چند عنصر اصلی از جمله بهره‌گیری از نقاط ضعف

و آسیب‌پذیری دشمن، استفاده از فناوری‌های پیشرفته و غیر قابل انتظار و بهره‌گیری از روش‌های مبتکرانه اشاره داشته و عدم تقارن در فناوری، تاکتیک و استراتژی را نشان می‌دهد. جنگ نامتقارن را می‌توان در ابعاد هسته‌ای، شیمیایی، بیولوژیکی، الکترومغناطیسی، سایبری و... بکار بست. با عنایت به این موضوع، مطالعه ابعاد جدید جنگ مانند کاربرد هوش مصنوعی در فضای سایبری ضروری می‌نماید. در مورد جنگ سایبری یک سؤال بسیار مهم پدید می‌آید و آن این است که: در جهانی که هرکسی می‌تواند دشمن باشد و یا یک دشمن می‌تواند در هر جایی باشد، عملکرد باید چگونه باشد و چطور باید فکر کرد. اندیشه در خصوص این سؤال، انگیزه‌ی لازم برای پژوهش فراهم می‌کند.

استفاده از فضای سایبری در سازمان‌های نظامی، توانایی یگان‌ها برای رسیدن به بهترین درجه از تصمیم‌گیری، تحرک و عملکرد بر اساس وقایع میدان نبرد و پیش‌بینی تفکر و رفتار دشمن را افزایش می‌دهد. در عوض، توانایی دستکاری همان اطلاعات می‌تواند منجر به تصمیم‌گیری غلط یا سبب دگرگونی نتایج عملیات نظامی شود. ارائه اطلاعات قابل اعتماد به فرماندهان نظامی سنگ بنای عملیات اخیر بوده و منجر به پیشرفت‌های بسیاری در کاربرد فناوری شده است. سایبر داده‌ها به‌عنوان یک سلاح در میدان نبرد معرفی شده‌اند؛ پالس‌های الکترونیکی از یک ماشین به ماشین دیگر از طریق حوزه سایبر ارسال می‌شوند. هنگامی که این داده‌ها در نقطه انتها بازیافت می‌شوند، اطلاعات استخراج می‌گردد. ارزش قابل اطمینان‌ترین داده‌ها با توانایی جمع‌آوری قابل اعتمادترین اطلاعات مساوی است. از این رو، هدف، واکاوی کاربرد هوش مصنوعی در فضای سایبری به عنوان یک سلاح با کاربرد نظامی است. بررسی ادبیات موضوع، خلأ پژوهش در ابعاد مختلف این موضوع را آشکار می‌کند. لذا در این پژوهش به این سؤال پاسخ داده شده است که کاربرد هوش مصنوعی در سامانه‌های نظامی چیست. در پاسخ، با مروری بر مفهوم فضای سایبری و جنگ سایبری، در مقاله حاضر به کاربردهای نظامی هفت‌گانه هوش مصنوعی در فضای سایبری پرداخته می‌شود.

## ۲ ادبیات موضوع

در میان مکتوبات زبان فارسی کتب یا مقالات مربوط به موضوع پژوهش حاضر اندک هستند. در مقاله «هوش مصنوعی، نحوه عملکرد آن در امنیت دفاعی کشورهای پیشرفته و کاربرد و ضرورت آن در امور نظامی» [۱] با اشاره گذرا به تاریخچه‌ی هوش مصنوعی، به استفاده سربازان آمریکایی از هوش مصنوعی در افغانستان و عراق و تلاش چین و کره جنوبی برای ارتقا این فناوری پرداخته شده است. در مقاله «هوش مصنوعی و آینده حملات گروه‌های تروریستی تکفیری» [۲] نویسندگان رابطه این فناوری و گروه‌های تروریستی را در چهار عرصه بهره‌برداری از فضای مجازی، استفاده از رسانه‌های دیجیتالی به عنوان اسلحه، ارتباطات به شدت محافظت‌شده، و مهار و کنترل فناوری‌های خودکار با بیان تجربه موفق داعش مطرح کرده‌اند. مقاله «واکاوی تأثیر سلاح‌های خودکار بر صلح و امنیت بین‌المللی» [۳] به تأثیرگذاری هوش مصنوعی در تسلیحات نظامی و صلح و امنیت بین‌المللی اختصاص یافته است. در زبان انگلیسی، تعداد منابع بسیار بیشتر از زبان فارسی است. البته بیشتر آن‌ها به ابعاد حقوق بشر دوستانه و خطرات ناشی از توسعه این فناوری بر زیست مردم پرداخته‌اند. در کتاب «ربات‌های قاتل: قانونی بودن و اخلاقی بودن سلاح‌های خودمختار» [۴] نویسنده به



بررسی ابعاد قانونی و فنی و اخلاقی ربات‌ها و تبیین فرصت‌ها و چالش‌های این تجهیزات اشاره می‌کند. در مقاله «برای متوقف کردن مسابقه تسلیحاتی هوش مصنوعی خیلی دیر شده است؛ در عوض باید آن را مدیریت کنیم» [۵] مؤلف با اشاره به خطرات موجود از لزوم همکاری جهانی و استفاده از دیپلماسی برای مدیریت این فرایند سخن می‌گوید.

در مقاله «مسابقه تا پرتگاه: مدلی از هوش مصنوعی» [۶] نویسندگان با ارائه مدلی برای توسعه کم‌خطر این فناوری به بررسی خطرات توسعه نظامی هوش مصنوعی می‌پردازند. این مقاله مدل ساده‌ای از یک مسابقه تسلیحاتی هوش مصنوعی را ارائه می‌دهد. نتایج مدل‌سازی نشان می‌دهد افزایش اطلاعات، خطرات را افزایش می‌دهد: هرچه گروه‌ها بیشتر از توانایی‌های دیگران (در مورد خود) بدانند، خطر بیشتر می‌شود. مروری بر ادبیات نشان می‌دهد بیشتر پژوهشگران به تنگنای حقوقی و اخلاقی، لزوم بکارگیری دیپلماسی و یا ارتباط موضوع با حقوق بشردوستانه توجه کرده‌اند. از این رو، پژوهش حاضر درصدد رفع بخشی از این خلأ علمی با بیان کاربرد و تأثیرات هوش مصنوعی بر نسل جدید جنگ‌ها است.

### ۳ فضای سایبری

فضای سایبری از سه لایه فیزیکی، اطلاعاتی و اجتماعی به وجود می‌آید که متشکل از پنج جزء (جغرافیایی، شبکه فیزیکی، شبکه منطقی، شخصیت سایبری و شخص) است. لایه فیزیکی شامل جزء جغرافیایی و جزء شبکه فیزیکی است. جزء جغرافیایی موقعیت فیزیکی عناصر شبکه است؛ در حالی که مرزهای ژئوپلیتیکی را می‌توان به راحتی در فضای مجازی با سرعتی نزدیک به سرعت نور عبور داد، هنوز جنبه فیزیکی به سایر حوزه‌ها گره خورده است. جزء فیزیکی شبکه شامل تمام سخت‌افزار و زیرساخت (سیم، بی‌سیم و نوری) است که از شبکه و اتصالات فیزیکی (سیم، کابل، فرکانس رادیویی، روترها، سرورها و کامپیوترها) پشتیبانی می‌کند. لایه منطقی شامل مولفه شبکه منطقی است که ماهیت فنی دارد و از اتصالات منطقی بین گره‌های شبکه تشکیل شده است. گره‌ها هر وسیله متصل به یک شبکه کامپیوتری مانند لپ‌تاپ‌ها و تلفن‌های همراه هستند. لایه اجتماعی شامل جنبه‌های انسانی و شناختی است و شامل مولفه‌های شخصیت سایبری و شخص می‌شود. مؤلفه شخصیت سایبری شامل هویت یا شخصیت یک شخص در شبکه (آدرس ایمیل، آدرس IP رایانه، شماره تلفن همراه و موارد دیگر) است. جزء شخص به افراد واقعی در شبکه اشاره دارد. یک فرد می‌تواند چندین شخصیت سایبری داشته باشد (به عنوان مثال، حساب‌های ایمیل مختلف در رایانه‌های مختلف) و یک شخصیت سایبری می‌تواند چندین کاربر داشته باشد [۷].

شبکه پروتکل فضای سایبری به این حقیقت تأکید دارد که محدوده عملیاتی به یک مکان فیزیکی محدود نمی‌شود. میدان‌های نبرد سنتی به فضای فیزیکی محدود می‌شوند اما گنجایش و ظرفیت فضای سایبری تا حد زیادی گسترده‌تر است و محدوده عملیات آن نیز پیچیده است. به عنوان مثال یک ویروس اجرا شده در فضای سایبری قادر است علاوه بر ضربه زدن به هدف تعیین شده به طور غیر مشخص به سامانه‌های موجود در دیگر کشورها از جمله خود کشور حمله‌کننده نیز لطمه بزند. خسارت‌های عظیم حملات معمولاً قابل پیش‌بینی نیست.

## ۴ جنگ سایبری

تغییر فناوری تسلیحات همواره بر جنگ تأثیرات ژرف گذاشته است. در قرن نوزدهم، نیروی زمینی و دریایی با قدرت توپخانه حرف اول را می‌زد، در قرن بیستم نیروی هوایی به عنوان بعد سوم توان نظامی و سپس در بعد چهارم فضا اضافه شد. در قرن بیست و یکم سایبر است که با چهار بعد دیگر آمیخته می‌شود. با پیشرفت فناوری و راهیابی هوش مصنوعی به این زمینه مخصوصاً در خصوص حمله بدافزارها و امنیت داده و امنیت سیستم با سلاحی مواجه هستیم که قابلیت کشتن انسان را دارد زیرا دیگر حمله فقط در فضای سایبر اتفاق نمی‌افتد؛ بلکه توانایی آسیب‌رساندن به تجهیزات فیزیکی نیروگاه‌ها، ایستگاه‌های راه‌آهن، فرودگاه‌ها، بیمارستان‌ها و... وجود دارد که کشتن مستقیم هزاران انسان را ممکن می‌کند. جنگ سایبری در فضای سایبری انجام می‌شود و دستیابی به توانمندی‌های جنگ سایبری به حمله‌کننده، قدرت تخریب جبران‌ناپذیری حتی بدون شلیک یک گلوله می‌دهد. با تمرکز بر سامانه‌های الکترونیکی و ارتباطی طرف متخاصم، نیازی به اعزام لشکرها یا ناوهای جنگی نیست و به جای آن از ویروس‌های رایانه‌ای و بمب‌های پالس الکترومغناطیسی استفاده می‌شود که قادر است خرابی‌های وسیعی را در مدارات الکترونیکی به وجود آورد.

توان فوق‌العاده‌ای که یک کشور از این طریق کسب می‌کند می‌تواند دشمن را همچون یک بمب اتم منفعل کند بدون اینکه نیاز به بکارگیری ارتش متعارف باشد. در جنگ‌های متعارف معاصر همچون جنگ‌های خلیج فارس، بالکان، افغانستان و عراق، همواره حمله‌های پیشگیرانه و ویران‌کننده علیه مراکز فرماندهی، سایت‌ها و سامانه‌های راداری دفاع هوایی، مراکز ارتباطی فرماندهی و کنترل، انجام و متعاقب آن یورش به کارخانه‌های برق، دپوهای مهمات، سوخت و مراکز اصلی نیروهای آفندی نظامی کشورهای هدف واقع شده است. در جنگ سایبری نیز چنین سناریویی با اولویت‌بندی مشابه طرح‌ریزی می‌شود تا با زمین‌گیر ساختن دشمن بدون هرگونه برخورد فیزیکی و تحمیل خسارت پیروزی حاصل شود. از این رو، در این گونه جنگ‌ها، هدف نهایی فلج کردن و از کار انداختن سامانه‌ها و سازمان‌های معمول نظامی کشور هدف بوده تا نتوانند به فعالیت ادامه بدهند.

توجه به شبکه جنگ زمینی و آمیخته شدن آن با قدرت سایبری به روشن شدن بحث کمک می‌کند. شبکه جنگ زمینی، شبکه‌ای فنی است که شامل تمام سامانه‌های مدیریت اطلاعات ارتش و سامانه‌های اطلاعاتی است که جمع‌آوری، پردازش، ذخیره، نمایش، انتشار و محافظت از اطلاعات در سراسر جهان را انجام می‌دهد؛ بنابراین یک شبکه ساده نیست. این شبکه اطلاعات مورد نیاز فرماندهان در هر محیط و در هر زمان را برای تسهیل اقدامات اساسی تأمین می‌کند.

با توجه به افزایش وابستگی توانمندی شبکه عملیات زمینی یکپارچه به فضای سایبری، تهدیدات پالس‌های الکترونیکی و هک اطلاعات حساسیت زیادی یافته است زیرا می‌توانند محرمانگی و یکپارچگی مأموریت سیستم فرماندهی و اطلاعات را به خطر اندازند. عملیات تهاجمی دشمن در فضای سایبری و طیف الکترومغناطیسی در عملیات خودی نیز تأثیر می‌گذارد. توانایی دشمنان برای دستیابی به فضای سایبری نظامی منجر به دستکاری اطلاعات در سامانه‌های نظامی می‌شود؛ این تغییر می‌تواند اقدامات بعدی را تحت تأثیر قرار دهد و به بی‌اعتمادی در سیستم‌های خودی بینجامد. بی‌اعتمادی، کاهش درک موقعیت از محیط

و اطلاعات نظامی را در پی دارد. فناوری حتی مرگ ناشی از سلاح‌های کلاسیک را افزایش می‌دهد؛ مثل استفاده از لینک‌های داده و شبکه‌های مبتنی بر سامانه‌های هدف‌دار، هدف قرار دادن و هدایت نهایی از طریق سامانه‌های لیزری. سامانه‌های تعیین موقعیت جهانی، سلاح‌های جستجوگر و سلاح‌های هوشمند، درک فرمانده از وضعیت و محیط را افزایش می‌دهند. به نظر می‌رسد در فاز اول جنگ‌های آینده، درگیری‌ها به صورت مستقیم و رو در رو نخواهند بود بلکه نبردها در حوزه پنجم و در فضای سایبر اتفاق خواهد افتاد و پس از آن شاهد جنگ‌های رو در رو خواهیم بود لذا درگیری در دو فاز نبرد سایبری و جنگ اتفاق خواهد افتاد در درگیری‌های عادی و برتری با نیرویی است که توانایی مدیریت صحنه نبرد در هر دو فاز را دارد. قدرت‌های جهانی از هوش مصنوعی برای توسعه و استقرار سامانه‌های تسلیحاتی خودمختار مرگبار که به عنوان «ربات‌های سلاح» یا «ربات‌های قاتل» نیز شناخته می‌شوند، بهره می‌گیرند. این ربات‌ها، سامانه‌های تسلیحاتی هستند که از هوش مصنوعی برای شناسایی، انتخاب و کشتن اهداف انسانی بدون دخالت انسان استفاده می‌کنند. لذا رقابت در این حوزه شدید است. باید توجه کرد که (۱) به‌طور گسترده‌تر، هر رقابت برای هوش مصنوعی برتر گاهی اوقات به‌عنوان یک «مسابقه تسلیحاتی» در نظر گرفته می‌شود؛ (۲) تلاش برای تسلط بر هوش مصنوعی نظامی با تلاش برای تسلط در بخش‌های دیگر همپوشانی دارد، به ویژه زمانی که کشوری به دنبال مزایای اقتصادی و نظامی است.

## ۵ هوش مصنوعی و کاربردهای نظامی در فضای سایبری

پیشرفت در هوش مصنوعی یادگیری عمیق و رباتیک قابلیت‌های جدیدی را امکان‌پذیر می‌کند که استراتژی‌های نظامی را به طور قطع تحت تأثیر قرار می‌دهد. پیامدهای این تحولات بر مجموعه‌ای از معیارهای نظامی شامل دانش، نظارت، شناسایی تا موازنه‌های حمله و دفاع و حتی خود برنامه‌های هسته‌ای اثر می‌گذارد. در ادامه به بررسی هفت کاربرد نظامی قابل توجه پرداخته می‌شود که با فناوری هوش مصنوعی در حال توسعه هستند [۸].

نیروهای رزمی و دفاعی در سراسر زمین در حال توسعه عنصر هوش مصنوعی در سلاح‌هایی هستند که در بخش‌های زمینی، هوایی، دریایی و فضایی استفاده می‌شوند. بهره‌گیری از هوش مصنوعی در سامانه‌های وابسته به این بخش‌ها پیشرفت‌های معمول جنگی را که کمتر به مداخله انسان وابسته هستند ممکن کرده است. همچنین هوش مصنوعی توانایی این را دارد که دسته یا گردان یا واحدی از سلاح‌های خودگردان و پرسرعت را مدیریت کرده و سرعت مدیریت و حملات را از چندین جهت افزایش داده و همچنین توانایی پدافند را بسیار کند نماید.

### ۱.۵ لجستیک و حمل و نقل

یکی از اجزای اساسی فعالیت‌های نظامی موفق شبکه حمل و نقل قوی، تدارکات تسلیحات، مهمات و مهم‌تر از همه نیروی انسانی است. یک مکانیسم دفاعی برای ایفای نقش محوری در لجستیک و حمل و نقل نظامی به کمک هوش مصنوعی نیاز زیادی دارد. ترکیب هوش مصنوعی با حمل و نقل نظامی می‌تواند هزینه‌های حمل

و نقل را به حداقل برساند و عملکرد انسان‌ها را بهبود بخشد. همچنین ناوگان‌های دریایی را قادر می‌سازد تا در مواجهه با مین‌های دریایی آن‌ها را راحت‌تر تشخیص دهند و سرعت خرابی اجزا را پیش‌بینی کنند و هزینه نگهداری آن را بسیار کاهش دهند. برای مثال ارتش ایالات متحده از پلتفرم هوش مصنوعی واتسون ساخت شرکت آی‌بی‌ام برای کمک به تعیین پیچیدگی‌های تعمیر و نگهداری در وسایل نقلیه جنگی Stryker استفاده می‌کند.

## ۲.۵ شناسایی اهداف

در موقعیت‌های نبرد چندگانه رویه‌های هوش مصنوعی برای افزایش دقت تشخیص هدف بسیار مفید بوده و این امکان با تجزیه و تحلیل اسناد و شواهد مستند، محتوای خبری و انواع اطلاعاتی امکان‌پذیر است. تحلیل داده‌ها، مأموران امنیتی را قادر می‌سازد تا دانش گسترده‌ای از حوزه‌های مختلف عملیات به دست آورند. تکنیک‌های چارچوب تشخیص هدف مبتنی بر هوش مصنوعی قادر به تخمین استراتژی دشمن و مجموعه‌ای از شرایط اقلیمی و محیطی و حتی فرهنگی هستند.

## ۳.۵ مراقبت‌های بهداشت و درمانی منطقه رزمی

با ترکیب هوش مصنوعی و علم رباتیک می‌توان در مناطق جنگی به طور کلی از جراحی از راه دور و تخلیه از راه دور انجام داد. تحت شرایط جنگی سامانه‌های مجهز به هوش مصنوعی می‌تواند مسائل پزشکی مربوط به سربازان را بسیار سریع‌تر پوشش دهند و به تشخیص‌های پیچیده کمک کنند. برای مثال در ایالات متحده یک ماژول نمونه اولیه استدلال بالینی که به عنوان تحلیلگر پرونده الکترونیک پزشکی شناخته می‌شود (EMRA)<sup>۱</sup> توسعه یافته است. در این فناوری، مکانیسم یادگیری ماشین برای پردازش تاریخچه‌ی پزشکی الکترونیکی بیماران و شناسایی و اولویت‌بندی اساسی‌ترین اختلالات آن‌ها به طور مؤثر به کار برده شده است. ناتو نیز با استفاده از هوش مصنوعی در پی ایجاد و توسعه سامانه گزارش‌دهی و ردیابی پزشکی دیجیتال برای وارد کردن مفهوم سلامت دیجیتال به میدان نبرد است [۹].

## ۴.۵ شبیه‌سازی رزمی و تمرین

شبیه‌سازی و یادگیری، طیفی چندوجهی است که شامل طراحی فرآیند و برنامه‌نویسی نرم‌افزار برای ایجاد برنامه‌های کاربردی نرم‌افزاری است که سربازان را با بسیاری از سامانه‌های جنگی که در طول عملیات نظامی به کار می‌روند آشنا کرده و به نوعی از آن‌ها مراقبت می‌کند. نیروی دریایی ایالات متحده سازمان‌هایی مانند SAIC, ATK را برای ارتقای پروژه‌های خود ثبت کرده است در حالی که طرح‌های ارتش ایالات متحده توسط نهادهایی مانند CACI, TORCH MILLENIUM ENGINEERING TECHNOLOGIES تقویت می‌شوند.

<sup>1</sup>Electronic Medical Record Analyst

## ۵.۵ نظارت بر تهدید و آگاهی از موقعیت

تشخیص تهدید و آگاهی از موقعیت به فعالیت‌های اطلاعاتی، نظارت و شناسایی (ISR)<sup>۲</sup> وابسته است. عبارت است از کسب، پردازش و ارائه به موقع، دقیق، اطلاعات مرتبط، منسجم و مطمئن برای پشتیبانی از اجرای فعالیت‌های هماهنگی و یکپارچگی فرماندهی. در ترتیبات رباتیک مورد استفاده برای انجام مأموریت‌های ISR از راه دور اطلاعات ساخته و از طریق مسیرهای از پیش تعریف شده ارسال می‌شود. از طرفی، تکمیل مجدد این سامانه‌ها از طریق هوش مصنوعی به شناسایی تهدیدها کمک می‌کند و در نتیجه آگاهی آن‌ها را افزایش می‌دهد. از طرف دیگر پهپادها با ویژگی‌های یکپارچه هوش مصنوعی با تفسیر تهدیدات احتمالی و انتقال داده‌های مربوط به این خطرات به محافظت از مناطق حساس مرزی کمک می‌کنند؛ بنابراین این استفاده از پهپادها می‌تواند ایمنی تأسیسات نظامی استراتژیک را تقویت کند و در عین حال امنیت و قدرت کنش و واکنش کارکنان نظامی را در میدان جنگ و بخش‌های دورافتاده بهبود بخشد.

## ۶.۵ هوش مصنوعی و پردازش داده‌ها

هوش مصنوعی برای سرعت زیاد و دقیق بودنش معروف است. این سرعت و دقت برای حجم زیادی از داده‌ها برای به دست آوردن اطلاعات ارزشمند مفید است. هوش مصنوعی می‌تواند به پردازش و جمع‌آوری اطلاعات از پایگاه داده‌های متنوع و همچنین به دست آوردن اطلاعات از منابع مختلف خارجی کمک کند؛ این کار ارتش را برای تفسیر الگوها و استنتاج روابط بسیار توانمند می‌سازد.

## ۷.۵ هوش مصنوعی و پرنده هدایت‌پذیر

پرنده هدایت‌پذیر از دور یا به اختصار پهپاد که به آن هواپیمای بدون سرنشین نیز می‌گویند، گونه‌ای هواگرد هدایت‌پذیر از راه دور و بی‌خلبان است. پرواز پهپادها ممکن است تحت کنترل از راه دور توسط یک اپراتور انسانی، یا با درجات مختلفی از خودمختاری، مانند کمک توسط خلبان خودکار تا هواپیماهای کاملاً خودمختار انجام شود که هیچ شرطی برای مداخله انسانی ندارند [۱۰].

از هوش مصنوعی در هواپیماهای بدون سرنشین برای هوشمندتر کردن این ماشین‌های پرنده استفاده می‌شود. این‌ها نوعی پهپاد هستند اما تنها یک ماشین پرنده مکانیکی ساده نیستند؛ آن‌ها محیط اطرافشان را آنالیز کرده و به محیط اطراف واکنش نشان می‌دهند یا به هر چیزی که در اطرافشان رخ می‌دهد. به طور همزمان الگوریتم‌ها به این ماشین‌های مستقل اجازه می‌دهند که در صف نزدیک به هم پرواز کرده و از وجود یکدیگر به مانند حضور انسان‌ها مطلع باشند. پهپادهای مختلفی شامل پهپادهای مجهز به هوش مصنوعی با قابلیت‌های پرواز ارتفاع بالا و انجام انواع مأموریت‌ها در ارتش‌های جهان در حال خدمت هستند.

<sup>2</sup>Intelligence Surveillance and Reconnaissance

## ۶ نتیجه‌گیری

جنگ سایبری برای تشریح نوع جدیدی از جنگ که بر سامانه‌های ارتباطی و الکترونیکی دشمن متمرکز می‌گردد، ابداع شده است. این جنگ یکی از ستون‌های اصلی جنگ نامتقارن است که عدم تقارن در فناوری، تاکتیک و استراتژی را آشکار می‌کند. نابرابری توان تجهیزاتی و قدرت نظامی کشورهای متخاصم منجر به بکارگیری تاکتیک‌های غیر کلاسیک از سوی طرف ضعیف‌تر شده است. در این نوع از جنگ، نیازی به اعزام لشکرها یا ناوهای جنگی نبوده و به جای آن از ویروس‌های رایانه‌ای و بمب‌های پالس الکترومغناطیسی استفاده می‌شود که قادر است خرابی‌های وسیعی در مدارات الکترونیکی به وجود آورد.

دستیابی به توانمندی جنگ سایبری، به حمله‌کننده، قدرت تخریب جبران‌ناپذیری حتی بدون شلیک یک گلوله می‌دهد. میدان نبرد تغییر می‌یابد، فنون نظامی جدیدی ابداع و ابعاد جدیدی از ژئواستراتژی و ژئوپلیتیک نبرد آشکار می‌شود. چنین فناوری‌هایی به دلیل توانایی‌های برتر محاسبه و تصمیم‌گیری‌شان، خودتنظیمی<sup>۳</sup>، خودکنترلی<sup>۴</sup> و خودفعال‌سازی<sup>۵</sup> را تقویت کرده‌اند. توان فوق‌العاده‌ای که یک کشور از این طریق کسب می‌کند، می‌تواند دشمن را منفعل کرده و در عین حال ارتش کلاسیک، سازمان‌یافته و منظمی هم به کار گرفته نشده باشد.

نسل جدید جنگ در روابط بین الملل با کاربرد هوش مصنوعی آغاز شده است. بهره‌گیری از هوش مصنوعی به عنوان یک سلاح در میدان نبرد برای توفیق در عملیات نظامی قدرت برتر را به کشورهایی خواهد بخشید که قدرت‌های جهانی نیستند اما نسلی پیشرو از نخبگان علمی با ایده‌های جدید را در اختیار دارند که می‌توانند توازن قدرت در عرصه بین‌المللی را تغییر دهند. پژوهش فعلی با آشکار کردن ابعادی از کاربرد هوش مصنوعی در فضای سایبری، راه را برای گسترش بحث در خصوص آثار آن بر موازنه قدرت و موازنه تهدید، بازدارندگی و سایر موضوعات مهم روابط بین‌الملل باز می‌کند.

## مراجع

- [۱] قلیزاده، میثم؛ حقیقی، مهدی؛ رضایی، علیرضا؛ و قاسمی، ابراهیم. هوش مصنوعی، نحوه عملکرد آن در امنیت دفاعی کشورهای پیشرفته و کاربرد و ضرورت آن در امور نظامی. مجموعه مقالات کنفرانس بین‌المللی امنیت، پیشرفت و توسعه پایدار مناطق مرزی، سرزمینی و کلان‌شهرها، راهکارها و چالش‌ها با محوریت پدافند غیرعامل و مدیریت بحران، ۱۳۹۷.
- [۲] شیروودی، محمدسجاد؛ همتی، مجید؛ و سیاه‌پوش، ابراهیم. هوش مصنوعی و آینده حملات گروه‌های تروریستی تکفیری. فصلنامه مطالعات آسیای جنوب غربی، ۱۳۹۹.
- [۳] عزیزی بساطی، مجتبی؛ و سکوتی، مرضیه. واکاوی تأثیر سال‌های خودکار بر صلح و امنیت بین‌المللی. سیاست خارجی، ۱۳۹۴.

[4] Krishnan, A. *Killer Robots: Legality and Ethicality of Autonomous Weapons*. Rutledge, 2009.

<sup>3</sup>self-regulation

<sup>4</sup>self-control

<sup>5</sup>self-actuation



- [5] Geist, E. M. It's already too late to stop the ai arms race, we must manage it instead. *Bulletin of the atomic scientists*, 2016.
- [6] Armstrong, S, Nick Bostrom Carl Shulman. Racing to the precipice: a model of artificial intelligence development. tech. rep., Future of Humanity Institute, <https://link.springer.com/article/10.1007/s00146-015-0590-y>, 2015.
- [7] Crowther, G. Alexander. National defense and the cyber domain. *2018 Index of Military Strength*, [https://www.heritage.org/sites/default/files/2017-10/2018\\_IndexOfUSMilitaryStrength-2.pdf](https://www.heritage.org/sites/default/files/2017-10/2018_IndexOfUSMilitaryStrength-2.pdf), 2018.
- [8] Abell, Nicholas. 7 key military applications of machine learning. <https://medium.com/@nqabell89/7-key-military-applications-of-machine-learning-9818dfa2ea86>, 2020.
- [9] Jänig, Ch. W., Koblenz B. Bringing digital health to the battlefield - a conceptual approach for a standardized nato digital medical reporting and tracking system. *Conference: Military Health System Research Symposium 2020 At: Kissimmee, Florida, July 2020*.
- [10] Cary, L., Coyne J. *ICAO Unmanned Aircraft Systems (UAS)*, pp. 112 – 115. Blyenburgh and Co., Paris, France, 2011.



## امکان سنجی معامله در فضای سایبر بر اساس فقه امامیه

محمد رضا صفایی تخت فولادی<sup>۱</sup>

<sup>۱</sup> دانش آموخته سطح چهار، حوزه علمیه اصفهان، اصفهان، ایران  
thakhtefolady@gmail.com

### چکیده

موضوع مورد بحث در این نوشتار معاملات در فضای مجازی و حکم آن است. در این نوشتار به پاسخ به این سؤال پرداخته می‌شود که آیا معاملات در فضای مجازی از نظر شرعی دارای وجهت است؟ مسئله‌ای که در اینجا باعث شکل‌گیری این پرسش شده این است که فضای مجازی با فضای عینی دارای تفاوت‌های ماهوی است و این تفاوت در چیستی وجودی سبب می‌شود تا این شبهه ایجاد شود که احکام فضای حقیقی در فضای مجازی قابل اجرا نیست. از این رو برای حل این مسئله پرسش فوق مطرح می‌شود. با بررسی انجام شده نتایج نشان می‌دهد برخی از شرایط عقود در فضای مجازی به دلیل ماهیت آن محقق نمی‌شود مانند بلوغ. در این میان برخی از این شرایط موضوعیت داشته و برخی طریق رسیدن به هدف دیگری است. شرایطی که طریق رسیدن به هدف دیگری است را می‌توان با راه‌های دیگر جایگزین نمود و معامله مجازی را تصحیح نمود ولی شرایطی که موضوعیت دارد، قابلیت جایگزینی ندارد و معامله مجازی در صورت فقدان آن صحیح نیست.

**کلمات کلیدی:** فضای سایبر، نرم‌افزار، معامله، فقه امامیه.

### ۱ مقدمه

فضای مجازی یکی از جهان‌های ممکن در کنار جهان خارجی و جهان فرامادی در زندگی امروزه به شمار می‌رود که وجود آن حقیقتی انکارناپذیر است؛ همان‌گونه که زندگی در جهان خارج تابع قوانین و مقرراتی است، جهان مجازی نیز باید شامل قوانین و مقرراتی باشد تا بتوان نظم موجود در آن و همچنین حقوق بایسته میان کاربران این فضای جدید را حفظ نمود. با توجه به تفاوت‌های ماهوی میان فضای مجازی و فضای خارجی، نمی‌توان به سادگی برای هر موضوع در این محیط حکم موضوع آن در فضای خارجی را صادر نمود هر چند اصل وحدت احکام در برخی از زوایای این جهان قابل اجرا است؛ ولی بازشناسی دقیق فضای حاکم بر این جهان نو، و تفاوت‌های میان این پدیده و جهان بیرونی و استخراج مبانی متناسب با آن و همچنین احکام بر پایه این مبانی بایسته می‌نماید، با توجه به این تفاوت میان فضای مجازی و جهان عینی و تاثیر آن بر قوانین رفتاری نویسنده را برانگیخته است تا به بررسی قواعد فقهی معاملات در فضای سایبری بپردازد؛

چرا که تاکنون این مسئله از نگاه فقهی به صورت خاص مورد توجه قرار نگرفته است. از این رو در این نوشتار نخست به تعریفی از معامله در فقه به عنوان پیش‌نیاز پرداخته خواهد شد و سپس در بخش اصلی با بیان انواع معاملات موجود در فقه به بررسی آنها در فضای مجازی پرداخته خواهد شد و در نهایت نتیجه بررسی مذکور بیان خواهد شد.

## ۲ مروری بر کارهای دیگران

با بررسی مقالات در زمینه‌ی قانون و فضای مجازی مشخص شد تاکنون نوشتاری که به طور مستقیم به بحث معاملات در فضای مجازی بپردازد به چاپ نرسیده است و مقالاتی در این مورد نیز از بیان این مهم نارسا است. به عنوان نمونه می‌توان به موارد ذیل اشاره نمود:

۱. مقاله بررسی حقوق و مقررات در فضای مجازی، نوشته اباست پورمحمد، و همکاران.

این نوشته در صدد آن است تا با بررسی چگونگی برنامه‌ریزی، طراحی و اجرای مقررات خاص و شکل‌دهی مناسب در کالبد فضای مجازی به بررسی حقوق این فضا بپردازد. روشن است این نوشته بر اساس قواعد حقوقی به بررسی مسئله پرداخته است و به طور ویژه مسئله معاملات را بررسی نکرده است.

۲. مقاله واکاوی اصول و قواعد فقهی بهره‌گیری از فضای مجازی، نوشته مرتضی نجفی.

در این نوشتار نویسنده چند اصل زیر را محور کار خود قرار داده است: اصل لزوم نفی تسلط کفار، اصل حرمت کمک به گناه و اصل حرمت اشاعه فحشا؛ و بر این باور است در بهره‌گیری از فضای مجازی یک انسان مسلمان و متدین باید از این موارد پیروی نماید. این نوشتار به مسئله معاملات نپرداخته است.

۳. مقاله اصول مقررات‌گذاری در فضای مجازی، نوشته فائزه طاهری.

این نوشتار نیز تنها به بیان حقوقی مقررات فضای سایبری پرداخته است و در آن نگاهی به بحث فقهی معاملات در این فضا ندارد.

۴. کتاب حقوق فضای مجازی، نوشته دکتر مصطفی‌السان.

محور کتاب در چند بخش محدود است، نخست تعهدات در فضای مجازی، حقوق مالکیت فکری در فضای مجازی، امضا و گواهی و دلیل الکترونیکی، جرایم فضای مجازی، آیین کشف و دادرسی جرایم مرتبط با رایانه؛ که در تمام موارد مذکور دیدگاه نویسنده بر اساس روش نگاه حقوقی به این فضا است در حالی که نوشتار پیش رو محور فقهی را در این مهم دخیل دانسته است.

### ۳ پیش‌نیازها

در این بخش نخست لازم است تا معنای معامله از نگاه فقه اسلامی مورد کنکاش قرار گیرد. از معانی که برای معاملات عنوان شده است، معنی عملی است که بر قصد و انشاء متوقف باشد: «آنچه که متوقف است بر قصد و انشاء» [۱]، در این تعریف دو قید قصد و انشاء ذکر شده است و به وسیله قید قصد امور گزارف مانند رفتارهای در خواب و امور توصلی مانند طهارت را خارج نموده است؛ زیرا در امور توصلی مانند طهارت چه قصد داشته باشد و چه قصد نباشد با ایجاد فعل، طهارت که نتیجه فعل است ایجاد می‌شود. اما با قید دوم یعنی انشاء، اراده شده عقود و ایقاعات داخل در تعریف شود؛ زیرا در اینجا انشاء به معنی لغوی آن مد نظر نیست. باید دانست، انشاء در لغت به معنی ایجاد است [۲]؛ که در این معنی شامل کل افعال مکلف می‌گردد و معنای ادبی آن یعنی کلامی که در آن صدق و کذب راه ندارد [۳] که اشکال آن این است که در این معنا شامل معاطات نمی‌شود، زیرا در معاطات کلامی وجود ندارد. پس صحیح‌تر آن است تا تعریفی نو از معاملات ارائه شود که در آن معامله به معنی عقود و ایقاعات لحاظ گردد: «ایجاد یا گسست یک رابطه یا مبادله یا تعهد بین دو یا چند نفر به وسیله کلامی یا رفتاری که قصد قربت در آن لحاظ نشود». در این تعریف با آوردن قید «ایجاد رابطه» عقد ازدواج و ضمانت و با قید «گسست رابطه» ایقاعی مانند طلاق داخل در تعریف می‌شود. همچنین با آوردن قید «مبادله» عقودی مانند بیع و هبه در تعریف جای داده می‌شود و با هر دو قید «ایجاد یا گسست یک رابطه یا مبادله‌ای» امور توصلی مانند طهارت خارج می‌شود؛ چرا که این امور نه رابطه ایجاد می‌کند و نه مبادله است. با قید «ایجاد یا گسست تعهد» اموری مانند یمین، عهد، نذر، ایلاء، ظهار، لعان، و فسخ داخل در تعریف می‌شود» همچنین با استفاده از دو قید «کلام و رفتار»، عقود لفظی و معاطاتی نیز داخل در تعریف گردید. همچنین با آوردن قید «طرفین» عقود چند جانبه مانند مشارکت را در تعریف وارد نموده با قید «عدم لحاظ قصد قربت» عبادات از تعریف خارج می‌شود.

### ۴ فرضیات

۱. میان فضای مجازی و فضای خارجی تفاوت‌های ماهوی وجود دارد؛ در نتیجه در برخی از احکام میان این دو تفاوت وجود دارد.
۲. میان معاملات در فضای مجازی و فضای خارجی تفاوت‌هایی وجود دارد؛ تفاوت در موضوعات تفاوت در احکام را نتیجه می‌دهد.
۳. میان معاملات در فضای مجازی و فضای خارجی شباهت‌هایی وجود دارد که باعث می‌شود در برخی احکام یکسان باشند.

## ۵ روش پیشنهادی

این نوشتار با استفاده از منابع کتابخانه‌ای و با بهره‌گیری از روش تحلیل اجتهادی به نگارش در آمده است و نویسنده در آن در صدد بوده است تا با رجوع به منابع دست اول فقه امامیه و با بررسی دقیق موضوع و شرایط حاکم بر آن به استخراج مبانی و اصول کلی فقهی فضای مجازی مبادرت ورزد.

## ۶ تحلیل و ارزیابی

در این قسمت به بررسی هرکدام از عقود موجود در فقه پرداخته و بررسی می‌شود که شرایط این عقود در فضای مجازی چگونه است.

### ۱.۶ بیع

شیخ مفید ره از فقهای عقل‌گرای مکتب بغداد در المقنعه بیع را به این معنی دانسته است: «بیع بر تراضی بین دو طرف در آنچه مالک آن می‌شوند منعقد می‌گردد و این زمانی است که دو طرف به عوض از همه جهت شناخت داشته باشند و بر بیع راضی شوند عوض را قبض نمایند و بدن‌هایشان از هم جدا شود» [۴]. در این تعریف یکی از ارکان بیع قبض و اقباض دانسته شده است، در حالی که در تعاریف فقها بعدی این رکن حذف شده و آن را از آثار بیع بر شمرده‌اند؛ چرا که در دیدگاه شیخ مفید ره بیع اعم از بیع لفظی و معاطاتی است؛ در حالی که بنا به دیدگاه فقها بعدی بیع منحصر می‌شود به عقد لفظی. در تعریف شهید اول ره از فقهای مکتب جبل عامل بیع عبارت است از: «ایجاب و قبولی که بر نقل ملک در مقابل عوض معلوم و متعین دلالت کند» [۵] که در این تعریف شرط وجود الفاظ ایجاب و قبول نشان‌دهنده‌ی آن است که ایشان بیع را تنها در موردی می‌پذیرند که لفظ وجود داشته باشد. این دیدگاه متناسب با دیدگاهی است که محقق حلی ره از فقها مکتب حله بیان می‌کنند. ایشان در تعریف بیع آورده‌اند: «بیع لفظی است که بر انتقال ملک از مالک به دیگری در برابر عوض معلومی دلالت می‌کند» [۶]، اما شیخ انصاری ره تحول‌گر اصول مکتب نجف آن را «ایجاد ملکیت عین در مقابل مال» تعریف می‌کنند [۷] و امام خمینی ره از فقها مکتب قم بیع را «تبادل در اضافه» [۸] تعریف می‌نمایند، که از این دو تعریف می‌توان دریافت بیع اعم از عقد به لفظ و عقد بدون لفظ است.

اما برای قضاوت میان این دو دیدگاه بایسته است به این نکته توجه نمود، که در عقود سیره شارع بر امضاء احکام است به این معنی که شارع بیشتر در صدد امضاء آن چیزی است که در میان عرف مرسوم است و نهایتاً محدود ساختن عرف و کمتر دست به جعل حکم در بحث معاملات می‌زند. بنا بر این برای بازشناسی معنای بیع در فقه باید آن را متناسب با همان معنای عرفی آن دریافت نمود؛ چنان که امام خمینی ره این مهم را در نظر داشته و به آن توجه داشته‌اند. البته نکته‌ای که نباید از آن غفلت ورزید این است که در شرع مواردی و قواعدی برای خرید و فروش در نظر گرفته شده که باعث شده فقها در صدد ابداع یک تعریف برای بیع برآیند؛ ولی آنچه از زبان شرع فهمیده می‌شود اینکه بیع یک نوع داد و ستد است چنان که از مفاد آیه: ۱۱۱ سوره توبه فهمیده می‌شود که در آن خداوند جان و مال مردم را در مقابل بهشت خریده است و خداوند در ادامه آیه به این تقابل و داد و ستد عنوان بیع داده است [۸]. پس در زبان شرع هر گونه داد و ستدی بیع



شمرده شده است و مسلم است بیعی چون آنچه در آیه عنوان شد بر اساس قبض و اقباض بنا شده است نه بر اساس عقد لفظی؛ پس به نظر می‌رسد دیدگاه شیخ مفید ره و امام خمینی ره که بیع را اعم از عقد لفظ و معاطات می‌دانسته‌اند، صحیح‌تر می‌نماید. با توجه به آنچه گفته شد هر گونه داد و ستدی که هدف از آن خرید و فروش باشد بیع شمرده می‌شود.

رکن اصلی بیع بنا به دیدگاه امام خمینی ره تبادل است که از این فهمیده می‌شود در بیع باید دو یا چند طرف وجود داشته باشد. به علاوه از این مهم فهمیده می‌شود باید دو فرد دست کم در بیع فعالیت داشته باشند: یکی فروشنده و دیگری خریدار و رکن دیگر آن قصد تملیک دائمی است، که ایجاد نوعی اضافه می‌کند و آن رابطه اضافی بین مالک و مملوک است با توجه به این نکته پس در حقیقت شرعی هر نوع تبادل به قصد تملیک دائمی در حیطة بیع قرار می‌گیرد. با توجه به این نکته اکنون بایسته است به بررسی بیع در فضای مجازی بپردازیم. با توجه به تعریف ارائه‌شده در این بخش باید دانست این نوع داد و ستد در رسانه‌های دو سویه و چند سویه ممکن است ولی در رسانه‌های یک سویه جایی برای بررسی این نوع از معاملات وجود ندارد؛ چرا که در رسانه‌های یک‌سویه مانند رادیو یا تلویزیون امکان تبادل وجود ندارد؛ به خلاف رسانه‌های دوسویه و چندسویه که قابلیت تبادل در آنها وجود دارد. پس در رسانه‌های دوسویه و چندسویه رکن اولیه بیع موجود است.

## ۲.۶ رهن

یکی از عقود دیگری که در بحث معاملات از آن سخن به میان آمده است بحث رهن است که در فضای مجازی جایی برای پرداختن به آن نیست و احکام آن با احکام فضای خارج یکسان است. پس از بحث پیرامون آن خودداری می‌شود. یکی از شرایطی که در رهن گذاشته شده است اینکه رهن باید عین باشد؛ با توجه به این نکته که کشورهایمانند چین و آمریکا ارزهای مجازی را به عنوان کالا در نظر می‌گیرند، پرسشی که در اینجا ممکن است مطرح شود اینکه آیا اعتبارات مجازی قابلیت این را خواهند داشت تا به عنوان رهن قرار گیرند یا نه؟ در پاسخ باید گفت از شرایط عوضین این است که ثمن و مثن دارای مالیت باشند [۹]. از آنجا که بیت‌کوین و سایر ارزهای دیجیتال مثل اثیریم ارزش ذاتی ندارند بلکه یک اعتبار صرف هستند، از نظر شرعی نمی‌توان آن‌ها را به عنوان عوضین در نظر گرفت. هر چند از جهت اعتباری و قراردادی بین طرفین، این ارز دیجیتال ارزشمند است، ولی به جهت نبود ارزش ذاتی نمی‌توان آن را در معاملات عادی مجاز دانست؛ چرا که اعتبار مذکور قابل از بین رفتن است. ولی در اشیائی که دارای ارزش ذاتی هستند مانند طلا این امکان وجود ندارد. به علاوه از آنجا که این ارزها به صورت متمرکز ساماندهی نمی‌شوند و در ظاهر مرکزی دولتی بر آنها نظارت ندارد استفاده از آنها برای روابط تجاری بین مسلمین جایز به نظر نمی‌رسد؛ چرا که عدم نظارت بر این ارزها قدرت حاکمیت را برای احقاق حق مسلمین در صورت انجام اقدام مجرمانه تحت شعاع قرار داده و احقاق حق را ناممکن می‌سازد. اما در صورتی که بتوان از آنها برای مواردی چون جنگ اقتصادی بهره برد استفاده از آن در این جهت بلا مانع می‌نماید. پس با توجه به این نکته که ارزهای اعتباری مثل بیت‌کوین ارزش حقیقی ندارند و گفته شد که بنا به دیدگاه ما دارای ارزش مالی نیستند نمی‌توان آنها را به عنوان موهون قرار داد. همینطور در سایر معاملات نیز استفاده از آن جایز نیست زیرا مصداق آیه ۲۹ نساء و عنوان

فقہی: «اکل مال به باطل» می‌شود.

## ۳.۶ ضمان

ضمان به دو معنی در فقه به کار برده شده است؛ نخست به معنی اشتغال ذمه و معنی آن این است که ذمه فرد به هر علتی که مشغول شود نسبت به آن ضامن است [۱۰]. معنای دیگری که برای ضمان در فقه عنوان شده است معنی تعهد و الزام می‌باشد. فاضل مقداد در تعریف آن عنوان می‌کند: «ضمان عقد شرعی برای الزام به [تحویل] نفس یا مال است» [۱۱].

ضمان در معنای نخست از بحث خارج است اما در مورد ضمان به معنی دوم در فضای مجازی نمی‌توان مصداقی پیدا نمود فقط این پرسش پیش می‌آید که آیا حواله یا تعهد در فضای مجازی از دیدگاه فقهی پذیرفته است یا نه؟ چرا که ضمان در اینجا به عقد است و برخی در عقود نیاز به لفظ را شرط دانسته و برخی آن را شرط ندانسته‌اند و باید عنوان نمود ضمانت در فضای مجازی دو سویه، مجاز و تعهدآور است.

## ۴.۶ صلح

شیخ یوسف بحرانی می‌گوید: «صلح عقدی است برای پایان دادن به درگیری» [۱۱]. شیخ طوسی ره آن را عقد مستقلی نمی‌داند [۱۲]. در حالی که مشهور فقها آن را عقد مستقل دانسته‌اند [۱۳]؛ با توجه به آنچه گفته شد اگر صلح را از عقود در نظر داشته باشیم تنها در رسانه‌هایی می‌توان از آن بحث نمود که دو سویه یا چند سویه باشند و اگر صلح جز ایقاعات باشد می‌تواند در رسانه یک سویه‌ای چون رادیو نیز مورد استفاده واقع شود؛ مانند بخش‌های عمومی.

## ۵.۶ شرکت

در تعریف شرکت شهید دوم عنوان نموده‌اند شرکت عقدی است که ثمره آن اجازه تصرف مالکان در یک چیز واحد به صورت مشاع است [۱۴]. با توجه به تعریف، شرکت به صورت عقدی و غیرعقدی هر دو صورت در فضای مجازی ممکن است. پیرامون شرکت‌های عقدی باید گفت شکل‌گیری این شرکت‌ها در فضای مجازی چند پرسش را ایجاد می‌کند؛ نخست آنکه آیا عقد شرکت در فضای مجازی صحیح است؟ در رسانه‌های دو جانبه یا چند جانبه صحیح است و برای رسانه‌های یک جانبه سالبه به انتفاع موضوع است. دوم اینکه آیا شرکت در اموال اعتباری مثل بیت کوین صحیح است؟ که با توجه به اثبات عدم مالیت این اقلام ایجاد شرکت با استفاده از این اعتبارات وجه شرعی ندارد.

## ۶.۶ مضاربه

در تعریف مضاربه گفته شده: «دادن مال به دیگری برای تجارت با آن و تقسیم سود بینشان» [۱۵]. مضاربه نیز به نوعی و هر دو در سود و زیان شریک هستند، این فرآیند اقتصادی به شرطی صحیح است که از پول رایج استفاده شود و با آن خرید و فروش صورت پذیرد و بدون این شرایط مضاربه صحیح نمی‌باشد. نکته‌ای که در این نوع معامله در فضای مجازی قابل بررسی است اینکه امکان بستن قرارداد مضاربه به صورت مجازی

ممکن است و اشکالی بر آن نیست و خرید و فروش اینترنتی نیز در این معامله پذیرفته است و عامل می‌تواند با سرمایه فرد در این تجارت گام بردارد؛ اما استفاده از ارز دیجیتال به عنوان سرمایه برای بحث مضاربه از دیدگاه شرعی پذیرفته نیست مگر در ضرورت؛ چرا که اثبات شد این گونه ارزها دارای مالیت نیستند.

## ۷.۶ مزارعة و مساقات

معامله مزارعه به معنی «معامله بر زمین زراعی بر قسمتی از محصول» [۱۶]، است یعنی کار زراعت از یک نفر و زمین از فرد دیگر و شراکت در محصول. مساقات نیز به معنی قراردادی است که در آن صاحب یا صاحب اختیار درختان میوه آنها را برای تربیت و رشد به دیگری واگذار می‌کند و هر دو در محصول نهائی شریک می‌شوند [۱۷]. این دو عقد عملاً در فضای مجازی محقق می‌شوند، ولی خود اجرای قرار داد تنها در بیرون از این فضای مجازی ممکن است؛ مگر آنکه این پرسش پیش آید که آیا در آبیاری به وسیله نرم‌افزار از راه دور نیز می‌تواند مصداقی از مصادیق بحث گردد. در پاسخ باید عنوان نمود چنین معامله‌ای معتبر است زیرا تنوع ابزار باعث تغییر موضوع فقهی نیست. تنها باید در این موارد به این نکته توجه نمود که آیا مدعی چنین خدماتی توانائی اجراء آن را نیز دارد؟ تا موضوع قاعده ضرر نباشد.

## ۸.۶ ودیعه

در مورد ودیعه باید عنوان نمود این نوعی عقد است که در آن فردی به عنوان نایب انسان در حفظ اموال قرار داده می‌شود [۱۸]. با توجه به آنچه گفته شد این سؤال پیش می‌آید که آیا ودیعه نهادن اموال نزد سایت‌های سایبری صحیح است یا نه؟ در پاسخ باید عنوان نمود فضای سایبری اگر قرینه‌ای بر اعتماد بر آنها وجود داشته باشد که بتوان به آن اعتماد نمود، بحث ودیعه نهادن نزد آنها بدون اشکال است و الا از نظر شرعی ودیعه محقق نمی‌شود چرا که احتمال غرر وجود دارد.

## ۹.۶ عاریه

سید ابوالحسن اصفهانی در تعریف عاریه می‌گوید مسلط ساختن دیگری بر عینی برای بهره‌برداری از آن به شیوه مجانی [۱۹]؛ با این تعریف آیا عاریه در این فضا قابل انجام هست؟ در پاسخ باید عنوان نمود صاحبان فضاهای مجازی می‌توانند محیط اختصاصی خود را به دیگران عاریه دهند. بنا به قاعده تسلیط [۲۰] این تصرف و اباحه جایز است. سؤالی دیگری که آیا فضای سایبر شرایط عاریه را دارد؟ در پاسخ باید گفت شرط عاریه، عین بودن شیء است و در اینجا عین خارجی وجود ندارد؛ ولی عین سایبری نیز از «ما یملک» به شمار می‌رود پس قابلیت عاریه داده شدن را نیز خواهد داشت.

## ۱۰.۶ اجاره

مشهور فقها امامیه تعریف اجاره را عقدی عنوان می‌نمایند که نتیجه آن بهره‌مندی از منفعت در مقابل عوض معلومی است [۲۱]. بر اساس این تعریف به چند پرسش محتمل می‌توان پاسخ داد. پرسش: آیا عقد اجاره در فضای مجازی جایز است؟ پاسخ: بدون شک این مهم جایز است؛ البته در رسانه‌های دو یا چند سویه.

سؤال: اجاره فضای سایبر ممکن است؟ پاسخ: مشکلی از نظر فقهی وجود ندارد. سؤال: آیا در بحث اجاره عمل می‌توان نرم‌افزار را اجیر نمود؟ پاسخ: در واقع اجیر صاحب نرم‌افزار است و منافع عمل نرم‌افزار متعلق به صاحب این گونه از نرم‌افزارها می‌باشد؛ هر چند این نرم‌افزارها هوشمند باشند ولی به جهت عدم استقلال و نیاز به بستر باز عواید آن متعلق به صاحب آن است.

## ۱۱.۶ وکالت

شهید ثانی در کتاب خود وکالت را نیابت ذاتی در تصرف معرفی می‌کند [۲۲] و برای آن شرایطی از جمله اینکه هر یک از وکیل و موکل باید بالغ و عاقل باشند و موکل از انجام آن کاری که به وکیل توکیل می‌کند شرعاً ممنوع التصرف نباشد [۲۳]. بحثی که در اینجا می‌توان از آن سخن به میان آورد اینکه آیا وکالت در فضای مجازی ممکن است یا نه؟ پاسخ این پرسش امکان و جواز آن است. پرسش دیگری که در اینجا مطرح است آنکه وکالت نرم‌افزارهای سایبری از انسان ممکن است؟ با توجه به اینکه که نرم‌افزارهای یکی از شرایط وکالت یعنی بلوغ را نمی‌توانند داشته باشند. در پاسخ باید گفت: بلوغ در بحث وکالت خود موضوعیت ندارد؛ بلکه طریق و نشانه‌ای است برای آنکه فرد در دایره تکلیف داخل شده و تکلیف به معنی آن است که مسئولیت رفتار به عهده خود فرد است؛ حال در جایی که مسئولیت رفتار به عهده فرد دیگر است مانند: بحث از نرم‌افزار در واقع وکالت از آن نرم‌افزار نیست، بلکه از آن صاحب اختیار آن یا سازنده‌ی آن است. پس وکالت نرم‌افزار از انسان از نظر فقهی مجاز است.

## ۷ نتیجه‌گیری

با توجه به آنچه بیان شد می‌توان دریافت برخی از شرایط متعاقبین یا ثمن در برخی فعالیت‌های مجازی وجود ندارد و اصولاً امکان وجود آن نیست مانند شرط بلوغ. در این میان برخی از این شرایط موضوعیت داشته و برخی طریق برای رسیدن به موضوعی دیگر است. به عنوان نمونه در بحث بلوغ، این تنها نشانه‌ای است برای رسیدن به محدوده سنی مکلف. حال اگر نشانه‌ای دیگر برای رسیدن به محدوده سنی مکلف به دست دهد می‌توان این شرط را ملغی نمود. از دیگر سو برخی از شروط موضوعیت دارند مانند ارزش ذاتی داشتن ثمن. عدم وجود این شرط موجب غرر است؛ از این رو در معاملات مجازی که ارزش ذاتی به عنوان ثمن قرار نمی‌گیرد مانند معاملات رمز ارزها از نظر شرعی غرر وجود دارد و این دست از معاملات مجازی از نظر شرعی وجاهت نخواهد داشت.

## مراجع

- [۱] شیرازی، ناصر مکارم. انوار الأصول، ص. ۶۰۵. مدرسه الامام، قم: امیر المومنین، ج ۱.
- [۲] راغب‌اصفهانی، حسین. مفردات قرآن کریم، ص. ۸۰۷. دار القلم، الدار الشامیه - دمشق بیروت، ۱۴۱۲.
- [۳] خوئی، سیدابوالقاسم. مصباح الفقاهة، ص. ۵۲. قم: مکتبه الداوری، ج ۲ بی‌تا.
- [۴] شیخ‌مفید. المقنعه، ص. ۵۹۱. قم: موسسه النشر الاسلامی، ۱۴۱۰.

- [۵] شهیداول. اللمعة الدمشقية لعمدة الدمشقية، ص. ۹۳. بيروت: دارالفکر، ج ۱.
- [۶] محقق حلی. شرایع الاسلام، ص. ۷. قم: موسسه اسماعیلیان، ج ۲، ۱۴۰۸.
- [۷] شیخ انصاری. مکاسب، ص. ۱۸. قم: تراث الشیخ الأعظم، ج ۱، بی تا.
- [۸] الموسوی الخمينی، سیدروح الله. البیع، ص. ۱۹. تهران: موسسه تنظیم و نشر آثار امام خمینی، ج ۱، ۱۴۲۱.
- [۹] کاشف الغطاء، حسن. انوار الفقاهة، ص. ۳۷. مکتبه کاشف الغطاء العامة، ج ۱، بی تا.
- [۱۰] صدر، سیدمحمد. ماوراء الفقه، ص. ۳۲۰. قم: المحبین للطباعة و النشر، ج ۴، ۱۴۰۶.
- [۱۱] مقداد، فاضل. التنقیح الرائع لمختصر الشرائع، ص. ۱۸۳. قم: مکتبه آیت الله المرعشی النجفی، ج ۲، ۱۴۰۴.
- [۱۲] شیخ طوسی. المبسوط في فقه الإمامية، ص. ۲۸۸. تهران: المکتبه المرتضوية لإحياء الآثار الجعفرية، ج ۲، ۱۳۸۷.
- [۱۳] محقق حلی. شرایع الاسلام، ج ۲، ص. ۳۶۷.
- [۱۴] شهیدثانی. مسالك الأفهام إلى تنقیح شرائع الإسلام، ص. ۳۰۱. قم: مؤسسة المعارف الاسلامية، ج ۴، ۱۴۲۳.
- [۱۵] طباطبائی، سیدمحسن. مستمسک العروة الوثقی، ص. ۲۳۷. بيروت: دار إحياء التراث العربي، ج ۱۲، ۱۳۹۲.
- [۱۶] طباطبائی مجاهد، سیدمحمد. کتاب المناهل، ص. ۲۱۱. مؤسسة آل البيت ع، بی تا.
- [۱۷] شهیدثانی. مسالك الأفهام إلى تنقیح شرائع الإسلام، ج ۵، ص. ۳۷.
- [۱۸] بحرانی، شیخ یوسف. الحدائق الناضرة في أحكام العترة الطاهرة، ص. ۳۹۸. مؤسسة النشر الاسلامي، قم، ج ۲۱، بی تا.
- [۱۹] اصفهانی، سیدابوالحسن. وسيلة النجاة، ص. ۴۱۵. تهران: موسسه تنظیم و نشر آثار الإمام الخمينی، ص ۴۱۵، ۱۴۳۴.
- [۲۰] علامه حلی. نهج الحق و كشف الصدق، ص. ۴۹۴. بيروت: دار الكتب اللبناني، ۱۹۸۹.
- [۲۱] بحرانی، شیخ یوسف. الحدائق الناضرة في أحكام العترة الطاهرة، ج ۲۱، ص. ۵۳۲.
- [۲۲] شهیدثانی. الروضة البهية في شرح اللمعة الدمشقية، ج ۲، ص. ۱۵.
- [۲۳] همان، ص. ۱۷.





## تأثیر فناوری سایبر در معماری

سیده نرگس حسینی<sup>۱</sup>، محمد امین دباغیان<sup>۲</sup>

<sup>۱</sup> کارشناسی ارشد معماری داخلی، دانشگاه آزاد اسلامی واحد علوم و فناوری پردیس، تهران، ایران  
narges\_hb@yahoo.com

<sup>۲</sup> کارشناسی ارشد مهندسی معماری، موسسه آموزش عالی کوثر، قزوین، ایران؛ هنرآموز هنرستان، رودهن، تهران، ایران  
amin.dabbaghian@yahoo.com

### چکیده

تحولات عظیم فناوری در این دوران، بر تمامی نهادها و ارکان زندگانی انسان تأثیر گذارده است. با آغاز قرن بیست و یکم، انقلاب سایبری، به یک حقیقت قابل لمس تبدیل شده و زندگی انسان را دگرگون ساخته است. در این میان، معماری نیز از این تحول بی نصیب نمانده است. این پژوهش، با هدف شناسایی تأثیر فضای سایبر در معماری شکل گرفت. برای پاسخ گویی به پرسش اصلی تحقیق و دستیابی به هدف پژوهش، جمع آوری داده‌ها با بهره‌گیری از منابع مطالعاتی از جمله مقالات معتبر بین‌المللی و داخلی به صورت توصیفی و کیفی و با رویکرد ترویجی و با اهداف کاربردی می باشد. طبق یافته‌های پژوهش، می‌توان تأثیرات فضای سایبر بر معماری را این‌گونه جمع‌بندی کرد: معماری سایبری، معماری مجازی و شکل گرفته در فضای دیجیتال است که به مراتب توانایی‌های گسترده‌تری را پیش روی معمار نسبت به روش کار سنتی معماری ارائه می‌دهد. با پیشرفت فناوری سایبر، نیاز به ساخت فضاهای فیزیکی روز به روز در حال کاهش است. فضای سایبر با حضور فراوانش، نیاز کمتر و کمتری به معماری دارد و سرانجام آن را غیر معمول و زائد می‌کند.

**کلمات کلیدی:** سایبر، معماری، معماری مجازی، معماری سایبرنتیک.

### ۱ مقدمه

تحولات عظیم اجتماعی، فرهنگی و فناوری در دوران حاضر سبب تغییر تفکرات بشر در باب اندیشه‌ها، باورها و سنن اجتماعی گشته و بر تمامی نهادها و ارگان زندگانی انسان تأثیر گذاشته است. قافله تمدن با اختراعات اکتشافات و دستاوردهای نوین فکری روز به روز در حال حرکت است و تبدلات فرهنگی، گسترش دنیای مجازی و کشمکش‌های حوزه‌های مختلف اجتماعی سطح دانستنی‌ها و آگاهی افراد را بالا برده و با وجود استقامت و انعطاف‌ناپذیری بخشی از جامعه، تمامی جنبه‌های زندگی بشر را تحت تأثیر قرار داده است. در این میان معماری نیز از این تحول بی نصیب نمانده است؛ بار معنای بناها تغییر یافته و نیاز به معانی جدیدی

که فراخور شرایط حاضر جوامع اطلاعاتی باشد، احساس می‌گردد. رویکرد معماری برای تأمین سرپناه انسان در اعصار مختلف زیستی، همواره متأثر از فناوری‌های روز بوده است. انسان عصر حجر در غارهای ساخته‌ی دست طبیعت می‌زیست. زیست بوم‌های انسان عصر صنعت در شهرهای بزرگ با سازه‌های فولادی شکل گرفته است. فناوری به مثابه دانش، بر شناخت و ایده هر اثر معماری تأثیرگذار است. در واقع فناوری دانش ما را تحت تأثیر قرار داده و شناخت ما را از جهان پیرامون تغییر می‌دهد و باعث می‌شود تا فضاهای معماری جدیدی را متصور شویم [۱].

فضای سایبر و معماری به دو صورت با یکدیگر ارتباط برقرار می‌کنند که در نگرش اول حضور فضای سایبر به عنوان راه حل در عرصه معماری قطعی است. در این نوع نگرش فضای سایبر با معماری در سه لایه‌ی ابزار، همکار و فضای اشتراکی ارتباط برقرار می‌کند. در نگرش دیگر، فضای سایبر به مثابه یک مسئله پیش روی طراحان قرار گرفته که فرایند طراحی را باید برای آن پی‌جویی کرد. در چند سال اخیر فضای سایبر از سوی برخی معماران به عنوان سیستمی مؤثر در عرصه طراحی معماری - مجازی یا حقیقی - توصیه شده است تا طراحان، فضایی متناسب با ویژگی‌های محیطی کاربران آن خلق کنند. معماری سایبر نیز معماری است که در حوزه سایبر فضاها شکل می‌گیرد، معماری بدون فضای فیزیکی و بدون توده و جرم. این فضاها دیجیتال که کاملاً به صورت حقیقی حس می‌شوند در نوع خود خارق‌العاده بوده و هیچ نشانی از روش‌ها و ویژگی‌های مصالح فیزیکی و اصول مورفولوژی مربوط به فضا و سازه که قید و بندهایی را بر معماری تحمیل می‌کنند در آن‌ها دیده نمی‌شود [۲].

روش‌های طراحی سایبر نه تنها منجر به بروز فرمی نوین می‌گردند، بلکه به معمار این اجازه را می‌دهند که مستقیماً با امکانات تولید ارتباط برقرار کند؛ در نتیجه آن پتانسیل و توانایی انتخاب و طراحی اجزای ساختمانی پیچیده و تخصصی را خواهد داشت [۱۵].

## ۲ بیان مسئله

دنیای سایبر تقریباً از دهه ۱۹۶۰ به کمک طراحی معماری آمد، در واقع هرگونه استفاده از رایانه در معماری به عنوان معماری دیجیتال شناخته می‌شود [۳].

این معماری را می‌توان رهیافتی بر تجسم و تحقق معماری کالبدی بر پایه فناوری واقعیت مجازی دانست که با نام‌های دیگری همچون معماری دیجیتالی، معماری فرافضا، معماری غیرخطی، معماری متا و فضای سایبری نیز شناخته می‌شود [۴].

ارتباط معماری با علوم سایبری بحثی گسترده است؛ به خصوص در دهه‌های اخیر می‌توان تأثیر گسترده رایانه و پیشرفت‌های علمی در این زمینه را در معماری دید. در اواخر دهه‌ی گذشته تفکر استفاده از تکنیک‌های رایانه‌ای در معماری آنقدر پررنگ گردید که در کمترین فاصله زمانی ممکن تأثیر شاخص خود را در اذهان و نتایج طراحان به جای گذاشت. به صورت موشکافانه می‌توان گفت این تصور و این نوع نفوذ رایانه در علم طراحی نه تنها در حیطه عملکردی معماران مؤثر واقع گردید، بلکه دیگر اعضای هیئت طراحان را نیز تحت تأثیر خود قرار داد و طراحان صنعتی، فیلمسازان و حتی موسیقیدانان را نیز از تأثیر خود بی‌بهره نگذاشت.

رایانه با تأثیر در این سیستم فکری هر روز نسبت به روز دیگر موفق‌تر عمل می‌نمود و در حال حاضر به طور گسترده‌ای شاهد استفاده از رایانه و تکنیک‌های دیجیتال و بر پایه‌ی فضای سایبر در معماری هستیم [۵]. ورود رایانه به حوزه طراحی دو تغییر عمده را در پی داشت [۳]:

۱. افزایش توانایی و سهولت طراحی، مدل‌سازی و ساخت فرم‌های معماری پیچیده و در نتیجه افزایش تولید، تسریع در روند بررسی گزینه‌های مختلف در تعداد بیشتری از آن‌ها.
۲. تحت کنترل درآوردن قدرت پردازش رایانه در جهت تولید و ارزیابی گزینه‌های طراحی.

معماران بهره‌گیری از فضای دیجیتال در معماری به دو دوره تقسیم نموده‌اند. دوره اول به دهه ۱۹۷۰ برمی‌گردد که استفاده از رایانه به عنوان یک وسیله ترسیمی و بیانی در تولید نقشه‌های معماری، تغییرات شگرفی را بر این جریان اعمال کرد [۶].

در دوره‌ی دوم، ابزارهای دیجیتال در ادامه فراهم‌سازی روش‌های پایه طراحی و ترسیم، در فرایندهای طراحی به کمک طراحان و برنامه‌ریزان آمدند. محیط دیجیتال، ادبیات جدیدی را در خلق آثار معماری پدید آورد. این ادبیات از مراحل اولیه طراحی کانسپت شروع و به مرحله ساخت ختم می‌شود [۳]. این مرحله، در پی تمایل طراحان به خلق فرم‌های پیچیده و تلاش برای ترکیب بیش از یک تابع اصلی در ساختمان یا ارائه‌ی پیچیده از طرح، که طراح را با مسائل پیچیده روبرو می‌کند به وجود آمد [۱۶]. فضایی که در محیط سایبر به وجود می‌آید، ایده‌هایی از جنبش‌های جدید معماری را با خود به همراه دارد. می‌توان مارکوس نواک را به عنوان پیشکسوتی در باب فضای سایبر دانست. او معماری در حوزه دیجیتال را تعریف کرد و تئوری معماری سیال را مطرح نمود. نواک خود را به عنوان یک معمار ایده‌آلیست مطرح می‌کند؛ به این علت که طرح‌های معماری او با رایانه زاده می‌شوند و برای یک حوزه مجازی طراحی شده‌اند. در معماری سیال، نواک دو معماری را پیشنهاد می‌کند که از پذیرش فرم‌های منطقی، پرسپکتیو و قانون جاذبه خودداری می‌کند. انحنایها، چرخش‌ها و تغییرات معماری سیال نواک در واکنش به عکس‌العمل شخصی است که در آن فضا قرار گرفته است؛ لذا انسان است که در درجه اول اهمیت است. معماری سیال نه تنها در پی سیالت فرم است بلکه در عملکرد نیز آن را می‌جوید. معماری سایبر، محدودیت‌های سایت که معمار در طرح‌های اجرایی با آن درگیر است در این معماری جایی ندارد و معمار در سایتی با گستره‌ای نامحدود می‌تواند به طراحی بپردازد و دومین امکان که توسط نواک در معماری سیال مطرح شده فراغت از جاذبه زمین است و همین ویژگی‌ها است که باعث گردیده تا نام معماری انجام‌نشده را برای آن برگزیند [۷].

### ۳ روش پژوهش

این پژوهش با هدف «تأثیر فناوری سایبر در معماری» شکل گرفته است. برای رسیدن به هدف پژوهش، پرسش زیر مطرح شد:

فناوری سایبر چه تأثیراتی در معماری دارد؟

رسیدن به پاسخ این سؤال یعنی رسیدن به نتیجه تحقیق که در ادامه این مقاله به آن اشاره می‌شود. برای پاسخگویی به پرسش اصلی تحقیق و دستیابی به هدف پژوهش، جمع‌آوری داده‌ها با بهره‌گیری از منابع مطالعاتی از جمله مقالات معتبر بین‌المللی و داخلی به صورت توصیفی و کیفی و با رویکرد ترویجی و با اهداف کاربردی انجام می‌گیرد.

## ۴ تعریف فضای سایبر

بر خلاف سایر اصطلاحات که دارای تعریفی روشن و معقول هستند، فضای سایبر از تعریفی بسیار گسترده و گاه مغشوش برخوردار است. اصطلاح فضای سایبر اولین بار در سال ۱۹۸۴ توسط «ویلیام گیسون»، نویسنده داستان‌های علمی تخیلی در رمان آینده‌نگرانه‌ی او به نام «نئورومنس» به کار گرفته شد. اصطلاح سایبر از کلمه یونانی کایبرنان به معنی هدایت و سایبرنتیک، علم مطالعه تطبیقی عملکردهای کامپیوترهای الکترونیکی و سیستم عصبی انسان مشتق شده است. کلمه سایبر به معنی پردازش‌شده‌ی کامپیوتری است که با پسوند «اسپیس» در هم آمیخته است و فضای پردازش شده با کامپیوتر معنی می‌دهد [۸].

بدین ترتیب فضای سایبر، محیط مجازی تولیدشده توسط کامپیوتر است که تنها از طریق بازنمایی و ارائه دیجیتال می‌تواند تجربه شود. هر چیزی در این فضای مجازی، پویا، سیال و در حرکت می‌باشد. «مایکل بندیکت» فضای سایبر را به عنوان یک واقعیت جهانی وابسته به شبکه، پشتیبانی‌شده توسط کامپیوتر، چند بعدی و ساختگی یا مجازی تعریف کرده است. نکته مهمی که باید در اینجا به آن اشاره کرد، این است که برخی فضای سایبر را همان اینترنت تعریف می‌کنند؛ در حالی که اینترنت فضای سایبر نیست، بلکه فضای سایبر دربردارنده تمامی محتوای است که از طریق فناوری اینترنت در دسترس و قابل استفاده می‌باشند. فضای سایبر یک نظام اجتماعی وابسته به ساختار ایجاد شده توسط سیستم تکنولوژی است که از افراد، مزایا، قابلیت‌ها و ارزش‌های مختلف و متعدد تشکیل می‌شود. در کل می‌توان گفت فضای سایبر جهان جدیدی را به ارمغان آورده است؛ جهانی به موازات عالم فیزیکی که به وسیله خطوط ارتباطی و کامپیوتری دنیا ایجاد شده و توسط آن‌ها پشتیبانی می‌شود؛ دنیایی که مبادله جهانی دانش، اسرار، اندازه‌ها، شاخص‌ها، سرگرمی‌ها و فعالیت‌ها مهم‌ترین مشخصه آن است [۹].

## ۵ معماری در فضای سایبر

«مارکوس نوواک» نظریه‌پرداز معماری و از پیشگامان نظریه دنیای مجازی عقیده دارد که معماری باید سیال و آبگونه باشد. عبارت معماری سیال که این روزها بسیار متداول است، از همان آغاز عصر الکترونیک و در سال ۱۹۸۵ میلادی به وجود آمد. نوواک در مقاله‌ای در مجله D A می‌نویسد: من در کارها و نوشته‌هایم سعی کرده‌ام تا سلسله مراتبی از توسعه تکنولوژی در معماری را به طور گسترده در عرصه فرهنگی منتشر کنم. بندهای این سلسله عناصری است که من برای رشد گرایش‌های فرهنگی درک کرده‌ام؛ یعنی الگوریتم‌های پیچیده، تغییرپذیری آبگونه، رویدادی و سرشار از تنوع بودن [۱۰].

شرایط اجتماعی تأثیرات غیرقابل انکاری را بر روند تحول معماری در طول تاریخ داشته است. بر همین

اساس، در عصر حاضر نیز معماری بر اثر ایجاد سیستم‌های ارتباطات الکترونیکی و اطلاعاتی و به تبع آن ظهور فضای سایبر، انجام وظایف زندگی روزمره مانند کار، خرید، تفریحات، مراقبت‌های بهداشتی، آموزش، خدمات عمومی، حکومت و نظایر آن را از راه دور ممکن ساخته و مردم به نحو روزافزونی از درون خانه‌هایشان به انجام کار و اداره امور روزمره می‌پردازند. فضای سایبر که به واسطه گسترش فناوری اطلاعات شکل گرفته، از جنبه‌های مختلف بر معماری امروز جهان تاثیر گذاشته و آن را متحول ساخته که می‌توان این تاثیرات را در حوزه تاثیر فضای سایبر بر فضاهای معماری بررسی نمود.

## ۶ تاثیر فضای سایبر بر فضاهای معماری

در جهان سنتی، رابطه تنگاتنگی میان ما و محیط فیزیکی وجود داشت و معماری در سازمان‌دهی کارکردها و رابطه میان فعالیت‌ها نقش مهمی ایفا می‌کرد [۹].

انقلاب اطلاعات باعث استحاله معماری و طراحی فضای شهری می‌شود. تکنولوژی‌های دیجیتال ماهیت و هدف تفکر و خلاقیت وابسته به معماری را دگرگون ساخته‌اند. اتصالات بین ماده و داده، بین واقعیت و مجاز، بین ارگانیک و غیر ارگانیک را کمرنگ ساخته‌اند؛ در حالی که محیط شناور و نامعین را خلق می‌کند، یعنی حد فاصلی بین فضای عمومی و خصوصی، امور مشترک و امور شخصی، و امر محلی و امر جهانی [۱۱]. فضای سایبر از جنبه‌های مختلف بر معماری امروز جهان تاثیر گذاشته است؛ به نظر می‌رسد این فضا با معماری در سه لایه‌ی متفاوت ارتباط پیدا کرده است: [۱۲].

۱. فضای سایبر به عنوان ابزار در معماری، به گونه‌ای که در روند طراحی، از امکانات شبیه‌سازی در سطحی گسترده بهره جسته می‌شود. به عبارت دیگر فضای سایبر با تاثیر بر فرایند کنش معماری و امکان ایجاد تصوراتی سیال در بازتولید واقعیت نقشی به سزا داشته است.

۲. فضای سایبر به عنوان همکار معمار را در فرایند طراحی یاری می‌کند. در واقع این همکاری بین انسان و رایانه به هر دوی آنها کمک می‌کند تا از توانایی‌های یکدیگر در راستای پیشبرد کار به خوبی استفاده کنند.

۳. فضای سایبر به عنوان فضای اشتراکی طراحی با شرایطی که شبکه جهانی فراهم کرده است، معماران در هر جای جهان می‌توانند ایده‌های خود را به اشتراک بگذارند.

برای شناخت بهتر تاثیر تکنولوژی سایبر بر معماری باید تاثیر آن را بر نتایج معماری، یعنی بناها و فضاهای معمارانه بررسی کرد. برخی از مهم‌ترین تاثیرات فضای سایبر بر فعالیت‌های روزمره‌ی زندگی و جنبه‌های فضایی آن‌ها به شرح زیر است:

فرایندهای کاریو ساختارهای شرکت‌های امروزی به طرز فزاینده‌ای در حال مجازی شدن هستند؛ آن‌ها بجای استفاده از ساختارهای عقلانی و تاریخی یک محیط معمارانه، بوسیله نرم‌افزار و اینترنت کار می‌کنند. گرایش به سمت کار کردن از راه دور در حال جایگزینی مکان‌های کاری مرکزی با اداره‌های خانگی و حذف

کاغذبازی سازمانی است. بدین ترتیب کارمندان در حال تبدیل شدن به خانه‌نشینان اداری هستند [۱۳]؛ زیرا مراکزی که در حومه‌های مناطق کلان شهری پراکنده‌اند و در آن تجهیزات رایانه‌ای شبکه‌ای وجود دارد، به کارکنان از راه دور امکان می‌دهد که از طریق شبکه با شرکت‌های خود کار کنند [۹].

عملیات بانکی از راه دور به سرعت در حال گسترش است و دلیل عمده این امر تمایل بانک‌ها به حذف شعبات و جایگزین کردن آن‌ها با خدمات شبکه‌ای مشتریان و تحویل داری اتوماتیک سیستم‌های تخصصی ارتباطات شبکه‌ای و ارسال تصاویر ویدئویی با کیفیت بالا، ارتباط از راه دور برای مراقبت‌های پزشکی را امکان‌پذیر ساخته است؛ مثلاً جراحان زبردست با استفاده از روشی که امروزه دست کم متداول شده، از طریق کنفرانس ویدئویی بر عمل‌های جراحی که در اقصی نقاط کشور یا جهان صورت می‌گرفت، نظارت می‌کردند. امروزه معاینات بهداشتی منظم نیز از طریق رایانه و تلفن بر مبنای اطلاعات رایانه‌ای و روزآمد بیماران انجام می‌شود. حاضر شکل‌های آموزشی گزینه دوم به شمار می‌روند. تجربیات گسترده‌ی دانشگاه‌های راه دور، صرف نظر از کیفیت آن‌ها، نشان می‌دهد که این دانشگاه‌ها در حال حاضر شکل‌های آموزشی گزینه دوم به شمار می‌روند. پیش‌بینی می‌شود در آینده نزدیک فروشگاه‌ها و مراکز خرید و شرکت‌ها به مفهوم امروزی وجود نخواهند داشت و هر فرد برای خرید مایحتاج زندگی از طریق رایانه وارد یک فروشگاه مجازی خواهد شد؛ سپس از طریق رایانه پول آن را پرداخت خواهد کرد و یا یک شرکت متشکل از یک ساختمان و تعدادی کارمند نخواهد بود؛ بلکه کارمندان هر شرکت در منزل و از طریق شبکه به حل و فصل امور مربوط به شرکت خواهند پرداخت. لذا سایبر به تمام و کمال همه ابعاد زندگی را در بر خواهد گرفت و فضای معماری نیز پسوند سایبر را خواهد پذیرفت [۸]. از این رو معماری جدیدی، از نظر فرم، کارکرد، فرایند و ارزش، در حال شکل‌گیری است؛ وارد شدن بیت‌های اطلاعاتی به فضای معماری بسیاری از تفکیک‌های فضایی و زمانی را از بین خواهد برد و از این پس اتاق‌ها و ساختمان‌ها به حلقه‌های اتصال میان جسم انسان و بیت‌های اطلاعاتی تبدیل خواهند شد [۹]. به این ترتیب می‌توان گفت معماری مجازی نوعی از معماری دیجیتال است که مقید به رعایت ضوابط فیزیکی دنیای سه‌بعدی نبوده و گاهی قابل پیاده شدن در عالم واقع هم نمی‌باشد؛ مانند فیلم‌های کارتونی. اما به هر حال می‌توان کلیه جزئیات هر طرحی را پیش از اجرا در عالم مجازی نمایش داد. با گذشت یک دهه از اینترنت به عنوان یک دنیای قابل تغییر، حال شبکه‌های مجازی به طور کلی به عنوان یک فضای چند بعدی در دنیای واقعی درک می‌شوند [۱۴].

بایستی پذیرفت که مفهوم فضا در آمیخته شدن با سایبر تغییر یافته و شاهد حیطه جدیدی از فعالیت هستیم که در گذشته وجود نداشته است؛ به تعبیری فضای سایبر مفاهیم فضایی را متحول نموده است. موزه‌های مجازی، شهرهای مجازی یا سایبر، فروشگاه‌های مجازی، مدلسازی‌های کامپیوتری و ... نمونه‌هایی از معماری مجازی در فضای سایبر هستند [۹].

## ۷ کلام آخر

در گذشته، رابطه به هم پیوستگی بین ما و فضاهای معماری وجود داشته است، تا حدی که می‌توان گفت معماری به زندگی ما شکل داده است. در قرن حاضر با پیشرفت تکنولوژی و گسترش دنیای سایبری، با تغییر



و دگرگونی در نیازهای فضایی معمارانه روبرو هستیم. طبق یافته‌های پژوهش، مهم‌ترین تأثیرات فضای سایبر بر فضای معماری در جدول ۱ بیان شده است:

جدول ۱: مقایسه فضای فیزیکی و فضای سایبر (نگارنده)

فضای معمارانه	فضای سایبر
دفاتر اداری	دورکاری سایبری
چاپخانه‌ها	نشر سایبری
فروشگاه کتاب، کافه کتاب‌ها، بانک کتاب	فضای ذخیره سایبری
گالری‌ها و موزه‌ها	تورهای سایبری
سینما و سالن تئاتر	شبکه‌های سایبری پخش فیلم
آموزشگاه‌ها، دانشگاه‌ها	آموزش سایبری
بیمارستان و مطب‌های پزشکی	پزشکی و جراحی سایبری
زندان و بازداشتگاه	تکنولوژی حفاظت سایبری
بانک‌ها و مراکز بورس	بانکداری سایبری
مراکز تجاری و فروشگاه‌ها	فروشگاه‌های سایبری

با توجه به تأثیرات فضای سایبر بر فرایند معماری که در جدول شماره ۱ بدان اشاره شد، می‌توان تأثیرات فضای سایبر بر معماری را اینگونه جمع‌بندی کرد:

معماری حقیقی، یک معماری مادی و فیزیکی است که با مصالح مختلف ساختمانی شکل می‌گیرد و سعی دارد از طریق ترکیب فرم و عملکرد به زندگی ما هویت بخشد. معماری سایبری، معماری مجازی و شکل گرفته در فضای دیجیتال است که به مراتب توانایی‌های گسترده‌تری را پیش‌روی معمار نسبت به روش کار سنتی معماری ارائه می‌دهد. در این معماری از فضای سایبری راهی برای ارائه و بازنمایی طراحی و فضا سازی معمارانه است.

در فضای سایبری، معماری دچار استحاله شده است؛ تا اندازه‌ای که دیگر این معماری در دنیای واقعی طراحی نمی‌شود؛ بلکه با برنامه‌ریزی‌های دیجیتال و در گام بعدی با هوش مصنوعی ارائه می‌گردد. با بررسی بناهای معمار ساخت امروز و معادل یا ما به ازای سایبر آن دسته فضاها، به خوبی ثابت می‌شود که نیاز به ساخت فضاهای فیزیکی روز به روز در حال کاهش است. بدون شك نفوذ اینترنت و وجود شرکت‌ها و فروشگاه‌های مجازی، میزان ساخت و ساز را در آینده‌ای نه چندان دور کاهش خواهد داد. بدین ترتیب فضای سایبر با حضور فراوانش نیاز کمتر و کمتری به معماری دارد و سرانجام آن را غیر معمول و زاید می‌کند.

معماری کنونی دیگر با نیازهای جدید هماهنگ نیست و شرایط نوین و ایده‌ها و راهکارهای جدیدی را در زمینه ساخت و ساز و مرتبط ساختن معماری با فضای سایبر طلب می‌کند. بر این اساس طی سال‌های اخیر تمامی مراکز دولتی، ادارات و ... مجبور به تغییرات وسیعی در ساختار فضایی و سازمانی خود شده‌اند تا جوابگوی امکانات و فناوری روز باشند. به نظر می‌رسد فناوری هزاره‌ی سوم هر چه را که با سرعت شتابان پیشرفت نمی‌کند، به کناری می‌گذارد؛ البته ناگفته نماند هر ساختمانی که به اطلاعات وابستگی بیشتری

داشته باشد، با تغییرات اساسی تری مواجه گردیده و کاربری‌ها مانند رستوران و مسکونی کمترین تغییر را در این گذار داشته‌اند.

## مراجع

- [۱] وفامهر، محسن. تعامل معماری و تکنولوژی. انتشارات فکرنو، ۱۳۹۱.
- [۲] تکزی، میلاد و فرخزاد، محمد. بکارگیری مفهوم فضای سایبر در خلق فضاهای معماری (معماری آینده و توجه به وجوه غیر فیزیکی انسان). مجموعه مقالات اولین همایش ملی ساختمان آینده، ۱۳۹۲.
- [۳] گلابچی، محمود، گرمارودی، علی، و باستانی، حسین. معماری دیجیتال: کاربرد فناوری‌های CAD/CAM/CAE در معماری. انتشارات دانشگاه تهران، ۱۳۹۰.
- [۴] پورجعفر، محمدرضا و اخوت، هانیه. مجله ساختمان و کامپیوتر، شماره ۲۳.
- [۵] تمیزی، منوچهر، نظری پورگل سفیدی، لیلا، و شعبانی، رویا. نقش علوم دیجیتال در طراحی معماری. مجموعه مقالات کنفرانس بین‌المللی پژوهش در علوم و تکنولوژی، برلین، آلمان، ۱۳۹۵.
- [۶] خبازی، زوبین. پارادایم معماری الگوریتمیک. مشهد: انتشارات کتابکده کسری، ۱۳۹۱.
- [۷] یوسف‌پور، کمال. معماری در فضای سایبری. مجله معماری ساختمان، شماره ۱، ۱۳۸۹.
- [۸] محمودی، مهناز. کنکاش پیرامون معماری مجازی. فصلنامه معماری و فرهنگ، شماره ۱، ۱۳۸۳.
- [۹] جلیلی، تورج. مفهوم سایبر در تبیین و خلق فضای معماری. مجموعه مقالات اولین همایش ملی و چهارمین همایش مؤسسه آموزش عالی خاوران. «فناوری‌های نوین در علوم مهندسی»، ۱۳۸۹.
- [۱۰] جورابچی، کیوان. مقدمه‌ای بر معماری مجازی. فصلنامه معماری ایران، شماره ۲۱ - ۲۲.
- [۱۱] ملک، م. واقعیت مجازی، جایی بین مرز واقعیت و رویا. ۱۳۹۲.
- [۱۲] غلامی. فضای سایبر در تعامل با معماری. فصلنامه آبادی، شماره ۶۱.
- [۱۳] کاشانی‌جو، خشایار. معماری در عصر اطلاعات. فصلنامه آبادی، شماره ۳۷، ۱۳۸۲.
- [۱۴] تقوی، زهرا بیگم و مدی، حسین. سیر تحول تکنولوژی از هوشمند و مجازی تا تعامل در معماری. مجموعه مقالات همایش ملی معماری و شهرسازی انسانگرا (دانشگاه آزاد اسلامی قزوین)، ۱۳۹۲.
- [15] Muckenheim, M., Demel J. *Inspiration: Contemporary Design Methods in Architecture*. Bispublishers, 2012.
- [16] Park, S., Elnimeiri, M., Sharpe, and D., KrawczykR. *Tall Building Form Generation by Parametric Design Process*. Ph.D. thesis, Illinois Institute of Technology, 2004.

## درآمدی بر انقلاب صنعتی پنجم: کنترل کربن، راهبردی برای کنترل جهان

سیده زهرا موسوی<sup>۱</sup>، محمدعلی شکوهیان راد<sup>۲</sup>

<sup>۱</sup>پژوهشگر و کارشناس ارشد شیمی آلی  
szmousavi@chmail.ir

<sup>۲</sup>پژوهشگر ارشد آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران  
cm@shokoohian.ir

### چکیده

در هر انقلاب صنعتی، متأثر از متغیر تحول آفرین آن انقلاب صنعتی، کیفیت و کمیت توانی که انسان برای اعمال کنترل بر محیط و دیگر انسان‌ها کسب نموده بی‌بدیل است. در یک نگاه، متغیر اصلی کنترل در انقلاب صنعتی یکم شامل ماشین‌های مکانیکی، در انقلاب صنعتی دوم شامل الکتروسیته، در انقلاب صنعتی سوم شامل کامپیوتر و در انقلاب صنعتی چهارم شامل دیجیتالی شدن فرایندها و تکنولوژی‌ها بر بستر هوشمندسازی و ارتباطات شبکه‌ای گسترده و همه‌جاحاضر است. این بدان معنا است که کنترل هر کدام از موارد فوق، تمامی زنجیره‌ی وابسته به آن را کنترل می‌نماید. از سویی بر اساس روندی که فضای بین‌الملل در حدود ۱۰ سال گذشته در حوزه‌ی معاهدات بین‌المللی زیست‌محیطی طی نموده و از سوی دیگر بر اساس برخی پروتکل‌های کنترلی مؤکد در انقلاب صنعتی چهارم نظیر کنترل هوشمند میزان مصرف سرانه‌ی کربن؛ پیش‌بینی می‌شود که اولاً جهان در آینده‌ی نه‌چندان دور با انقلاب صنعتی پنجم مواجه شود و ثانیاً مبنای کنترلی آن، عنصر کربن و تمامی مشتقات صنعتی آن باشد. در این زمینه، تعامل ویژه‌ی دانش سایبرنتیک و تکنولوژی‌های هوش مصنوعی با مقوله‌ی کنترل تولید و مصرف کربن که زمینه‌ساز اجرای «استاندارد کم‌کربن» در سند توسعه‌ی پایدار ۲۰۳۰ است، جایگاه ویژه‌ای دارد که باعث می‌شود انقلاب صنعتی پنجم بر بستر انقلاب صنعتی چهارم به‌وقوع بپیوندد. آنچه در این میان برای جمهوری اسلامی ایران بسیار مهم است، این است که مراقبت نماید تا اجرای پروتکل‌های استاندارد کربن، موجب توقف انواع صنایع کشور که به‌صورت‌های مستقیم و غیرمستقیم به کربن و مشتقات آن وابسته هستند، نگردد.

**کلمات کلیدی:** سایبرنتیک، انقلاب صنعتی پنجم، استاندارد کربن، کنترل کربن، کنترل جهان.

### ۱ مقدمه

کربن و مشتقات آن، حائز جایگاه کلیدی در خلقت و تمدن بشری هستند. این اهمیت تا آنجا است که وقوع اکثر انقلاب‌های صنعتی بدون حضور اشکال مختلف کربن غیر ممکن به‌نظر می‌رسد. ترکیبات هیدروکربنی

یکی از موضوعات اصلی مطالعات شیمی و پلیمر، مواد نفتی و پتروشیمی و بسیاری صنایع دیگر است. به سختی می‌توان ماده‌ی دیگری را یافت که طیف تنوع آن به این میزان گسترده باشد و هر یک از ساختارهای آن چون الماس، گرافیت، الیاف کربن، گرافن، نانو لوله‌ی کربن، فولرن و مشتقات آنها، ویژگی‌های منحصر به فردی را ارائه دهد. از این رو شاید بتوان گفت تحول‌آفرینی نانو در کربن بیش از دیگر حوزه‌ها مشهود و مؤثر است. امکان ایجاد و یا تغییر در پیوندهای شیمیایی کربن، منشأ ساختارهای متنوع آن است؛ از این رو آن را به مهندسی پذیرترین عنصر طبیعت تبدیل کرده که سهم صنعتی، اقتصادی و تکنولوژیک خاصی را در جهان کنونی ایفا می‌نماید.

حال با توجه به توضیحات فوق، می‌توان ادعان داشت که اگر تولید و مصرف کربن و انواع مشتقات آن در یک کشور کنترل شود؛ به تبع می‌توان تقریباً تمامی صنایع وابسته به آن را کنترل نمود. بر این اساس، کربن ظرفیت بالایی دارد که به یک متغیر کنترلی جهانی تبدیل شود.

این مهم، ریشه در نگاه دانش سایبرنتیک دارد و محرز است که هر چقدر یک متغیر کنترلی، نقش گسترده‌تر و عمیق‌تری را در بسترسازی بخشی از تمدن ایفا کند، اعمال کنترل از طریق آن متغیر بر تمدن بیشتر، مؤثرتر و سریع‌تر خواهد شد. لذا از منظر سایبرنتیک، کنترل کربن یک متغیر بسیار مهم برای جهت‌دهی به رفتار، سمت‌گیری و شکل‌دهی آینده‌ی کشورها و جوامع می‌باشد، خصوصاً از منظر وابستگی صنعتی و همچنین پیشرفت تکنولوژی‌های نوین و نوظهور. این گزاره تا آنجا می‌تواند عمیق و گسترده گردد که به‌عنوان مبنا و زمینه‌ساز **انقلاب صنعتی پنجم** مدنظر قرار گیرد. لذا توجه به پروتکل‌ها و استانداردهای بین‌المللی و ملی کنترل کربن، بسیار حائز اهمیت است.

پژوهش حاضر از این جنبه دارای نوآوری است که اولاً موضوع کنترل کربن را از منظر مقوله‌ی کنترل در دانش سایبرنتیک مورد مطالعه و بررسی قرار داده است و ثانیاً ترسیم آینده‌ی جهان بر بستر کنترل کربن را در قالب انقلاب صنعتی پنجم تشریح و ترسیم نموده.

بدین منظور، ساختار محتوایی پژوهش حاضر چنین است که ابتدا نقش کلیدی کربن در صنعت، اقتصاد و تکنولوژی تشریح می‌شود؛ سپس برخی پروتکل‌ها و استانداردهای سنجش میزان کربن معرفی می‌گردد؛ پس از آن نقش پروتکل‌های مذکور و سایر موارد مشابه در کنترل جهانی کربن توضیح داده می‌شود و نهایتاً مبتنی بر نگاه دانش سایبرنتیک مشخص می‌گردد که چگونه مقوله‌ی کنترل کربن، ظرفیت تبدیل شدن به انقلاب صنعتی پنجم در جهان را دارا است.

## ۲ پیشینه‌ی پژوهش

بیل گیتس در پیشگفتار کتابی با عنوان «چگونه از فاجعه اقلیمی جلوگیری کنیم؟» به اصطلاح «۵۱ میلیارد به صفر» اشاره کرده است. وی در بخش مذکور بیان می‌دارد «انسان‌ها برای جلوگیری از گرم شدن هوا و جلوگیری از بدترین اثرات تغییر اقلیم - که این تأثیرات بسیار بد خواهند بود - باید از اضافه کردن گازهای گلخانه‌ای به جو پرهیز کنند؛ یعنی میزان ۵۱ میلیارد تن گاز گلخانه‌ای سالانه را تدریجاً به صفر برسانند» (بیل گیتس، ۱۴۰۰). گیتس در کتاب مذکور به پروتکل‌ها و استانداردهایی اشاره می‌کند که ذیل یک همکاری

جهانی می‌تواند هدف فوق را محقق سازد.

در **سند توسعه‌ی پایدار ۲۰۳۰** و ذیل هدف سیزدهم، صراحتاً به استاندارد کم کربن و صفر شدن میزان کربن دی‌اکسید اشاره شده است. در بخشی از سند مذکور آمده است «جهان در رسیدن به هدف توافقنامه‌ی پاریس مبنی بر محدود کردن گرمایش جهانی به ۵.۱ درجه‌ی سانتی‌گراد بالاتر از سطح قبل از صنعتی شدن و رسیدن به صفر خالص انتشار دی‌اکسید کربن در سطح جهان تا سال ۲۰۵۰، به طرز تأسف باری از مسیر خارج شده است» (سازمان ملل، ۲۰۲۱).

مقاله‌ی «انتقال به اقتصادهای کم کربن تحت دستور کار ۲۰۳۰: به حداقل رساندن مبادلات تجاری و افزایش منافع مشترک اقدام در زمینه تغییر اقلیم برای اهداف توسعه پایدار»<sup>۱</sup> که توسط گابریلا ایلینا یاکوبوتا<sup>۲</sup> و همکارانش نگاشته شده است، تلاش نموده تا با روش‌های مختلف، با تأکید بر هدف‌گذاری سند توسعه‌ی پایدار ۲۰۳۰ نسبت به عملیاتی‌سازی استاندارد کم کربن، راه‌حلی برای کنترل مصرف کربن ارائه نماید. وی بیان داشته «از طریق بررسی ادبیات گسترده، متوجه شدیم که اقدامات کاهش تغییرات آب و هوایی به‌طور مستقیم بر بیشتر اهداف ۲۰۳۰، عمدتاً از طریق منافع مشترک، تأثیر می‌گذارد. بهبود بهره‌وری انرژی، کاهش تقاضای خدمات انرژی و روی آوردن به انرژی‌های تجدیدپذیر بیشترین مزایا را به همراه دارد. در مقابل، جذب و ذخیره‌سازی کربن و انرژی هسته‌ای احتمالاً به مبادلات متعدد منجر می‌شود.» (ایلینا یاکوبوتا و همکاران، ۲۰۲۱).

سابق بر این در قراردادهای بین‌المللی نیز **معاهده‌ی اقلیمی پاریس و قرارداد مونترال**، به موضوع کنترل جهانی تولید و مصرف کربن و تعهد کشورها برای کاهش میزان آن بر اساس پروتکل‌های بین‌المللی اشاره و تأکید شده است. قرارداد مونترال یا پروتکل مونترال در خصوص مسائلی است که باعث تخریب لایه‌ی ازن می‌شوند و اساساً یک معاهده‌ی بین‌المللی است که برای محافظت از لایه‌ی ازن با خاتمه دادن به تولید مواد بی‌شماری که عامل کاهش ازن هستند طراحی شده است (خبرگزاری ایمن، ۱۴۰۰).

اعظم محمدباقری در مقاله‌ای با عنوان «اقتصاد کم کربن و سیاست‌های کاهش انتشار گازهای گلخانه‌ای»، در خصوص پروتکل‌های کم کربن‌سازی اقتصاد بیان داشته «حرکت به سوی اقتصاد کم کربن، مستلزم انجام فعالیت‌هایی است که ... از انتشار دی‌اکسید کربن جلوگیری کند که ... سیستم‌های کنترل هوشمند ساختمان نمونه‌هایی از تکنولوژی‌ها، فرایندها و خدماتی هستند که پاسخگوی این ضرورت می‌باشند» (محمدباقری و همکاران، ۱۳۹۲، صص ۱۸-۲۰). لذا تأکید شده که زیرساخت هوشمند از ضرورت‌های کنترل کربن می‌باشد.

در مقاله‌ای دیگر با عنوان «ارزیابی پایداری محله‌های شهری با رویکرد محله‌ی کم کربن» صابر محمدپور نسبت به الگوی اجرای کم کربن، بیان داشته «دانشمندان برای دستیابی به جامعه‌ی کم کربن و توسعه‌ی پایدار، تمرکز خود را بر روی نظام‌های طراحی و برنامه‌ریزی به‌منظور ارزیابی محله‌ی کم کربن معطوف کرده‌اند» (محمدپور و همکاران، ۱۳۹۹). وی در ادامه با بررسی‌های کیفی و کمی، روش‌های برتر آزموده

<sup>1</sup> Transitioning to Low-Carbon Economies under the 2030 Agenda: Minimizing Trade-Offs and Enhancing Co-Benefits of Climate-Change Action for the SDGs

<sup>2</sup> Gabriela Ileana Iacobuță

شده در خصوص کنترل کربن را معرفی و تشریح می‌نماید.

مهدی مجیدپور نیز در مقاله‌ای با نام «جذب و ذخیره‌سازی کربن، سیاست‌گذاری فناوری برای گذار به اقتصاد کم کربن» به این مهم اشاره می‌کند که «فوریت پاسخگویی به تغییرات اقلیمی ناشی از مصرف سوخت‌های فسیلی باعث شده است تا توسعه‌ی تکنولوژی‌های کم کربن، بیش از پیش مورد توجه قرار بگیرد» (مجیدپور، ۱۳۹۱). وی در ادامه تأکید دارد که برای اجرای پروتکل‌های کم کربن، باید از سد چهار دسته چالش فنی، اقتصادی، اجتماعی و زیست‌محیطی عبور کرد؛ زیرا کنترل کربن بر حوزه‌های مذکور اثرگذار است.

## ۳ ادبیات پژوهش

### ۱.۳ نقش کلیدی کربن در صنعت، اقتصاد و تکنولوژی

به دلیل گستردگی ترکیبات کربنی و هیدروکربنی و کاربردهای بسیار زیاد آنها؛ امکان بررسی تمامی ترکیبات موجود در پژوهش حاضر میسر نیست. لذا صرفاً به میزانی از بیان موارد فوق اکتفا می‌شود که بتوان جایگاه این عنصر مهم و حیاتی را برای ورود به مبحث اصلی مشخص و اثبات نمود.

#### - زغال سنگ، نفت، گاز

زغال سنگ، ماده‌ی اصلی در تولید محصولاتی چون کربن فعال است. از زغال سنگ، کک تهیه می‌شود که سوخت نیروگاه‌های برق را فراهم می‌آورد (IEA, ۲۰۲۱). در حال حاضر ۳۵٪ تا ۳۸٪ برق جهان به‌وسیله‌ی زغال سنگ تأمین می‌شود (انجمن جهانی زغال سنگ، ۲۰۲۱). پس از تولید انرژی الکتریکی، صنایع فولاد و سپس تولید سیمان رتبه‌های بعدی مصرف زغال سنگ را دارا هستند. از زمان امضای توافقنامه اقلیمی پاریس ۲۱ کشور متعهد شده‌اند که تولید با سوخت زغال سنگ را از بخش برق خود تا سال ۲۰۳۰ حذف کنند. این ۲۱ کشور ۳.۲ درصد از تولید برق جهانی در سال ۲۰۲۰ و یا تولید ۱٪ از دی‌اکسید کربن جهان را تشکیل می‌دهند (IEA, زغال سنگ، ۲۰۲۱).

درباره‌ی جایگاه نفت و گاز نیازی به توضیح نیست اما می‌توان ضرورت تولید برق که نیاز الزامی دیگر صنایع به انرژی‌های فسیلی در جهان است را از جدول ۱ استخراج و با نسبت مصرف به امضاکنندگان معاهده‌ی پاریس بیشتر مقایسه نمود.

طبق گزارش مؤسسه‌ی جهانی زغال سنگ، تولید ۷۰٪ فولاد جهان به روش کوره‌ی بلند با بهره‌گیری از زغال سنگ تولید می‌شود (انجمن جهانی زغال سنگ، ۲۰۲۲). همچنین زغال سنگ در صنایع دیگری مانند آلومینا، صنایع شیمیایی و دارویی، بازیابی آمونیاک برای تولید کود شیمیایی، تولید آلیاژها و فروآلیاژها به دلیل تولید انرژی کاربرد دارد. به‌عنوان مثال تولید آلومینیوم نیاز شدیدی به برق دارد و در سال ۲۰۲۰ میزان برق مصرفی جهانی برای ذوب اولیه‌ی آلومینیوم ۱۴۲۷۳ KWH/T<sup>۳</sup> تخمین زده شده است (IEA, آلومینیوم، ۲۰۲۱).

<sup>۳</sup> کیلووات ساعت بر تن



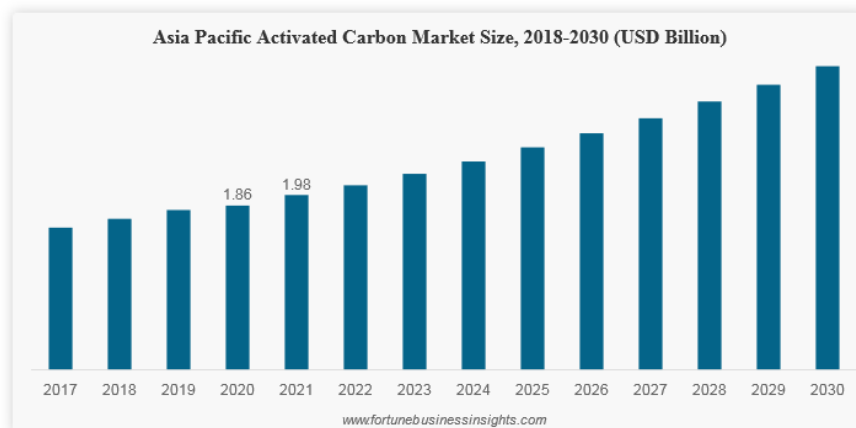
جدول ۱: میزان تولید برق از سوخت‌های فسیلی در کشورهای جهان

Electricity generation by fuel\*

Terawatt-hours	2020							2021								
	Oil	Natural Gas	Coal	Nuclear energy	Hydro electric	Renewables	Other†	Total	Oil	Natural Gas	Coal	Nuclear energy	Hydro electric	Renewables	Other†	Total
Canada	2.9	73.6	38.6	97.5	386.5	49.3	0.6	649.1	2.9	75.9	38.7	92.0	380.8	50.0	0.7	641.0
Mexico	32.4	200.1	18.9	11.2	26.9	36.2	-	325.7	32.8	203.3	13.6	11.9	34.7	39.7	-	336.0
US	18.6	1746.4	844.3	831.5	282.8	547.7	13.5	4284.8	20.2	1693.8	978.5	819.1	257.7	624.5	12.7	4406.4
<b>Total North America</b>	<b>54.0</b>	<b>2070.1</b>	<b>901.9</b>	<b>940.1</b>	<b>696.3</b>	<b>633.2</b>	<b>14.1</b>	<b>5259.7</b>	<b>55.9</b>	<b>1973.0</b>	<b>1030.7</b>	<b>923.0</b>	<b>673.3</b>	<b>714.1</b>	<b>13.5</b>	<b>5383.5</b>
Argentina	7.1	88.0	1.6	10.7	23.7	13.0	0.6	144.6	7.9	93.3	2.9	10.8	19.6	17.2	0.6	152.5
Brazil	10.5	53.5	20.3	14.1	396.4	126.5	-	621.3	21.9	86.9	24.1	14.7	362.8	144.0	-	654.4
Other S. & C. America	66.3	90.5	49.1	-	271.2	59.5	†	536.6	66.1	100.9	45.3	-	277.7	68.1	†	558.0
<b>Total S. &amp; C. America</b>	<b>83.9</b>	<b>231.9</b>	<b>71.1</b>	<b>24.7</b>	<b>691.2</b>	<b>199.1</b>	<b>0.6</b>	<b>1302.5</b>	<b>95.9</b>	<b>281.1</b>	<b>72.3</b>	<b>25.5</b>	<b>660.1</b>	<b>229.3</b>	<b>0.6</b>	<b>1364.8</b>
Germany	4.7	95.0	134.6	64.4	18.3	231.8	24.8	573.6	4.8	89.0	162.6	69.0	19.1	217.6	22.4	584.5
Italy	11.4	133.7	15.1	-	45.7	68.8	5.8	280.5	8.3	146.4	14.5	-	43.1	71.4	3.5	287.2
Netherlands	1.4	72.6	7.6	4.1	†	33.0	4.9	123.6	1.4	56.3	17.8	3.8	0.1	40.1	2.1	121.6
Poland	1.7	17.3	109.4	-	2.1	25.3	1.3	157.1	1.5	15.5	131.7	-	2.3	27.8	1.3	180.0
Spain	10.7	69.7	6.1	58.3	30.5	83.2	4.7	263.4	10.3	69.2	6.1	56.5	29.6	95.8	4.7	272.1
Turkey	0.3	70.9	105.8	-	78.1	51.5	-	306.7	0.3	110.4	104.2	-	55.7	62.7	-	333.3
Ukraine	0.3	14.2	40.2	76.2	7.6	9.4	-	147.8	0.8	10.3	36.8	86.2	10.4	11.0	-	155.5
United Kingdom	0.8	111.4	5.5	50.3	6.8	127.8	9.3	312.0	1.5	124.2	6.5	45.9	5.0	116.9	9.9	309.9
Other Europe	17.4	180.5	145.4	580.0	468.8	291.8	30.3	1714.2	19.1	178.1	151.9	621.4	484.4	303.2	30.3	1783.3
<b>Total Europe</b>	<b>48.9</b>	<b>765.4</b>	<b>669.7</b>	<b>833.2</b>	<b>657.9</b>	<b>922.7</b>	<b>81.1</b>	<b>3879.0</b>	<b>47.9</b>	<b>799.3</b>	<b>632.0</b>	<b>882.8</b>	<b>649.7</b>	<b>946.5</b>	<b>74.2</b>	<b>4032.5</b>
Kazakhstan	0.1	27.3	69.4	-	9.7	2.3	-	108.6	0.1	32.9	69.3	-	9.1	3.0	-	114.4
Russian Federation	8.2	464.9	175.8	215.9	212.4	3.5	4.7	1085.4	8.5	496.8	204.7	222.4	214.5	5.4	4.7	1157.1
Other CIS	2.7	153.6	4.3	3.1	41.1	1.0	0.7	206.6	3.4	156.6	4.3	7.8	42.7	1.2	0.6	216.5
<b>Total CIS</b>	<b>11.0</b>	<b>645.8</b>	<b>249.5</b>	<b>219.0</b>	<b>263.2</b>	<b>6.8</b>	<b>5.3</b>	<b>1400.7</b>	<b>11.9</b>	<b>686.4</b>	<b>278.3</b>	<b>230.2</b>	<b>266.3</b>	<b>9.6</b>	<b>5.3</b>	<b>1488.0</b>
Iran	37.0	268.2	0.7	6.3	23.2	1.8	-	337.2	48.7	288.3	0.7	3.5	14.9	1.8	-	357.8
Saudi Arabia	130.8	207.0	-	-	-	0.2	-	338.0	139.9	215.9	-	-	-	0.8	-	356.6
United Arab Emirates	†	132.7	-	1.6	-	4.6	-	137.3	†	123.7	-	10.5	-	5.2	-	139.4
Other Middle East	114.7	282.7	19.0	-	4.9	9.1	†	430.4	117.6	301.8	17.0	-	4.6	10.7	-	451.7
<b>Total Middle East</b>	<b>282.5</b>	<b>890.7</b>	<b>19.7</b>	<b>8.0</b>	<b>28.1</b>	<b>15.7</b>	<b>†</b>	<b>1243.0</b>	<b>306.1</b>	<b>929.7</b>	<b>17.7</b>	<b>14.1</b>	<b>19.5</b>	<b>18.5</b>	<b>-</b>	<b>1305.6</b>
Egypt	22.7	151.3	-	-	14.9	9.7	-	198.6	26.9	157.6	-	-	14.6	10.5	-	209.7
South Africa	1.4	-	202.6	13.9	0.7	15.7	5.1	239.5	1.6	-	209.6	10.4	1.4	16.5	4.8	244.3
Other Africa	42.5	185.8	37.2	-	130.8	20.0	0.7	417.0	47.7	197.9	37.8	-	137.4	22.0	0.7	443.5
<b>Total Africa</b>	<b>66.7</b>	<b>337.0</b>	<b>239.8</b>	<b>13.9</b>	<b>146.4</b>	<b>45.4</b>	<b>5.8</b>	<b>855.1</b>	<b>76.2</b>	<b>355.6</b>	<b>247.4</b>	<b>10.4</b>	<b>153.4</b>	<b>49.0</b>	<b>5.5</b>	<b>897.5</b>
Australia	4.5	53.1	142.9	-	14.4	49.9	0.4	265.2	4.7	47.6	137.4	-	16.0	61.3	0.4	267.5
China	10.8	252.5	4920.8	366.2	1321.7	863.2	43.8	7779.1	12.2	272.6	5339.1	407.5	1300.0	1152.5	50.2	8534.3
India	2.1	74.5	1125.8	44.6	163.7	152.0	0.6	1563.3	2.3	64.2	1271.1	43.9	160.3	171.9	1.1	1714.8
Indonesia	6.8	51.3	180.9	-	24.3	28.6	†	291.8	6.6	56.3	190.0	-	24.7	31.5	0.3	309.4
Japan	36.7	353.6	298.0	43.0	77.4	117.8	70.6	997.0	31.3	326.1	301.9	61.2	77.6	130.3	91.3	1019.7
Malaysia	0.9	53.6	84.2	-	27.9	2.8	-	169.5	1.1	63.3	77.3	-	32.4	3.1	-	177.2
South Korea	6.7	159.9	209.6	160.2	3.9	31.1	3.7	575.3	7.0	176.4	211.7	158.0	3.1	40.2	4.1	600.4
Taiwan	4.4	99.9	125.9	31.4	3.0	10.4	4.9	280.0	5.3	108.3	128.9	27.8	3.5	12.1	5.0	290.9
Thailand	0.7	113.9	36.8	-	4.5	20.5	†	176.5	0.7	113.1	36.1	-	4.5	21.9	†	176.3
Vietnam	1.3	34.0	114.8	-	73.4	12.1	-	235.4	0.2	26.2	114.1	-	75.9	28.3	-	244.8
Other Asia Pacific	39.9	234.6	147.8	9.5	148.5	35.4	0.6	616.3	54.7	239.3	158.1	15.9	153.7	36.9	0.7	659.1
<b>Total Asia Pacific</b>	<b>114.8</b>	<b>1480.7</b>	<b>7387.7</b>	<b>655.0</b>	<b>1862.9</b>	<b>1323.7</b>	<b>124.7</b>	<b>12949.3</b>	<b>126.3</b>	<b>1493.4</b>	<b>7965.6</b>	<b>714.3</b>	<b>1851.6</b>	<b>1690.1</b>	<b>153.1</b>	<b>13904.4</b>
<b>Total World</b>	<b>661.7</b>	<b>6371.7</b>	<b>9439.3</b>	<b>2694.0</b>	<b>4346.0</b>	<b>3146.6</b>	<b>230.0</b>	<b>26889.2</b>	<b>720.3</b>	<b>6518.5</b>	<b>10244.0</b>	<b>2800.3</b>	<b>4273.8</b>	<b>3657.2</b>	<b>252.2</b>	<b>28466.3</b>
of which: OECD	145.6	3399.6	2065.6	1872.3	1483.3	1766.1	168.2	10900.7	142.5	3372.4	2253.0	1911.0	1440.3	1910.1	181.0	11210.2
Non-OECD	516.0	2972.0	7373.7	821.7	2862.7	1380.5	61.8	15988.5	577.8	3146.1	7991.0	889.2	2833.6	1747.2	71.2	17256.1
European Union	45.5	561.4	369.1	683.8	343.2	710.6	65.4	2779.0	43.0	548.0	439.2	732.2	344.4	730.2	58.4	2895.3

بر اساس گزارش سالانه‌ی مرکز تحقیقات و سیاست اقتصاد انرژی<sup>۴</sup> بیش از یک تریلیون تن ذخایر ثابت زغال سنگ در سراسر جهان وجود دارد که بیشترین استخراج و تولید به ترتیب متعلق به کشورهای چین، اندونزی، هند، استرالیا و آمریکا است و در رقم ارزی واردات نیز چین معادل ۴۰۱۶ میلیارد دلار، ژاپن ۹۵۰۱۵ میلیارد دلار، هند ۱۵/۸۷ میلیارد دلار است. با این تفاسیر جایگاه مصرف‌کنندگان زغال سنگ در دنیا به ترتیب کشور چین به تنهایی ۵۰٪، هند ۱۱/۳٪، آمریکا ۸/۵٪، و سپس ژاپن می‌باشد (آمار جهانی انرژی، ۲۰۲۲). به روشنی قابل استنباط است که ایران جایگاه قابل توجهی را در هیچ یک از موارد تولید، واردات و یا مصرف زغال سنگ ندارد و به همین نسبت با تقسیم بر صنایع اصلی مصرف‌کننده‌ی زغال سنگ؛ صنایع تولید برق، فولاد، سیمان و... هریک سهم ناچیزتری را به خود اختصاص می‌دهند.

<sup>4</sup>Centre for Energy Economics Research and Policy



شکل ۱: سهم ارزی رو به رشد بازار آسیا از مصرف کربن فعال

### - کربن فعال

این ماده که در صنعت به چارکول<sup>۵</sup> نیز معروف است به دلیل مساحت سطحی بالا، کاربرد بالایی در جذب گازها، تصفیه‌ی هوا، آب و پساب، جذب ناخالصی‌ها و بو و طعم نامطلوب دارد. از دلایل مصرف بالای چارکول سهولت جمع‌آوری آن از مواد ترکیب شده و غیر سمی بودن آن در صورت استعمال است. سهم بازار جهانی آن ۴/۷۷ میلیارد دلار در سال ۲۰۲۱ ارزش‌گذاری شده و پیش‌بینی برای سال ۲۰۳۰ معادل ۷/۷۳ میلیارد دلار است (گزارش تحقیق بازار، ۲۰۲۲).

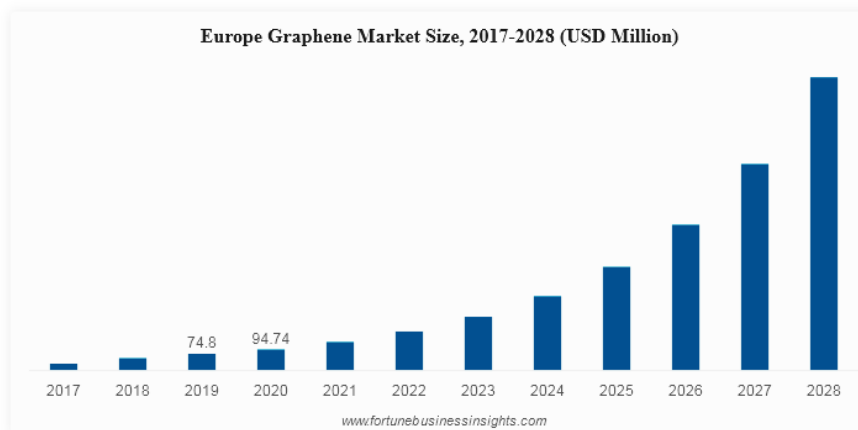
### - گرافیت

شکلی از کربن است که خواص فلزی و غیرفلزی از جمله هدایت گرمایی و الکتریکی بالای آن، این ماده را برای مصارف صنعتی ایده‌آل نموده است. عمده‌ی مصرف گرافیت کربن در نسوزها، ریخته‌گری، روان‌سازها، باتری لیتیومی، صنایع فولاد و لاستیک است. افزودن ۰/۰۵ تا ۲/۱ درصد وزنی کربن به فولاد (فولاد کربنی) موجب افزایش استحکام آن می‌شود. همچنین استفاده از الکتروود گرافیتی برای کوره‌ی قوس الکتریکی در تولید فولاد ضروری است (دنیل استپیچ، ۲۰۲۱). صنعت نسوز شامل آستر برای کوره‌ها، راکتورها و زباله‌سوزها می‌شود. مقیاس بازار جهانی از مصرف این ماده ۶۰/۱۳ میلیارد دلار در سال ۲۰۲۰ بوده و تا سال ۲۰۲۸ به ۷۰/۲۵ میلیارد دلار خواهد رسید (گزارش تحقیق بازار، ۲۰۲۱، ص ۱۰).

### - گرافن

گرافن یک نانو ماده‌ی دو بعدی با دوام، انعطاف‌پذیر و نیمه‌هادی است که از جداسازی ورقه‌های لایه ماند گرافیت به ضخامت یک لایه‌ی اتم تهیه می‌شود (بلال ناسف، ۲۰۲۰). اهمیت این محصول که با تکنیک‌های خاصی تولید می‌شود به واسطه‌ی خواص ویژه و منحصر به فرد خود و دیگر موادی که از آن مشتق می‌شود

<sup>5</sup>Charcoal



شکل ۲: مقیاس بازار گرافن در اروپا، بازه‌ی زمانی ۲۰۱۷ تا ۲۰۱۸ میلادی - ارقام بر حسب میلیون دلار

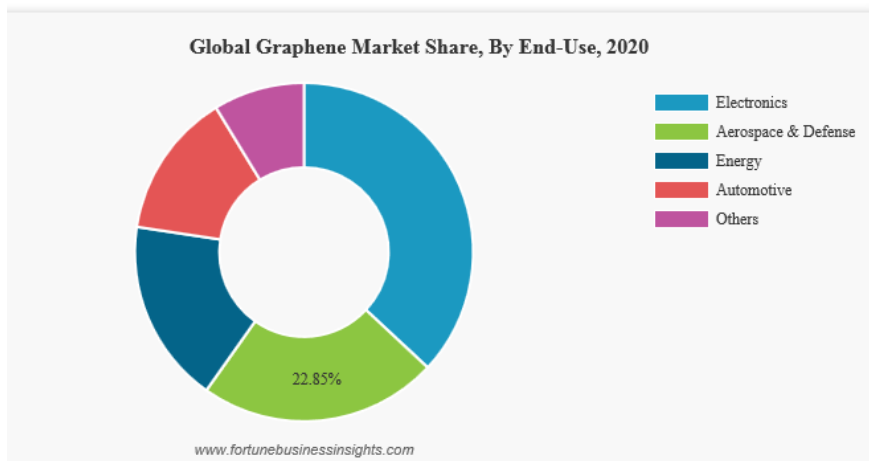
مانند اکسید گرافن، نانوپلاکت گرافن، نانولوله‌ی تک لایه و دولایه؛ بسیار مورد توجه بازار اقتصاد و تکنولوژی است. گرافن از لحاظ شیمیایی بی‌اثر و دارای ظرفیت بالای انتقال الکترون است (وونبونگ چوی، ۲۰۱۰). کاربردهای متنوع مانند الکترونیک، ذخیره‌ی انرژی، کامپوزیت‌ها، رنگ‌ها و روکش‌ها در بازار، محرک رشد تقاضای تجارت گرافن بوده است. پیش‌بینی می‌شود اندازه‌ی بازار گرافن از ۸۲۱/۲ میلیون دلار در سال ۲۰۲۱ به ۷/۵ میلیارد دلار در سال ۲۰۲۸ افزایش یابد و فقط سهم بخش الکترونیک تا سال ۲۰۳۰ معادل ۳۷۰ میلیون دلار باشد.

بخش خودرو تا سال ۲۰۳۰ بیش از ۱۵ درصد از سهم بازار گرافن را در اختیار خواهد داشت. صنعت خودرو بر تولید خودروهایی با وزن سبک‌تر و در عین حال مطابق با استانداردهای ایمنی اجباری تمرکز دارد. انتظار می‌رود که سازندگان خودرو، استفاده از کامپوزیت‌ها را در مقیاس بزرگ برای تولید خودروهای سبک وزن با کیفیت برتر افزایش دهند.

گرافن برای تولید چسب‌های هوشمند، نانوکامپوزیت‌ها برای حسگرهای یکپارچه و سایر اجزای خودرو که احتمالاً در آینده‌ی نزدیک تجاری می‌شوند، استفاده می‌شود. بازیگران بازار به طور مداوم بر توسعه‌ی محصول و نوآوری تمرکز می‌کنند تا به مزیت رقابتی در صنایع مختلف مصرف نهایی<sup>۶</sup> دست یابند.

در سال ۲۰۲۰ میلادی، آسیا و اقیانوسیه بیشترین سهم بازار جهانی را داشتند. عامل اصلی رشد بازار در این منطقه برای گرافن از الکترونیک، رنگ‌ها و پوشش‌ها، پلیمر، ذخیره‌ساز انرژی و صنایع خودرو است. بخش‌های الکترونیک پیشرفته و ذخیره‌ی انرژی به‌ویژه در ژاپن، چین و کره‌ی جنوبی موجب ادامه‌ی افزایش مصرف گرافن در آسیا و اقیانوسیه خواهد شد. این منطقه از کشورهای در حال توسعه مانند چین، هند، کره‌ی جنوبی، سنگاپور، تایوان و اندونزی تشکیل شده است. این کشورها دارای امکانات تولید در مقیاس بزرگ در بخش‌های مختلف از جمله مواد شیمیایی، ساختمانی، خودرو و الکترونیک هستند. علاوه بر این سرمایه‌گذاری در توسعه‌ی تکنولوژی‌ها در چین نیز عامل مهمی برای تقاضای گرافن در منطقه است. بنابراین

<sup>6</sup>End Use



شکل ۳: سهم بازار جهانی گرافن بر مبنای مصرف نهایی؛ به ترتیب: الکترونیک، فضایی و دفاعی، انرژی و خودرو

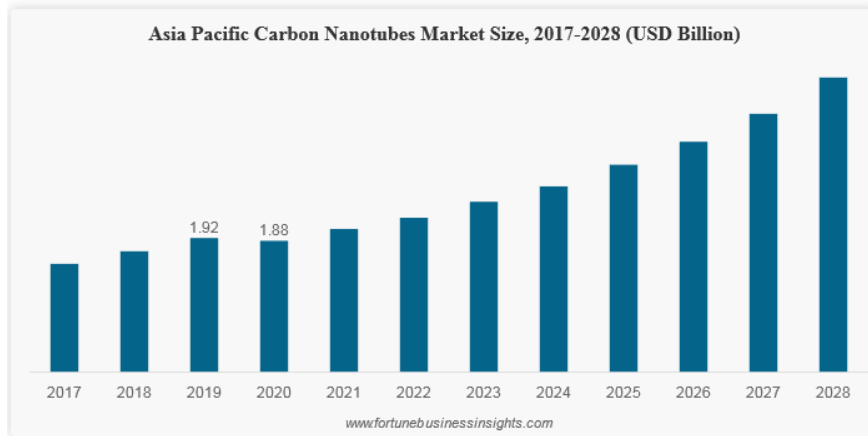
رشد صنایع مصرف کننده نهایی باعث ایجاد بازار گرافن می شود. علاوه بر این آمار، با توجه به نمودار شماره ۳ که پیش بینی بازار تقاضای گرافن در قاره ی اروپا است، مشاهده می شود که همچنان کشور ایران سهم آماری قابل بینی را در گزارش های بین المللی دارا نیست (بینش بازار جهانی، ۲۰۲۱ و گزارش تحقیق بازار، ۲۰۲۲، ص ۸۰).

### - نانو لوله ی کربن

نانو لوله ی کربن<sup>۷</sup> یک ساختار لوله مانند توخالی است که از لوله شدن یک صفحه ی گرافن تولید می شود. گستره ی بازار جهانی نانو لوله ی کربن معادل ۴۹.۴ میلیارد دلار در سال ۲۰۲۰ میلادی بوده است و انتظار می رود تا سال ۲۰۲۸ به ۵۲.۱۰ میلیارد دلار برسد. برای توجیه چنین ارقام بالایی باید گفت که نانو لوله های کربنی در زمینه های خاص و پیشرفته کاربرد دارند، نظیر مواردی که نیاز به استحکام بالا، دوام، کم وزنی در عین استحکام و هدایت حرارتی در مقایسه با مواد دیگر باشد. از این رو جایگاه ویژه ای در صنایع نظامی و هوافضا دارد.

تحقیقات مدل سازی ناسا پیش بینی می کند کامپوزیت هایی که از تقویت کننده ی نانو لوله استفاده می کنند، می توانند به کاهش ۳۰ درصدی جرم کل یک وسیله منتج شود. در پژوهشی دیگر مهندسان دانشگاه MIT در سال ۲۰۱۹ یک ریزپردازنده ی پیشرفته تر از ترانزیستور، توسط نانو لوله ی کربنی ساخته اند که جایگزین همتایان ترانزیستوری خود با ده برابر بازده انرژی بیشتر است. همچنین در آنتن برای دستگاه های الکترومغناطیسی و رادیویی، باتری لیتیومی، سلول های خورشیدی و سوختی، نمایشگر انتشار میدانی و ... تقاضای نانو لوله ی کربنی وجود دارد.

<sup>7</sup>Carbon Nano Tubes (CNTs)



شکل ۴: پیش‌بینی میزان بازار نانو لوله‌ی کربن در آسیا، سال ۲۰۱۷ تا ۲۰۲۸ بر حسب میلیارد دلار

بر اساس داده‌های سال ۲۰۲۰ میلادی در حوزه‌ی مصارف و کاربردهای نانو لوله‌های کربنی، حوزه‌های پلاستیک و کامپوزیت در جایگاه نخست قرار دارد و پس از آن صنایع الکتریکی و الکترونیکی و انرژی در رده‌های دوم و سوم هستند (گزارش تحقیق بازار، ۲۰۲۱، ص ۲۰۰). همچنین مصارف گسترده‌ای برای نانو لوله‌های کربنی در زمینه‌ی پزشکی وجود دارد که اهم آنها در نمودار شماره ۶ مشخص شده است (بوشان مورجانی، ۲۰۲۲).

### - فیبر کربن

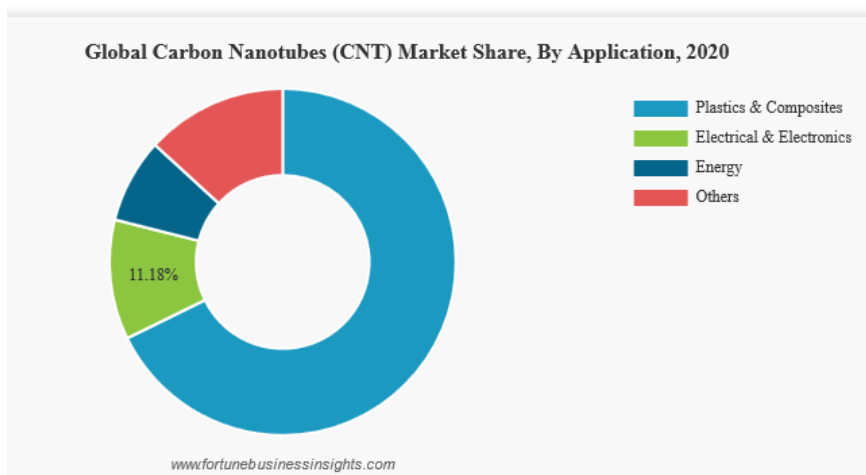
پلیمرهای هیدروکربنی که بالای نود درصد کربن داشته باشند، در فرایند دمایی بالا تبدیل به فیبر می‌شوند که هدایت الکتریکی چشمگیر و استحکام بالایی (تقریباً ده برابر فولاد با یک سوم وزن آن) را دارند. ترتیب سهم کاربرد فیبر کربن در انرژی بادی، هوافضا، تجهیزات ورزشی (از جمله دریایی) و خودرو است (پایگاه استاتیسنا، ۲۰۲۱).

### ۲.۳ سنجش میزان کربن مصرف شده

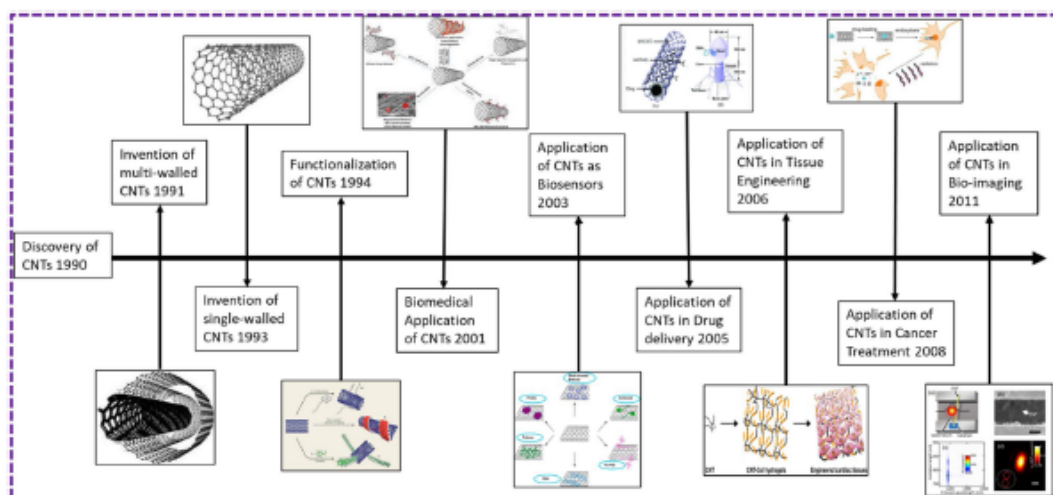
اندازه‌گیری‌های مداوم انتشار کربن نظیر دی‌اکسید کربن صنعتی با استفاده از ابزارهای رایج و متنوع توسط دستگاه‌های کوچک قابل حمل، به سهولت در دسترس است. برای اندازه‌گیری‌های جوی بسیار دقیق، از آشکارسازهای لیزری پالسی (رادار جذب دیفرانسیل ناشی از لیزر یا LIDAR<sup>۸</sup>) استفاده می‌شود که در طول موج‌های کمی بیش از ۲ میکرومتر عمل می‌کنند. همچنین برای نظارت بر غلظت دی‌اکسید کربن در جو، شبکه‌ی مشاهده ستون کربن کل (TCCON)<sup>۹</sup> در سال ۲۰۰۴ تشکیل شد. TCCON یک شبکه‌ی جهانی از ایستگاه‌ها است که مقادیر دی‌اکسید کربن، مونو اکسید کربن، متان، اکسید نیتروژن و سایر گازهای کمیاب

<sup>۸</sup>LIDAR: Laser Induced Differential Absorption Radar

<sup>۹</sup>TCCON: Total Carbon column Observing Network



شکل ۵: سهم بازار جهانی نانوتیوپ کربن بر اساس کاربرد در سال ۲۰۲۰؛ به ترتیب: پلاستیک و کامپوزیت، الکترونیک و انرژی



شکل ۶: تایم لاین نانوتیوپ کربن و کاربردهای زیست پزشکی



موجود در جو را اندازه گیری می کند. برای این شبکه تا سال ۲۰۱۵ میلادی، ۲۳ ایستگاه نظارتی در سراسر جهان احداث شد. هدف TCCON بررسی جریان (شار) کربن بین جو، زمین و اقیانوس (به اصطلاح بودجهی کربن یا چرخه ی کربن) است. این هدف با اندازه گیری جرم اتمسفر کربن (کسری در هوا) به دست می آید.

### ۱.۲.۳ تلاش ناسا برای اندازه گیری دی اکسید کربن

ادعا شده که اندازه گیری های فضایی دی اکسید کربن، در پاسخ به سؤالات مربوط به چرخه ی کربن کره ی زمین کمک می کند. اولین مأموریت ماهواره ای مانیتور تداخل سنجی برای گازهای گلخانه ای<sup>۱۰</sup> توسط ماهواره ی ADEOS I در سال ۱۹۹۶ انجام شد که کمتر از یک سال به طول انجامید. از آن زمان، اندازه گیری های فضایی اضافی، از جمله اندازه گیری های دو ماهواره با دقت بالا (بهتر از ۰/۳ درصد یا دقت 1ppm) انجام شده است.

دو دهه تلاش ناسا در LIDAR و توسعه ی «فرستنده ی دو میکرونی» منجر به قابلیت جدیدی برای اندازه گیری از راه دور سطح دی اکسید کربن شد (ناسا، ۲۰۲۰ و بلا لیپتیک، ۲۰۱۹).

### ۳.۳ چرا کنترل جهانی کربن؟

تمام آنچه تاکنون در پژوهش حاضر بیان گردید، صرفاً بدین منظور است که مشخص شود:

۱. کربن و انواع مشتقات آن در حوزه های مختلف، از سطوح فردی تا اجتماعی و از سطوح فنی تا راهبردی حائز اهمیت بی بدیل است.

۲. برخی کشورها نظیر آمریکا در تلاش هستند از طریق دستیابی به روش های عملیاتی و تکنولوژی های لازم، میزان کربن آزاد شده را اندازه گیری کنند که معادل میزان کربن مصرف شده است. یعنی هر چقدر در یک کشور، آثار جوی کربن بیشتر مشاهده شود؛ آن کشور استفاده ی بیشتری از این عنصر به عنوان ماده ی اصلی موجود در ترکیبات مادر مورد نیاز در زیرساخت ها و احتمالاً دیگر مواد کربنی با کاربردهای خاص تر را دارد. پس در نتیجه از صنایع و جامعه ی به روز تر و پیشرفته تری برخوردار است، زیرا بسیاری از حوزه های امروزی مصارف کربن نظیر گرافن، نانو لوله ی کربنی و ... نه به سادگی تولید می شوند و نه به سادگی مصرف می گردند.

حال پرسش مهم این است که:

۱. آیا احتمال دارد سنجش های مداوم جهانی میزان مصرف کربن و توسعه ی تکنولوژی اندازه گیری گازها، فقط به منظور کنترل مصرف کربن باشد؟

۲. در این صورت آیا به تبع کنترل میزان مصرف کربن، کشورها در حوزه های مختلف از علوم آزمایشگاهی گرفته تا تجهیزات و تسلیحات نظامی، صنایع مادر، پزشکی و ... کشف، شناسایی و کنترل نمی شوند؟

<sup>10</sup>IMG: Interferometric Monitor for Greenhouse Gases

۳.۳. اساساً کنترل فوق چگونه امکان تحقق دارد و اگر توسعه یابد، چه فضایی را در جهان رقم می‌زند؟

### ۱.۳.۳ سایبرنتیک، دانش کنترل

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»<sup>۱۱</sup> واژه‌ی سایبرنتیک را به کار برد.

وینر در خصوص انتخاب واژه‌ی سایبرنتیک چنین بیان می‌دارد: «تا دوران اخیر، واژه‌ای که مبین این گروه از افکار [منظور، کنترل پدیده‌ها 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 به معنای سکاندار و از منشأ انگلیسی Governor انتخاب کردم» (وینر، ۱۳۶۶، ص ۱). 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 غیرزیستی. از تلفیق و ضرب ماتریسی گزاره‌های فوق، چنان نتیجه می‌شود که سایبرنتیک، کنترل تمام جامعه را مدنظر قرار داده است. لذا در یک جمله می‌توان سایبرنتیک را دانش کنترل تمامی پدیده‌ها 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.

### ۲.۳.۳ نسبت‌شناسی دانش سایبرنتیک و انقلاب‌های صنعتی

مفهوم انقلاب صنعتی<sup>۱۲</sup> اشاره به رخدادهایی دارد که در قرن هجدهم آغاز شد و عموماً به جنبه‌های فنی تحولات بزرگی نظیر احداث پل آهنی در ۱۷۷۹، احداث اولین خط آهن عمومی در بریتانیا در ۱۸۲۵، اختراع کوره‌ی آهن در ۱۸۵۶ و حفر اولین چاه نفت در ۱۸۵۹ میلادی اشاره دارد که از مهم‌ترین نقاط انقلاب صنعتی هستند (دانشنامه‌ی رشد، انقلاب صنعتی). مبتنی بر روایت تاریخی، اکثر رخدادها و اختراعات مهم انقلاب صنعتی، ابتدا در بریتانیا بوده و سپس به سایر بخش‌های اروپا و آمریکای شمالی انتقال یافته است.

اما این روند متوقف نشد و با ماهیتی نوین و به شکلی متفاوت ادامه یافت. لذا این نتیجه برای دانشمندان حاصل شد که دوره‌ی زمانی ۱۷۵۰ تا حدود ۱۸۵۰ میلادی را به‌دلیل وقوع رخدادها، ابداعات و اختراعاتی که ذات مشابه داشته و آغاز راه انقلاب صنعتی بوده‌اند را به‌عنوان اولین مرحله از انقلاب صنعتی دسته‌بندی نمایند. به‌طور کل، شاخصه‌ی نوآوری‌های نخستین انقلاب صنعتی، جایگزینی ماشین‌های مکانیکی با انسان

<sup>11</sup>Cybernetics: Or Control and Communication in the Animal and the Machine

<sup>12</sup>Industrial Revolution

و حیوان در کاربردهای مختلف مانند کشاورزی، حمل و نقل، تولید و استخراج معادن است (ویجایا کایاستا، ۲۰۱۹).

در ادامه از حدود سال ۱۸۵۰ میلادی تا حدود ۱۹۳۰ میلادی، **انقلاب صنعتی دوم** شکل گرفت که هر چند بر پایه‌ی دستاوردهای انقلاب صنعتی یکم است اما ماهیتی متفاوت دارد. انقلاب صنعتی دوم که به انقلاب الکتریسیته نیز شهرت دارد، مقطعی است که ظهور و بروز تکنولوژی‌های مبتنی بر الکتریسیته را در بر دارد. مشاهیری مانند توماس ادیسون<sup>۱۳</sup> و نیکولا تسلا<sup>۱۴</sup> و دستاوردهایی نظیر انرژی الکتریسیته، تلفن، هواپیما و خودرو از اهم تاریخ انقلاب صنعتی دوم هستند.

در ادامه‌ی توسعه‌ی ارتباطات راه‌دور بر بستر الکتریسیته، **سومین انقلاب صنعتی** که کانون بسط آن عموماً ایالات متحده‌ی آمریکا است، بر اساس بر تکنولوژی‌های اطلاعاتی شکل گرفت و فضایی را پدید آورد که شاید بهترین تعبیر برای آن «صنعت متکی بر کامپیوتر و خودکارسازی» باشد. همچنین در کنار آن، تلاش برای دستیابی به انرژی‌های پایدار و جایگزینی با انرژی‌های فسیلی نیز آغاز شده است. انقلاب صنعتی سوم، با آغاز پایه‌گذاری دانش سایبرنتیک و طرح مسأله‌ی ماشین هوشمند و نظریه‌ی اطلاعات مقارن است. به عبارت دیگر، انقلاب صنعتی سوم، دوره‌ی طلوع سایبرنتیک و تکنولوژی‌های اولیه‌ی متأثر از این دانش است که به نوبه‌ی خود، عموم بخش‌ها از صنعت عمومی گرفته تا تسلیحات نظامی را با تحول جدی مواجه ساخت. از مهم‌ترین رخدادهای انقلاب صنعتی سوم، ابداع شبکه‌های کامپیوتری و عملیاتی‌سازی ورود کامپیوترهای نسل یکم تا چهارم به حوزه‌های مختلف حاکمیتی اعم از امنیت و دفاع، اجتماع، فرهنگ، سیاست و اقتصاد است.

اما **انقلاب صنعتی چهارم** که به نحوی امتداد انقلاب صنعتی سوم بوده و زمانه‌ی حاضر را شامل می‌شود، حاصل همه‌گیری مهندسی کامپیوتر پیشرفته و هوشمند می‌باشد که ظرفیت پیاده‌سازی تمام و کمال دانش سایبرنتیک را دارا است. اکنون که سیستم‌های دیجیتال کاملاً گسترده شده و توسعه یافته است، اینترنت به یکی از عادی‌ترین، اجتماعی‌شده‌ترین و زیرساختی‌ترین پدیده‌های بشری مبدل گشته و از نسل‌های جدید ارتباطی مانند 5G و 6G گرفته تا زیرساخت‌های ارتباطی همه‌جا حاضر مانند اینترنت اشیا<sup>۱۵</sup> رونمایی و بهره‌برداری شده است؛ انقلاب صنعتی چهارم آماده است تا بر اساس دانش سایبرنتیک و سیستم‌های سایبر فیزیکی<sup>۱۶</sup>، دنیای جدیدی را تعریف و مستقر نماید.

از این رو دانش سایبرنتیک، اولاً متولی دو انقلاب از چهار انقلاب صنعتی است (مخصوصاً انقلاب‌های صنعتی سوم و چهارم) و ثانیاً مبنای انقلاب صنعتی چهارم است زیرا از عمق مفاهیم فلسفی، دیدگاه‌های نظری و روش‌های عملیاتی و تکنولوژیک برخاسته است.

<sup>13</sup>Thomas Edison

<sup>14</sup>Nikola Tesla

<sup>15</sup>IoT: Internet of Things

<sup>16</sup>Cyber Physical Systems

### ۳.۳.۳ بازنگری انقلاب‌های صنعتی از منظر اعمال توان کنترل

بررسی انقلاب‌های صنعتی از منظر عملیاتی‌سازی توان کنترل چنین می‌نمایاند که اولاً بشر در هر دوره از انقلاب‌های صنعتی به توان کنترلی جدیدی دست یافته که سابق بر آن در اختیار نداشته است. بر این اساس در دوره‌ی انقلاب صنعتی یکم، بشر از طریق دانش‌هایی نظیر فیزیک، مکانیک و مباحثی مانند ترمودینامیک و ... دریافت که می‌توان از تبدیل انرژی‌ها به انرژی مکانیکی، توان حرکتی بسیار بیشتر از آنچه حیوانات ارائه می‌کنند را به دست آورد. در نتیجه تقریباً تمامی شئون زندگی انسانی از سطح فردی گرفته تا ملی و فراتر از آن، تحت تأثیر این یافته و خروجی‌های حاصل از آن قرار گرفت. در نتیجه بشر موفق شد مواردی را کنترل نماید که تا پیش از آن یا در سلطه نداشته یا به صورت جامع و کامل نبوده است. برای نمونه سفرهای منظم از طریق خطوط ریلی با توان جابجایی و ترابری انبوه، عظیم و طولانی مدت؛ از جمله مواردی است که به واسطه‌ی دریافت انرژی از ماشین بخار و سوزاندن زغال سنگ حاصل شده است. پس به دنبال آن، ورود به سایر مناطق و تلاش برای تسلط بر آنها و سپس انتقال منابع آنها به سرزمین‌های غربی در دستور کار قرار گرفت. بنابر این به طور خلاصه، دستاورد انقلاب صنعتی یکم برای بشر غربی، افزایش چشمگیر توان کنترل بر ابعاد فیزیکی زمین و دیگر ملت‌ها است.

انقلاب صنعتی دوم، ضمن حفظ دستاوردهای انقلاب صنعتی یکم؛ با ارائه‌ی انرژی الکتریسیته و وسایل مبتنی بر آن، قابلیت کنترل با سرعت بالاتر، دقت بیشتر، هزینه‌ی کمتر و مساحت گسترده‌تر را به بشر عرضه کرد. در نتیجه ضمن بروزرسانی ابزارهای مکانیکی به الکتریکی، ابزارهای جدیدی نیز ارائه نمود که امکان پیاده‌سازی آنها از طریق زیرساخت تماماً مکانیکی انقلاب صنعتی یکم میسر نبود. از مهم‌ترین نقاط تولید قدرت کنترل در دوره‌ی انقلاب صنعتی دوم، امکان ارتباطات راه دور به واسطه‌ی تلگراف و تلفن است. پس اکنون بشر می‌تواند در چند دقیقه، فرمان خود را از سویی به سوی دیگر زمین ارسال نماید تا بلافاصله اعمال گردد. این یعنی تحولی بی‌بدیل در عرصه‌ی عملیاتی‌سازی فرماندهی و کنترل.

اما انقلاب صنعتی سوم، پا را از ارتباطات فراتر گذاشت و مسأله‌ی محاسبات را مطرح ساخت. اکنون بشر نیاز داشت با همان سرعت و ظرفیتی که فرمان خود را ارائه می‌کند، محاسبات اطلاعاتی را انجام دهد تا اولاً دریابد چینه‌ی محیطی که داده‌ها توصیف‌گر آن هستند چگونه است و ثانیاً چه تصمیمی اخذ و چه فرمانی صادر کند که شرایط را به سمت وضعیت مطلوب خودش سوق دهد؟ همچنین بشر نیازمند بود تا امور معمول محاسباتی را از خود دور نموده و به ابزارها بسپارد تا بتواند صرفاً بر حوزه‌های کلان و راهبردی تمرکز کند. تمام نیازمندی‌های فوق در مفهوم کامپیوتر گنجانده شد و تدریجاً برای تحقق آن تلاش گردید. از این رو قلب تپنده‌ی انقلاب صنعتی سوم، انقلاب در عرصه‌ی محاسبات است؛ چه از منظر روش‌ها و الگوریتم‌های آن، چه از حیث ابزار و وسایل اجرای محاسبات.

حال بشر، توان جابجایی سریع، انتقال سریع اطلاعات و محاسبه و ذخیره‌سازی آن را به دست آورده است و کم‌کم دریافته که شاکله‌ی اصلی کنترل «اطلاعات» است. اما اگر این مهم را بپذیرد - که پذیرفته است - یعنی هم‌زمان باید بپذیرد که هر پدیده‌ی غیراطلاعاتی، از دامنه‌ی کنترلی وی خارج است. به تعبیر دیگر، اگر پدیده‌ای از اطلاعات اثر نپذیرد، آنگاه کنترل نیز نخواهد شد، مگر با همان روش‌های سابق فیزیکی و مکانیکی

که سخت‌تر، محدود، زمان‌بر، هزینه‌بر و غیر دقیق بوده و سنخیتی با فضای کلان کنترل که به واسطه‌ی انقلاب صنعتی سوم پدید آمده است، ندارند. از سوی دیگر، بشر دریافته بود که هرچند توان ادراک اطلاعات یا همان هوشمندی، ابتدا به ساکن طبیعی است، اما ظاهراً می‌توان آن را در بعضی پدیده‌های غیرهوشمند نیز شبیه‌سازی کرد. بدین معنا که درجاتی از هوشمندی مصنوعی در پدیده‌های غیر هوشمند ایجاد گردد تا بتواند تحت تأثیر جریان اطلاعات، کنترل شود؛ و این یافته، سرآغاز انقلاب صنعتی چهارم گردید.

کلاوس شواب در خصوص ویژگی‌های منحصر به فرد انقلاب صنعتی چهارم و تفاوت‌های ماهوی آن با سه انقلاب صنعتی پیش از خود چنین بیان می‌دارد: «به اعتقاد من، سه دلیل وجود دارد که انقلاب صنعتی چهارم، متمایزاً در حال انجام است:

۱. سرعت. برخلاف انقلاب‌های صنعتی قبلی که سرعت تکوین آنها خطی است، این انقلاب دارای سرعت تصاعدی است و حاصل آن جهان چند وجهی و عمیقاً مرتبط است که ما در آن جهان با این واقعیت زندگی می‌کنیم که تکنولوژی‌های جدید، هر روز بهتر و حتی با امکانات بیشتر می‌شوند.

۲. دامنه و عمق. انقلاب صنعتی چهارم در بستر ترکیبی از تکنولوژی‌های چندگانه و انقلاب دیجیتال در دوره‌ی انتقالی پارادایم بی‌سابقه در اقتصاد، کسب و کار، اجتماع و افراد جاری است. این انقلاب نه تنها «چه»<sup>۱۷</sup> را و «چگونه»<sup>۱۸</sup> را، بلکه مفهوم «چه کسی هستیم»<sup>۱۹</sup> را نیز تغییر می‌دهد.

۳. تبعات سیستم. انقلاب صنعتی چهارم شامل گذار از کل سیستم‌ها، در کلیه‌ی کشورها، شرکت‌ها، صنایع و جامعه به‌عنوان یک مجموعه [یکپارچه] است... تأکید من بر شیوه‌های ناظر بر همزیستی تکنولوژی و بقاء جامعه است؛ زیرا تکنولوژی یک نیروی برون‌زادی نیست که ما کنترلی بر آن نداشته باشیم» (کلاوس شواب، ۱۳۹۸، صص ۱۵-۱۶).

آنچه شواب مطرح کرده، مؤید تفسیری است که نسبت به انقلاب صنعتی چهارم بیان شد. چرا سرعت بیشتر؟ چون اطلاعات مشمول محدودیت‌های مادی و فیزیکی نیست. چرا دامنه و عمق فراتر؟ زیرا بشر منطبق با فهم خود تصمیم‌گیری و اقدام می‌کند و اطلاعات، کانون اصلی شکل‌گیری فهم بشر نسبت به هر موضوعی است. پس انقلاب صنعتی چهارم به عمیق‌ترین لایه‌ی شناخته از انسان توجه دارد. چرا تبعات سیستمی؟ چون جریان اطلاعات، منطبق با ساز و کار و منطق سیستم‌های سایبرنتیکی ایجاد و کنترل می‌شود که ریشه در نظریه‌ی سیستم‌ها دارد. در نتیجه تمامی پدیده‌های زیستی و غیرزیستی محیط را به مثابه اجزایی در نظر می‌گیرد که در نسبت با یک کل (مجموعه) بر اساس روابط معنادار به یکدیگر مرتبط شده‌اند و به محیط خود، خدمات ارائه می‌کنند. لذا کنترل از منظر نگاه سیستمی معنا می‌یابد، نه موردی و تفکیک شده. در یک نگاه، هر انقلاب صنعتی توانسته عمق و گستره‌ی کنترل بشر در سطح جهان را افزایش دهد. با این اوصاف پرسش مهم این است که آیا کربن می‌تواند یک متغیر کنترلی برای کنترل جهان باشد؟

<sup>17</sup>What

<sup>18</sup>How

<sup>19</sup>Who

### ۴.۳.۳ کنترل کربن و انقلاب صنعتی پنجم

اهمیت روزافزون کربن در حوزه‌های مختلف و همچنین تحولات عظیم و بی‌بدیلی که مشتقات نوین آن رقم زده‌اند؛ این ظرفیت را برای کربن ایجاد نموده‌اند که بتوان آن را مؤلفه و مبنای یک انقلاب صنعتی جدید دانست. به عبارت دیگر امروزه کربن، چنان جایگاه بی‌بدیلی یافته که با هیچ چیز دیگر قابل جبران نیست، نظیر نقش بی‌بدیلی که ماشین بخار در انقلاب صنعتی یکم، الکتروسیته در انقلاب صنعتی دوم، کامپیوتر در انقلاب صنعتی سوم و هوش مصنوعی در انقلاب صنعتی چهارم دارند. از این رو می‌توان کربن را مبنای انقلاب صنعتی پنجم دانست.

همچنین در چند سال اخیر، بخش مهمی از تمرکز پژوهشی در جهان به موضوع ترسیب کربن<sup>۲۰</sup> اختصاص یافته است. ترسیب کربن به معنای دریافت کربن موجود در هوا به وسیله‌ی جذب در خاک و گیاهان است. اما از سوی دیگر، ادبیات علمی این حوزه در سال‌های اخیر به سمت وضع «استاندارد کم کربن» یا «استاندارد کربن صفر» میل پیدا کرده است. منظور از استاندارد کم کربن، عدم تولید کربن در فرایندهای مختلف اجتماعی، حاکمیتی، صنعتی، نظامی، پزشکی و ... است.

این موضوع تا آنجا مهم انگاشته شد که حتی برخی معاهدات بین‌المللی مانند معاهده‌ی اقلیمی پاریس با توجه ویژه به عدم تولید و انتشار کربن تدوین شده است؛ به گونه‌ای که کشورهای عضو معاهده، متعهد شده‌اند از طریق برنامه‌ی مشارکت ملی<sup>۲۱</sup> میزان انتشار مشتقات کربن نظیر دی‌اکسید کربن را کاهش دهند.

تحلیل‌گران بسیاری به این مهم دست یافتند که معاهده‌ی پاریس در واقع بستری است برای کنترل رشد اقتصادی کشورها، کنترل فضای زیست‌محیطی آنها طبق پروتکل‌های اعلامی، نظارت بر نوع و گستره‌ی صنایع کشورها از طریق سنجش آلاینده‌های کربنی تولید شده و سایر موارد. اما نسل جدید مشتقات بسیار مهم و راهبردی کربن - که در همین پژوهش اجمالاً معرفی شدند - از یک سو و تشدید استاندارد کم کربن از سوی دیگر حاکی از آن است که سطح کنترل به واسطه‌ی کربن بر کشورها در حال افزایش است.

آنچه باعث می‌شود که نتوان باور کرد هدف اصلی استاندارد کربن و نظارت‌های اینچنینی، محیط‌زیست جهانی است، آمارهایی است که نشان می‌دهد آمریکای شمالی و اروپای غربی دائماً در حال افزایش تولید مشتقات کربنی و توسعه‌ی صنایعی هستند که کربن تولید می‌کند؛ در حالی که عمل به مفاد معاهده‌ی پاریس را به دیگر کشورها تذکر می‌دهند.

در عین حال محرز است که یکی از عناصر اصلی که در بطن هر چهار انقلاب صنعتی یکم تا چهارم نقش دارد، کربن است. از این رو کنترل کربن، به معنای ممانعت از پیشرفت کشورها در مسیر چهار انقلاب صنعتی سابق است.

با این اوصاف اگر انقلاب صنعتی پنجم را یک انقلاب صنعتی مبتنی بر کربن بدانیم؛ بدین معنا خواهد بود که کشورهای پیشرو از سویی در تلاش برای رسیدن به جدیدترین کاربردهای کربن در حوزه‌های مختلف دانش و تکنولوژی هستند و از سوی دیگر، به بهانه‌ی مسائل زیست‌محیطی مانع از رشد و پیشرفت سایر کشورها

<sup>20</sup>Carbon Sequestration

<sup>21</sup>NDC: Nationally Determined Contribution



شده و از طریق پروتکل‌هایی که در استاندارد کربن وضع شده و معاهدات حقوقی بین‌المللی، تلاش می‌کنند تا این خواست خود را به سایر کشورها تحمیل نمایند.

## ۴ نتیجه‌گیری

سرعت رشد تحولات صنعتی کربن‌پایه در عصر حال و آینده و تکنولوژی‌های پیشرفته‌ی وابسته به کربن و مشتقات آن به قدری فزاینده و جایگاه کاربردهای راهبردی آن به قدری مسلم است که کنترل دانش‌ها و تکنولوژی‌های کربن‌پایه، بیش از آنکه به حفظ محیط‌زیست منجر شود، به حذف رقبا بین‌المللی خواهد انجامید. یکی از مصادیق این ادعا، به‌کارگیری تحلیل‌کننده‌ها و تجهیزات کنترلی بسیار پیشرفته و دقیق در حد تشخیص غلظت یک در میلیون<sup>۲۲</sup> و ایجاد پایگاه‌های متعدد در سراسر دنیا و خارج از جو برای ترکیبی است که هرچند تجمع و انتشار بالای هزاران تن از آن تغییرات زیست‌محیطی را ایجاد نموده است (به فرض صحت ادعا) اما در مقیاس کم، سمی و خطرناک نیست. به‌عبارت دیگر این حد از دقت برای تشخیص آلاینده‌های کربنی به‌منظور حفاظت از محیط‌زیست، توجیه علمی و فنی ندارد و کاملاً شبیه به رصد هرگونه فعالیت کربن‌پایه از حیث کیفی و کمی است.

این در حالی است که جامعه‌ی جهانی، نظیر چنین اقداماتی را در دهه‌های گذشته که ایام توسعه‌ی تکنولوژی‌ها و زیرساخت‌های هسته‌ای بوده، به بهانه‌ی تلاش برای شناسایی و کنترل نشت مواد خطرناک رادیواکتیو یا فعالیت‌های نامتعارف در کشورهای مختلف انجام داده است اما بعداً مشخص گردید که تماماً به نیت ممانعت از رسیدن کشورها به توان هسته‌ای است.

دومین شاهد این ادعا، سهم یک درصدی کشورهای متعهد و تحت کنترل از انتشار گازهای گلخانه‌ای در جهان به ادعای IEA<sup>۲۳</sup> است. با توجه به آمارهای ارائه شده در پژوهش حاضر مشخص می‌شود کنترل کربن برای کشور ایران که در حال دستیابی به تکنولوژی‌هایی مانند تولید گرافن و به‌کارگیری آنها در مقیاس بالاتر از آزمایشگاهی در صنایعی چون الکترونیک، فضایی، خودروسازی، دفاعی و ... است؛ در نقش واگذاری اطلاعات حساس در حوزه‌ی روند دستیابی، میزان توسعه و گستره‌ی مصرف کربن کشور به پایگاه‌های بین‌المللی جمع‌آوری داده‌های کربن است.

از سوی دیگر به دلیل استفاده‌ی صنایع مادر و پشتیبان کشور مانند برق، پتروشیمی، فولاد، سیمان و ... از سوخت‌های فسیلی و محدودیت جایگزینی آن با انواع دیگر انرژی به‌دلیل سایر تعهدات بین‌المللی (مثلاً عدم استفاده‌ی گسترده از انرژی هسته‌ای برای تأمین نیرو به‌دلیل معاهده‌ی برجام) کشور را از پیشرفت زیرساختی، تکنولوژیک و صنایع نوین باز خواهد داشت.

## مراجع

[۱] بیل گیتس، «چگونه از فاجعه اقلیمی جلوگیری کنیم؟»، مترجم: محسن صالحی اصیل، نشر گویا، تهران، ۱۴۰۰.

<sup>22</sup>PPM: Part Per Million

<sup>23</sup>IEA: International Energy Agency

- [۲] خبرگزاری ایمننا، «پروتکل مونترال و لزوم حفاظت از لایه ی ازن»، ۲۵/۶/۱۴۰۰، پیوند:  
<https://www.imna.ir/news/522179>
- [۳] اعظم محمدباقری و سعید اسفندیاری، «اقتصاد کم کربن و سیاست‌های کاهش انتشار گازهای گلخانه‌ای»، مجله اقتصاد انرژی، شماره‌های ۱۵۷ و ۱۵۸، خرداد و تیر ۱۳۹۲.
- [۴] صابر محمد پور و مهرداد مهرجو، «ارزیابی پایداری محله‌های شهری با رویکرد محله‌ی کم کربن»، مجله‌ی توسعه‌ی محلی؛ دوره‌ی دوازدهم، بهار و تابستان ۱۳۹۹.
- [۵] مهدی مجیدپور، «جذب و ذخیره‌سازی کربن، سیاست‌گذاری فناوری برای گذار به اقتصاد کم کربن»، سیاست‌نامه‌ی علم و فناوری، شماره ۲، بهار ۱۳۹۱.
- [۶] نوربرت وینر، «استفاده‌ی انسانی از انسان‌ها»، ترجمه‌ی مهرداد ارجمند، تهران، سازمان انتشارات و آموزش انقلاب اسلامی، ۱۳۶۶.
- [۷] محمد علی شکوهیان‌راد، «نظریه‌ی جنگ در عصر سیستم‌های فرماندهی و کنترل»، تهران، مؤسسه‌ی آموزشی و پژوهشی شهید صیاد شیرازی، ۱۳۹۷.
- [۸] دانشنامه‌ی رشد، سرفصل جامعه و علوم اجتماعی، بخش تاریخ، صفحه‌ی انقلاب صنعتی، پیوند:  
<http://daneshnameh.roshd.ir/mavara/mavara-index.php?page=&SSOReturnPage=Check&Rand=0>
- [۹] [۹] کلاوس شواب، «انقلاب صنعتی چهارم»، مترجم: مرتضی شانی، انتشارات شرکت چاپ و نشر بازرگانی، تهران، سال ۱۳۹۸.
- [10] Sustainable Development Goal indicators website, United Nation, “Take urgent action to combat climate change and its impacts,” Link: <https://unstats.un.org/sdgs/report/2021/goal-13/>.
- [11] Sustainable Development Goal indicators website, United Nation, “Take urgent action to combat climate change and its impacts,” Link: <https://unstats.un.org/sdgs/report/2021/goal-13/>.
- [12] Gabriela Ileana Iacobuță and Coworks, “Transitioning to Low-Carbon Economies under the 2030 Agenda: Minimizing Trade-Offs and Enhancing Co-Benefits of Climate-Change Action for the SDGs,” Sustainability Journal, 2021, Link: <https://doi.org/10.3390/su131910774>.
- [13] International Energy Agency, “Global Energy Review 2021, Coal,” Link: <https://www.iea.org/reports/global-energy-review-2021/coal>.
- [14] World Coal Association, “Coal & Electricity,” Link: <https://www.worldcoal.org/coal-facts/coal-electricity/>.
- [15] International Energy Agency, “Coal,” Link: <https://www.iea.org/fuels-and-technologies/coal>.
- [16] International Energy Agency, “Aluminum,” Link: <https://www.iea.org/fuels-and-technologies/aluminium>.
- [17] BP Statistical Review of World Energy 2022, 71st edition, Centre for Energy Economics Research and Policy, Heriot-Watt University, Link: <https://ceerp.hw.ac.uk>.

- [18] World Coal Association, "Coal Facts," Link: <https://www.worldcoal.org/coal-facts/>.
- [19] "Activated carbon market size, share & covid-19 impact analysis by type," 2022-2030, Market Research Report, Page 300, 2022, Report ID: FBI102175.
- [20] "Industrial carbon and graphite materials," volume I: raw materials, production and applications, I chapter 6-5-3, graphite electrodes for electric arc furnaces. Daniel Steppich 2021, John Wiley and Sons.
- [21] "Graphite market size, share & covid-19 impact analysis by product (synthetic and natural)," by application, 2021-2028, Market Research Report, Page 110, 2021, Report ID: FBI105322.
- [22] Belal G. Nassef, Galal A. Nassef, "Graphene and its industrial applications-A review," International journal of Materials Engineering, 2020, 10 (1):1-12.
- [23] Wonbong Choi, Inderanil lahiri, "Synthesis of graphene and its applications: A review," Critical Review in Solid State and Materials Science 2010, 35: 52-71.
- [24] "Industry Overview," Global Market Insights, Link: <https://www.gminsights.com/industry-analysis/graphene-market>.
- [25] "Graphene market size, share & covid-19 analysis by product (Graphene oxide (GO), Graphene nanoplatelets (GNP), others)," by end-use, 2021-2028, Market Research Report, Page 80, 2022, Report ID: FBI102930.
- [26] "Carbon nanotubes (CNT) Market size, Share & covid 19 impact analysis," by product (Multi walled carbon nanotubes (MWCNT), 2021-2028, Market research report, 2021, Page 200, Report ID: FBI102700.
- [27] Bhushan Murjani, Parikshit S. Kadu, "Carbon nanotubes in biomedical applications: current status, promises, and challenges," Carbon Letters, 2022. Link: <https://doi.org/10.1007/s42823-022-00364-4>.
- [28] Statista, "Distribution of carbon fiber consumption worldwide in 2020 by end-use market," Link: <https://www.statista.com/statistics/702145/global-carbon-fiber-consumption-share-by-end-use-market/>.
- [29] NASA, "Advanced earth observing satellite," Link: <https://eosposo.nasa.gov/missions/advanced-earth-observing-satellite>.
- [30] Bela Liptake, "Measuring Atmospheric Carbon Dioxide," 2019, Link: [www.ControlGlobal.com](http://www.ControlGlobal.com).
- [31] Dr. Vijaya Kayastha, "Role of Materials in Performance of Printed Temperature Sensors," Brewer Science, June 2019, Link: [https://www.brewerscience.com/wp-content/uploads/2019/07/2019\\_Sensors\\_Expo\\_Brewer\\_Science.pdf](https://www.brewerscience.com/wp-content/uploads/2019/07/2019_Sensors_Expo_Brewer_Science.pdf).



## بررسی گلوگاه سایبری در ورود به گام دوم انقلاب

مجتبی شیخی ده‌آبادی<sup>۱</sup>، ابوالفضل امامی میبیدی<sup>۲</sup>

<sup>۱</sup> دانش‌آموخته حوزه و دکترای علوم اقتصادی (پژوهشگر ابرفقه و نظام اقتصاد)  
msheikhy97@chmail.ir

<sup>۲</sup> دانش‌آموخته حوزه و دکترای فقه سیاسی و روابط بین‌الملل (کاشف ابرفقه)  
abolfazlemami@chmail.ir

### چکیده

سامانه سایبری «پیشرفته» اسلام، پنج لایه دارد: «عقل، فکر، قلب، حس و عضو». پیوند میان این لایه‌ها، امام - مأمومی است. این نوشتار، با نگاهی فشرده به سامانه سایبری پیشرفته (ابر فقه)، با روش فقهی و با کمک دو خوانشگر، می‌کوشد تا گلوگاه حیاتی نظام سایبری کنونی را نشان دهد. سامانه کنونی ما، «پیش‌نظام» و برپایه دو رکن امام و امت است. برای نیرومندسازی پیش‌نظام و رسیدن به «نظام پیشرفته» (امام، لایه‌های سه‌گانه میانی و مردم) در گام دوم انقلاب، باید از گلوگاه سایبری کنونی (پیوند میان امام و مأموم) پاسداری کرد؛ زیرا سامان‌واره سایبری گلوبالی، با سرسختی در پی نشانیدن اولیای طاغوت به جای «ائم» و ابتر کردن امتداد «امام» در سامانه است. از این رو آسیب‌شناسی سایبری انقلاب اسلامی و نیرومندی «حلقه‌های وصل» در میان امام و امت، اولویت برجسته‌ی ورود به گام دوم انقلاب است. در این نوشتار به فراخور کشف یک گستره‌ی دانشی، ناگزیر به برخی واژه‌سازی‌ها پرداخته‌ایم.

**کلمات کلیدی:** گلوگاه سایبری، نظام اسلام، دانش سایبری، ابرفقه، فضای سایبر، اهداف توسعه پایا، گلوبالیزم، نرم‌افزار حکمرانی.

## ۱ مقدمه

برای گذر از گام نخست انقلاب و رسیدن به گام دوم انقلاب (نظام پیشرفته)، دو آسیب بزرگ در ساماندهی جامعه و حکمرانی سایبری در انقلاب اسلامی هست؛ یکی «نبود سامانه سایبری پیشرفته» که به سخن رهبر انقلاب اسلامی، کارآمدی سامانه تراز را به هیچ کاهش می‌دهد<sup>۱</sup> و دیگری «کاستی در گلوگاه پیش‌نظام کنونی» است که می‌تواند به نابودی همین نظام کنونی (پیش‌نظام) بینجامد.

در این نوشتار به آسیب گلوگاه سایبری در پیش‌نظام کنونی می‌پردازیم. رکن «حیات‌بخشی» در دانش

<sup>۱</sup> «حکومت اسلامی... اگر نرم‌افزار مناسب خودش را نداشته باشد، به هیچ کار نمی‌خورد.» [۲]، بیانات در تاریخ ۴ اسفند

سایبری اسلام، آن است که «حیات» لایه بالایی سامانه، به لایه زیرین برسد<sup>۲</sup>، این کار وابسته به «امام بودن» لایه بالایی (العقول أئمة الأفكار). و مأمومیت کردن لایه زیرین است که آن را «ایتمام» می‌نامیم<sup>۳</sup>. در «پیش‌نظام»، سامانه با دو لایه اصلی «امام و امت» روبرو است که به درستی جایابی و پیوند یافته‌اند؛ ولی در حلقه میانی (حلقه وصل) دچار گسیخت و کاستی است. از این رو، دشمن از سامانه پیچیده‌ای برای رخنه در لایه میانی بهره می‌برد و پیش‌نظام کنونی انقلاب نیز از همین آشفتگی حلقه میانی و نیرومندی رخنه‌گری دشمن در لایه‌های میانی، دچار آسیب‌های بسیاری است که در سخن رهبر نیز نمودار است: «هدف این است که توده‌های مردم مورد اغوا قرار بگیرند اما وسیله اغوای توده‌های مردم، اغوای خواص است ... وقتی خواص، اغوا شدند، ... راحت توده مردم را اغوا خواهند کرد»<sup>۴</sup>.

این آسیب‌ها می‌تواند به گسست در رکن «حیات‌بخشی» و نابودی نظام بینجامد! ولی دانش سایبری اسلام، پیشنهاد روشن و نیرومندی برای به‌هم‌بستن این «گسل» و توان گذر از این باتلاق را دارد. پشتیبان ما برای پوشاندن گسل‌ها و رخنه‌های سایبری، «فقه» است؛ فقه، پوشاننده رخنه‌ها و کاستی شناخت ما با کمک خدا و ولی خدا است تا بتوان به نیازهای شناختی سامانه برای «بود» و «بهبود» دست یافت. فکر ما در برابر همه گزاره‌ها توان دآوری و چاره‌سازی ندارد؛<sup>۵</sup> پس گزاره‌ها بر دو بخش «گزیرا» و «ناگزیرا» هستند و گزاره‌هایی را که برای فکر ما ناگزیرا هستند، باید از دانایان برگزید. اگر نتوانیم این گزاره‌ها را از دانایان برگزینیم، دچار تقلید جاهل از جاهل شده‌ایم که کاری ناسازگار با سرشت شناختی بشر است. از این رو، بزرگترین رخنه سایبری، «جا» زنی نادان‌ها به جای دانایان و جازنی گزاره‌های نادرست به جای گزاره‌های درست است. یکی از کارکردهای دین، به دست دادن نیازهای شناختی زیست انسان است. دین با کمک دو دسته «فقه»، نیازهای شناختی ما را برآورده می‌کند، فقه الهی (اطیعوا الله) و فقه ولایی (اطیعوا الرسول و اولی الامر منکم). «فقه الهی»، قضایای حقیقیه و نیازهای شناختی پایداری است که در حوزه احکام علمی (مانند دانش کلام نقلی) و در حوزه احکام عملی به ما می‌رسد. و «فقه ولایی»، نیازهای شناختی ناپایداری است که به پیوندهای میان انسان و دیگر عناصر پیچیده سامانه می‌پردازد و با نام «حکم حکومتی» شناخته می‌شود.

بررسی‌های ما نشان می‌دهد که کشف یک سامانه سایبری پیشرفته در فقه اسلام تاکنون انجام نشده

<sup>۲</sup> برای کارکرد پیشرفته سامانه، به پنج رکن نیاز است: آ. رکن «حیاتی» سامانه، برای زنده بودن آن؛ ب. رکن «حیات‌بخشی» به لایه‌های زیرین سامانه؛ ج. رکن «حیات‌بخشی» در همه لایه‌های سامانه؛ د. رکن «حیات‌سنجی»، برای شناخت توازن رشد و برخورداری درست هر لایه؛ ه. رکن «حیات‌ورزی» برای پیشرفت سامانه. بنگرید: [۱۰]، درس ۱۲ (ارکان کارکرد): ۱۱۲ تا ۱۲۰.

<sup>۳</sup> «یَقُولُونَ: إِمَامٌ، أَمَا وَاللَّهِ مَا أَنَا بِإِمَامٍ إِلَّا لِمَنْ أَطَاعَنِي، فَأَمَّا مَنْ عَصَانِي فَلَسْتُ لَهُ بِإِمَامٍ لِمَ يَتَعَلَّقُونَ بِاسْمِي». [۱۸]، ج ۱۵، ص ۸۲۰.

<sup>۴</sup> [۲]، بیانات رهبری در ۱۹ اسفند ۱۴۰۰ در نشست خبرگان. برخی از فرمایش‌های رهبری درباره لایه‌های میانی و حلقه وصل: «پیشرو بودن و ورود، یک حلقه وصلی لازم داشت، یک حلقه واسطی لازم داشت؛ این حلقه واسطی حوزه علمیه قم بود و البته حوزه‌های علمیه دیگر... نسبت حوزه قم با انقلاب این است.» [۲]، همان، ۲۵ اسفند ۱۳۹۴. «این تمرکز، این ایجاد برنامه کار، پیدا کردن راهکار، ارائه راهکار، برنامه‌ریزی ... به عهده جریانهای حلقه‌های میانی است... به عهده مجموعه‌هایی از خود ملت است ... ما نخبه‌های فکری در زمینه‌های گوناگون مورد نیاز، در میان جوانان [و] در میان مسئولین خودمان داریم.» [۲]، همان، ۱ خرداد ۱۳۹۸. «مطبوعات باید با تفرقه و از هم‌گسیختگی و از دست رفتن اعتماد به نفس و تضعیف روحیه ملی مقابله کنند و به هر آنچه که مایه ارتباط و حلقه وصل آحاد یک ملت است وفادار باشند.» [۲]، بخش اخبار، ۲۴ اردیبهشت ۱۳۷۳.

<sup>۵</sup> «وَمَا أَوْتِيتُمْ مِنَ الْعِلْمِ إِلَّا قَلِيلًا». [۱]، اسراء، ۸۵.



و برخی کارهای غیرفقهی یا شبهفقهی انجام شده، نمی‌تواند مبنا و الهام‌بخش کار فقهی در این مسئله ویژه باشد. آثاری چون «زبر تفقه نظام اسلام»، «زبر تفقه نظام پیشرفته دین» و «غرب‌شناسی فقهی با تمرکز با گلوبالیزم»، در راستای فقه سایبری اسلام و پشتوانه فقهی این مقاله است.

در ادامه، پس از بررسی فشرده دانش سایبری اسلام، به بررسی لایه فکر آن سامانه، با کمک دو خوانشگر می‌رسیم و سپس به تبیین گلوگاه سایبری کنونی و نوک پیکان نبرد سایبری گلوبالی با تمدن اسلام و نتیجه‌گیری می‌پردازیم.

## ۲ نگاهی فشرده به دانش سایبری اسلام

ریشه واژه «سایبرنتیک» به معنای ملوانی کشتی و حکمرانی با سامانه اطلاعات و ارتباطات است<sup>۶</sup>؛ و دانش سایبری پیشرفته اسلام با شناخت لایه‌های سامانه انسان و جامعه و پیوند درست میان آنها دارای یک الگوی ریاضی پیشرفته است که جلوی بی‌نظمی و بی‌نظامی و آسیب‌های گلوگاهی پیش‌نظام ما را می‌گیرد<sup>۷</sup>.

چنانکه دیدیم، ولی امر، حکومت را سخت‌افزاری می‌دانند که اگر نرم‌افزار درخور خود را نداشته باشد، به هیچ کار نمی‌خورد؛ پس کشف نرم‌افزار فرمان‌روایی (سایبری) برای رسیدن به «نظام پیشرفته»، ارزش حیاتی و تعیین‌کننده دارد. ما به «آن فقهی که ارزش حیاتی» دارد، «ابرفقه» می‌گوییم. ابرفقه، نشان‌دهنده سامانه تراز انسان، جامعه، جهان و دانش‌ها است که هسته بنیادین آن در فرمایش امیرالمؤمنین (ع) آمده است: «العقولُ أئمةُ الأفكارِ و الأفکارُ أئمةُ القلوبِ و القلوبُ أئمةُ الحواسِّ و الحواسُّ أئمةُ الأعضاء»<sup>۸</sup> عقل‌ها امامان فکرها هستند و فکرها امامان دل‌ها هستند و دل‌ها امامان حس‌ها هستند و حس‌ها امامان عضوها.

پس سامانه پیشرفته اسلام، پنج لایه دارد و میان لایه بالا و پایین، رابطه امام-مأمومی است. بُنمایه و ژرفای حیاتی سامانه، «عقل» نامیده می‌شود که به معنای «بند» است و «عقل» یعنی «بنده» و «تعقل» یعنی پیوند هر پنج لایه، برای انجام نیکی. این معنای حقیقی عقل، غیر از معنای مجازی «مُدِرک کلیات» و «قوه استدلال» است! این دو معنا، کار «فکر» است؛ نه عقل!<sup>۹</sup> عقل، اصول و سوگیری کلان را نشان می‌دهد و فکر از آنها، تفریح کرده، برنامه تفصیلی می‌سازد و آنگاه بر قلب، امامت می‌کند. فرق عقل و فکر، در اندازه فرق امام و مأموم است! گاه عقل کسی خوب است ولی در فکرش دچار استضعاف است! و گاه فکر کسی خوب است ولی عقلش خوبی‌ها را پی نمی‌گیرد. قلب به معنای دگرگونی است و با دگرگونی‌های پیاپی، حب و بغض و انگیزه را برای انجام برنامه فکر، فراهم می‌کند و با امامت بر لایه حس، انگیزه‌ها را به حس می‌رساند. حس به معنای دریافت‌های معنادار از بیرون و رساندن آن به مرکز یا وارونه این فرایند است و «حس» را همان

<sup>۶</sup> «سایبرنتیک» از ریشه یونانی «κυβερνήτης» به معنای تحت‌اللفظی ملوان کشتی‌ها است و به گونه فراگیر، به معنای رهبری شهر یا کشور است. [۲۰]؛ یا از ریشه یونانی «κυβερνητική» به معنای هنر فرمان‌روایی [۲۱] است. این معنا، در هر زمانی، با برخی عناصر برجسته ویژه همراه است. در تعریف وبستر-میرام، سایبرنتیک یعنی دانش نظریه ارتباطات و مهار که به گونه ویژه به بررسی تطبیقی سامانه‌های مهار خودکار؛ مانند سامانه عصبی و سامانه‌های ارتباطی مغز و مکانیکی-الکترونیکی می‌پردازد. [۲۲]

<sup>۷</sup> بنگرید: [۱۰، ۹، ۱۱] و نیز [۷]، تاریخ نوشته: ۲۳ فروردین ۱۳۹۱.

<sup>۸</sup> [۱۵]، ج ۱، ص ۲۰۰. این روایت به سبب بُنمایه غیرتعبدی و تفهیمی بودن، بر پایه مبنای «وثوق الصدور»ی و نیز تبیین تفهیمی محتوای درونی آن و نیز تواتر معنوی استوار است.

<sup>۹</sup> بنگرید: [۱۰]، درس ۹ (تبیین ساده نقلی از نظام و چرخه کار جمعی): ۷۷ تا ۹۱.



شکل ۱: هسته بنیادین ابرفقه؛ لایه‌های سامانه و نسبت میان آنها

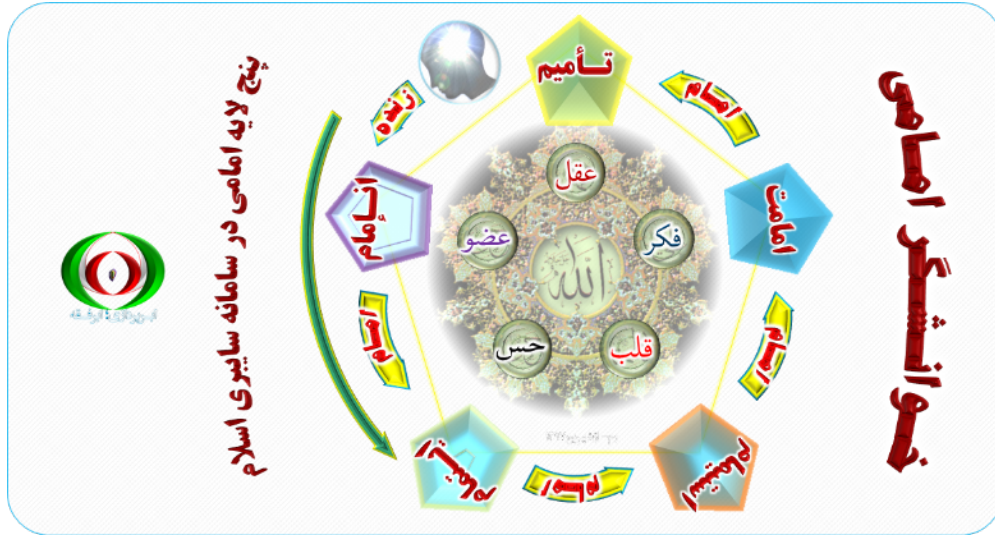
«شبكة ارتباطی و انتقالی» می‌دانیم. حس، امام لایه عضو است و نیروی بهینه را در زمان و جهت درست، به عضو، می‌رساند. عضو یعنی هر فرد یا هر بخشی از سامانه؛ که دارای کارویژه مستقل است. برپایه آنچه گفته شد، «تعقل» یعنی پیوند لایه‌ها، برای انجام کار درست.

### ۳ بررسی لایه فکر و پیوند آن به لایه عقل

بنابر آنچه از سامانه پیشرفته سایبری اسلام گذشت، فکر مأموم عقل است و باید اصول و سوگیری های کلان را از عقل (امام) بگیرد و با تفریع آنها برنامه تفصیلی بسازد. کار اصلی قوه فکر، فکر کردن نیست؛ بلکه پذیرش امام بودن عقل است. اما کارویژه فکر، حرکت در چارچوب راهنمایی کلان عقل و معیارهای عقل (عقیله تفکر)، برای رسیدن به «مطلوب» و سپس انتقال مناسب آن، به لایه قلب می‌باشد. پس کار فکر، حرکت از نامعلوم به معلوم نیست؛ چه رسد به این که چنین چیزی اصل کار فکر یا تنها کار فکر پنداشته شود. بنابراین مهمترین کار لایه فکر، پذیرش امام بودن لایه عقل است. پس از آن، نوبت به پذیرش امامت لایه عقل، برای انجام درست کار فکر می‌رسد. کارویژه فکر، «حرکت از مجهول به مطلوب» است. پس از آن، نوبت به امامت لایه فکر، بر لایه قلب می‌رسد؛ به این امور، «تفکر» می‌گوییم.

اگر شناخت یا تحقق چیزی با کمک فکر، مطلوبیت عقلی نداشته باشد، خود آن شناختن، «جهالت» است و نشناختنش، معقول است؛ بنابراین از علم غیر مفید، همانند جهل، استعاده می‌کنیم.<sup>۱۰</sup> بنابراین «تفکر کردن» یعنی قوه فکر، در بی اطاعت از عقل، فرمان عقل را بپذیرد و بر پایه اصول درست

<sup>۱۰</sup> «اللَّهُمَّ إِنِّي أَعُوذُ بِكَ ... مِنْ عِلْمٍ لَا يَنْفَعُ» [۱۳]، ج ۱، ص ۷۵. حضرت محمد (ص): «تَعَوَّذُوا بِاللَّهِ مِنْ عِلْمٍ لَا يَنْفَعُ». [۱۲]، ص ۵۲۴.



شکل ۲: خوانشگر امامی؛ نشانگر پنج لایه مربوط به امام در سامانه سایبری اسلام

اندیشیدن (عقیده تفکر) مجهول را به دست آورد و آنگاه برای اجرایی شدن آن، نتیجه کار را امامانه به قلب برساند.<sup>۱۱</sup>

#### ۴ خوانشگر «امامی» و کاربست آن در دانش سایبری اسلام

برای رسیدن به سامانه پیشرفته نیازهای شناختی، باید خوانشگر «امامی» را به کار بست. خوانشگر امامی، پنج لایه دارد: آ. «امام‌پذیری (انامام)؛ ب. امامت‌پذیری (ایتمام)؛ ج. امام‌ورزی (استیمام: تلاش برای امام شدن)؛ د. امامت‌کردن بر لایه زیرین؛ ه. پرورش و تبلیغ امام لایه زیرین و رساندن او به مقام امام‌بودن (تأمیم).<sup>۱۲</sup> بنابراین لایه فکر نخست باید امام بودن لایه عقل را بپذیرد، سپس امامت (عمل به دستورات) او را بپذیرد، سپس تلاش کند تا خود را به مقام امام‌بودن بر لایه قلب برساند، سپس به امامت‌کردن بر لایه قلب بپردازد و در پایان یکی از مأموم‌های خود را پرورش دهد تا او بتواند به مقام امام‌بودن بر لایه زیرین خود برسد.

#### ۵ خوانشگر «استیمامی» و کاربست آن در سامانه دانش سایبری اسلام

پس از امام‌پذیری (انامام)، سامانه، «زنده» می‌شود و آنگاه با اطاعت از امام (ایتمام) وارد چرخه رشد می‌شود تا بتواند به جایگاه «امام‌بودن» برای لایه زیرین برسد. خوانشگر «استیمامی» بایسته‌های هر لایه (مانند لایه فکر) برای رشد را وانمایی می‌کند: آ. «جراحی» شناخت نیازها؛ ب. «چه‌گاهی» آن؛ ج. «چه‌چیزی» نیاز

<sup>۱۱</sup> بنگرید: [۱۰]، درس ۱۰ (تبیین نخستین لایه سطح؛ «فکر»): ۹۲ تا ۹۹.

<sup>۱۲</sup> بنگرید: [۸]، درس ۱ (نیازهای بود و به‌بود: «دین»): ۲۳ تا ۴۵.



شکل ۳: خوانشگر استیمامی

شناختی؛ د. «چه‌گونی» رسیدن به نیازشناختی؛ ه. به «چه‌کار» گرفتن نیازهای شناخته شده. فراهمش این پنج ویژگی، کار عقل است و شناخت پیشرفته و بسامان این خوانشگر، کار فکر سامانه پیشرفته سایبری است.

بنابراین خرد (العقل)، پایه و مایه (اصل) هر آفریده و سامانه و پیشوای درونی است. خرد می‌کوشد که درستی را شناخته، آن را برای انجام، پیگیری کند. خرد، پیشوای فکر است و آن را در انجام کار درست، پیشوایی (امامت) کرده، چرایی، چگاهی، چه چیزی، چگونه و چه کاری را به وی می‌آموزد. فکر، بنیاد سامانه نیست؛ بلکه پیرو خرد است؛ پس بر سفارش خرد اندیشیده، آن را برنامه می‌کند. فکر پیشوای دل است و آن را در انجام کار درست، پیشوایی (امامت) کرده، چرایی، چگاهی، چه چیزی، چگونه و چه کاری را به وی می‌آموزد.<sup>۱۳</sup> بنابراین کارویژه فکر، فراهمش بهنچار برنامه و رسیدن به شناخت گسترده است؛ مانند این که خرد بگوید: «برای این، در این زمان، این چیز (سامانه لایه فکر) را با این شیوه بیابید و آن را به چرخه کار پیوند بزنید». در اینجا لایه فکر باید در پی کاوش برنامه گسترده برای انجام کار و برنامه برگزاری پیوندهای بخردانه (تعقل) باشد.<sup>۱۴</sup>

## ۶ کارکرد لایه فکر در دانش سایبری اسلام

لایه فکر باید خوانشگر «امامی» را پی بگیرد و پس از پذیرش امام (انامام)، امامت‌پذیری (ایتمام) کرده، با خوانشگر «استیمامی»، شیوه ورز یافتن برای رشد و رسیدن به جایگاه امام بر لایه‌های زیرین را بیاموزد. آنگاه این فرد یا لایه سامانه، آماده امامت‌کردن بر لایه زیرین (مانند دل) می‌شود و می‌کوشد تا لایه زیرین را نیز به

<sup>۱۳</sup>بنگرید: [۸]، درس ۱ (نیازهای بود و به‌بود: «دین»): ۲۳ تا ۴۵.

<sup>۱۴</sup>بنگرید: [۸]، درس ۴ (دیش، کارکرد و بیخت): ۶۶ تا ۷۵.



رشد بیشینه و امام شدن بر لایه زیرین برساند (تأمیم) و به این شیوه لایه‌های سامانه پیشرفته سایبری، سالم و سالم‌ساز (اسلامی) می‌شوند<sup>۱۵</sup>

یکی از بزرگترین شخصیت‌های سامانه نیمه‌پیشرفته سایبری کنونی اسلام (پیش‌نظام)، سپهبد قاسم سلیمانی است؛ او در وصیت‌نامه‌اش، شرط پایه و راز پیروزی را در «ان‌امام و ایتام» می‌داند: «کسی که در جمهوری اسلامی می‌خواهد مسئولیتی را احراز کند، شرط اساسی آن [این است که] اعتقاد حقیقی و عمل به ولایت فقیه داشته باشد»<sup>۱۶</sup>

## ۷ تبیین گلوگاه سایبری کنونی

نظام‌واره سایبری کنونی در جهان تا اندازه زیادی بر الگوی ارسطویی است که رکن حیاتی و تعیین‌کننده سامانه را «فکرِ مُدرک مفاهیم کلی» می‌داند و انسان را «حیوان ناطق» یعنی متفکر می‌داند؛ چنانکه مولوی هم می‌گوید که «ای برادر! تو همه اندیشه‌ای!» در این نظام، انسان بودن انسان و بهینه بودن سامانه به این است که اندیشه‌ورزی آزاد و ناوابسته انجام شود. در اینجا لایه «عقل» سامانه، خانه‌نشین می‌شود و رابطه امام‌بودن و امامت‌کردن نیز از میان می‌رود و حیات از سامانه پر می‌کشد کسی دانتر می‌باشد که اندیشه‌ورزی آزاد و رهاتری داشته باشد یعنی در چارچوب و عقل و بند[گی] نباشد. اما رکن حیاتی سامانه سایبری اسلام ناب و شاه‌رگ آن، «امام» است. اینجا است که برپایه توانش‌های سامانه سایبری اسلام و برجستگی شگفت‌آور و به جای «امام» رخنه سایبری گلوبالی در سامانه سایبری اسلام بسیار دشوار می‌شود. تلاش سامانه سایبری گلوبالی بر «تغییر امام حق» و جانشینی اولیای طاغوت برای دگرگونی جهان است.<sup>۱۷</sup> شیطان پس از گمراه کردن مردم (لَا ضَلَّئَهُمْ) به آرزو زده کردن آنان روی آورده است (لَأْمَنِّيَّهِمْ) و سپس قوه جاهله گلوبالی را به جای قوه عاقله نظام می‌نشانند و به امامت (پروتکل نویسی) برای اداره جهان می‌پردازد. پس نبرد بنیادین در سامانه سایبری اسلام ناب با سامان‌واره سایبری گلوبالی، نبرد بر سر «ائمه»، در سامانه سایبری اسلامی است: «العقول أئمة الأفكار و...». ابترشدن سامانه، یعنی بریدن پیوند امام و مأموم و نشانیدن اولیای طاغوتی به جای آن؛ مانند: نشانیدن فیلسوف یا فقیه (لایه فکر) به جای لایه عقل و ولیّ فقیه، نشانیدن هنرپیشه (لایه قلب) به جای امام، نشانیدن اینستاگرام و توییتر (لایه حس) به جای امام و نشانیدن پولداران یا زورمندان (لایه عضو) به جای امام؛ و گاه ترکیبی از همه اینها. از همین رو است که امام زمان فرموده‌اند که در پیشامدهای دشوار (أما الحوادث الواقعة)،<sup>۱۸</sup> باید به ولیّ امر رجوع کرد و همین مسأله راز حیاتی سامانه سایبری اسلام است. شناخت ولیّ امر و پذیرش وی (ان‌امام) برای ایتام و اطاعت است. اوست که سوگیری کلان کشور و هر تنگنای کلانی را نشان می‌دهد و دیگران باید در دنباله آن به کاوش بپردازند؛ وگرنه لایه فکر بریده از عقل، جاهل است؛ زیرا امام خود، یعنی لایه عقل و چارچوب‌ها و سیاست‌گذاری‌های کلان راهنمای

<sup>۱۵</sup> بنگرید: [۸]، همان.

<sup>۱۶</sup> بنگرید: [۶]، تاریخ خیر: ۲۴ بهمن ۱۳۹۸.

<sup>۱۷</sup> بنگرید: [۱۷]، بر پایه آیه ۱۱۸ و ۱۱۹ سوره نساء: «لَا تَخَذَنَّ مِنَ عِبَادِكُمْ نَصِيبًا مَّفْرُوضًا و لَأَضَلُّنَّهُمْ و لَأَمْنِيَّهِمْ و لَأَمْرُنَّهُمْ فَلْيَتَّبِعَنَّ آذَانَ الْأَنْعَامِ و لَأَمْرُنَّهُمْ فَلْيَتَّبِعَنَّ خَلْقَ اللَّهِ».

<sup>۱۸</sup> [۱۹]، ج ۲، ص ۴۸۴ و [۱۴]، ص ۲۹۱. بررسی بیشتر در: [۱۶]، ص ۱۸ و ۲۴.

اندیشه را نشناخته است.

سامانه سایبری اسلام، بیش از ده سده از کار افتاده بود و شاه‌رگ سامانه سایبری، همانا «فقه ولایی» است؛ یعنی چارچوب‌هایی که باید از ولی امر گرفته تا بتوان در برابر سامان‌واره بسیار پیشرفته سایبری گلوبالی چیره شد. اینک بسیاری از کارگزاران کشور و بزرگان حوزه علمیه و دانشگاه، هنوز در دنیای پیش از امامت‌پذیری (ایتمام) هستند و بی‌گمان با چنین رویکردی نمی‌توان در برابر بازوهای بسیار نیرومند سامانه سایبری گلوبالی در برنامه «اهداف توسعه پایا»<sup>۱۹</sup> با هدف رسمی «دگرگون ساختن جهان ما؛ دستور کار ۲۰۳۰ برای توسعه پایا»<sup>۲۰</sup> ایستاد. این برنامه همه ستون‌های نظام سایبری اسلام را هدف گرفته است و می‌خواهد همه ارکان حکمرانی کشور ایران و جهان را در خود فرو برده، جهانی دیگر با نظم و نظامی دیگر بسازد که با سلطه سایبری ابلیس و خلافت بر همه جهان سازگار باشد تا تأویل وارونه «إِنِّي جَاعِلٌ فِي الْأَرْضِ خَلِيفَةً»<sup>۲۱</sup> باشد.

## ۱.۷ نوک پیکان نبرد سایبری گلوبالی با تمدن اسلام

یک زمانی فتح جاسوس‌خانه آمریکا انقلاب دوم بود و اینک فضای مجازی ایران، سفارت سایبری آمریکا شده است و از مغز و حتی ناخودآگاه و قلب هر ایرانی جاسوسی می‌کنند و تمام داده‌ها و اطلاعات فرد را می‌گیرند. انقلاب دوم اکنون کجا است؟ امام خامنه‌ای می‌فرماید که «حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد».<sup>۲۲</sup> بنابراین پاسداران انقلاب، باید لایه سایبری و اشغال شده کشور در فضای مجازی را دریابد که همانا این، انقلاب دوم برای این روزگار است! چنان که رهبری می‌فرماید: «اگر من امروز رهبر انقلاب نبودم حتماً رئیس فضای مجازی کشور می‌شدم»<sup>۲۳</sup> باید از مسئولین پرسید که آیا اهمیت فضای مجازی را هم اندازه اهمیت انقلاب اسلامی می‌دانند؟ آیا شبیه‌ترین کسان به رهبری را در آن جایگاه گذاشته‌اند؟ امام جامعه می‌فرماید: «امروز قوت در فضای مجازی حیاتی است».<sup>۲۴</sup> بنابراین باید «وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ»<sup>۲۵</sup> را در اینجا پی گرفت و آن را برجسته نمود. در حالی که ما هنوز در این فضا استقلال هم نداریم و بخش بزرگی از فضای مجازی ما سرزمین اشغالی است! امام خامنه‌ای اصل و اولویت در مسئله فضای مجازی را مدیریت و اختیارداری آن می‌دانند: «آنچه عرض من است و من روی آن تکیه می‌کنم این است که فضای مجازی بدون اختیار ما، از بیرون از اختیار ما دارد مدیریت می‌شود؛ بحث این است<sup>۲۶</sup> پیامد غفلت از فضای مجازی سایبری «قتلگاه حقیقی جوانان و نوجوانان»<sup>۲۷</sup> است.

<sup>۱۹</sup> Sustainable Development Goals

<sup>۲۰</sup> Transforming our world: the 2030 Agenda for Sustainable Development، بنگرید: [۲۳].

<sup>۲۱</sup> «وَإِذْ قَالَ رَبُّكَ لِلْمَلَائِكَةِ إِنِّي جَاعِلٌ فِي الْأَرْضِ خَلِيفَةً»، [۱]، بقره، ۳۰.

<sup>۲۲</sup> [۴]، تاریخ خبر: ۲۶ اسفند ۱۳۹۰.

<sup>۲۳</sup> [۵]، تاریخ خبر: ۴ فروردین ۱۴۰۰.

<sup>۲۴</sup> [۲]، بیانات رهبری در تاریخ ۳ فروردین ۱۳۹۹.

<sup>۲۵</sup> «وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ وَ مِنْ رِبَاطِ الْخَيْلِ تُرْهَبُونَ بِهِ عَدُوَّ اللَّهِ وَ عَدُوَّكُمْ»، [۱]، انفال، ۶۰.

<sup>۲۶</sup> [۲]، بیانات رهبری در تاریخ ۲ شهریور ۱۳۹۹ در نشست با هیأت دولت.

<sup>۲۷</sup> [۳]، تاریخ نوشته: ۱۲ تیر ۱۴۰۰، بیانات رهبری در تاریخ ۱۹ آبان ۱۳۹۵ در نشست «قرارگاه قرب».



## ۸ نتیجه‌گیری

در روزگار کنونی، مدیریت سامانه‌های هوشمند، با بهره از دانش سایبری، بسیار پیچیده شده است و نمی‌توان از برجسته کردن دانش سایبر و به‌ویژه کشف سامانه سایبری اسلام (ابرفقه) چشم پوشید. این نوشتار، با کاربست یک واژه از خوانشگر «هسته بنیادین» فقه سایبری؛ یعنی واژه «أئمة»، توانست گلوگاه سایبری اسلام را یافته، به خوانش پیشاپیش یورش سایبری گلوبالی برای گرفتن تنگه راهبردی نظام سایبری تمدن اسلامی برسد. شبیخون سایبری گلوبالی در پی بریدن پیوند میان «سر» و «تن» سامانه سایبری اسلام و به‌ویژه ایران است؛ تا بتواند یک مغز گلوبالی را بر تن گیتی بنشاند؛ از این‌رو، آنان در پی فروکاست عقل نظام اسلامی از جایگاه «امام‌بودن» و «امامت‌کردن» (أئمة)، به جایگاهی زینتی هستند! یورش گلوبالی، کمابیش این جابه‌جایی را در فضای مجازی جهان و ایران، انجام داده است!

## مراجع

- [۱] قرآن کریم.
- [۲] بیانات رهبری، پایگاه دفتر حفظ و نشر آثار مقام معظم رهبری، <https://farsi.khamenei.ir/speech>، بازدید: ۲۲/۷/۱۴۰۱.
- [۳] توصیه‌های مهم امام خامنه‌ای در ضرورت مدیریت فضای مجازی، خبرگزاری تسنیم، <https://www.tasnimnews.com/fa/news/1400/04/12/2531593>، بازدید: ۲۲/۷/۱۴۰۱.
- [۴] این فضا به اندازه انقلاب اسلامی اهمیت دارد، پایگاه دفتر حفظ و نشر آثار رهبر معظم انقلاب، <https://khl.ink/f/19272>، بازدید: ۲۲/۷/۱۴۰۱.
- [۵] تأکیدات مهم رهبری درباره مدیریت فضای مجازی چیست؟ خبرگزاری مهر، [mehrnnews.com/xTZ7z](http://mehrnnews.com/xTZ7z)، بازدید: ۲۲/۷/۱۴۰۱.
- [۶] وصیت‌نامه سردار شهید قاسم سلیمانی، خبرگزاری ایسنا، [isna.ir/xdFhH2](http://isna.ir/xdFhH2)، بازدید: ۲۲/۷/۱۴۰۱.
- [۷] انقلاب اسلامی در تولید علم، با طراحی ابرطبیعیات، پایگاه رجانیوز، <http://rajanews.com/node/105567>، بازدید: ۲۲/۷/۱۴۰۱.
- [۸] امامی میبیدی، ابوالفضل. زبر تفقه نظام پیشرفته دین و برسواژ زبان فارسی. در دست ویرایش برای چاپ.
- [۹] امامی میبیدی، ابوالفضل. تفکر اسلامی یا تفلسف اسلامی. چاپ اول، طبس: فراونگ، ۱۳۹۸.
- [۱۰] امامی میبیدی، ابوالفضل. زبر تفقه نظام اسلام. چاپ اول، میبد: انتشارات میبد، ۱۴۰۰.
- [۱۱] امامی میبیدی، ابوالفضل. زبر پردازای فقه استراتژیک. چاپ اول، طبس: فراونگ، ۱۳۹۷ش.
- [۱۲] پاینده، ابوالقاسم. نهج الفصاحة. چاپ چهارم، تهران: دنیای دانش، ۱۳۸۲.
- [۱۳] طوسی، محمد بن الحسن. مصباح المتهجد و سلاح المتعبد. بیروت: موسسه فقه الشیعه، چاپ اول، ۱۴۱۱ق.
- [۱۴] طوسی، محمد بن الحسن. الغیبة. چاپ اول، قم، دارالمعارف الاسلامیه، ۱۴۱۱ق.
- [۱۵] کراچکی، محمد بن علی. کنز الفوائد. چاپ اول، قم: دار الذخائر، ۱۴۱۰ق.
- [۱۶] امامی میبیدی، ابوالفضل. فقه جهاد تبیین درباره فضای مجازی. چاپ اول، میبد، انتشارات میبد، ۱۴۰۱.

- [۱۷] امامی میبیدی، ابوالفضل و ترکیان، هانیه. غرب‌شناسی فقهی با تمرکز بر گلوبالیزم. در دست ویرایش برای چاپ.
- [۱۸] کلینی، محمد بن یعقوب. کافی. چاپ اول. قم: دارالحدیث، ۱۴۲۹ق.
- [۱۹] ابن بابویه (صدوق)، محمد بن علی. کمال الدین و تمام النعمة. چاپ دوم. تهران: اسلامیه، ۱۳۹۵ ق.
- [20] CYBER, Accademi Adella Crusca, <https://accademiadellacrusca.it/it/consulenza/cyber/1417>, Visited: 14 October 2022.
- [21] CIBERNETICA, treccani dictionary, <https://www.treccani.it/vocabolario/cibernetica>, Visited: 14 October 2022.
- [22] Cybernetics, merriam-webster dictionary, <https://www.merriam-webster.com/dictionary/cybernetics>, Visited: 14 October 2022.
- [23] Do you know all 17 SDGs?, Department of Economic and Social Affairs, Sustainable Development, <https://sdgs.un.org/goals>, Visited: 14 October 2022.

## سایبرنتیک و طراحی رفتارگرا

سید علی فارغ<sup>۱</sup>، مهدیه رمضان خواه<sup>۲</sup>

<sup>۱</sup> استادیار گروه طراحی صنعتی، دانشکده طراحی، دانشگاه هنر اسلامی تبریز، آذربایجان شرقی، ایران  
sfaregh@tabriziau.ac.ir  
<sup>۲</sup> دانشجوی کارشناسی ارشد طراحی صنعتی، دانشکده طراحی، دانشگاه هنر اسلامی تبریز، آذربایجان شرقی، ایران  
m.ramezankhah@gmail.com

### چکیده

طراحی رفتارگرا، رویکردی است که با هدف ایجاد یا حذف رفتاری خاص در کاربر، اقدام به طراحی محصولات و خدمات می‌کند. این رفتارها، گستره‌ای از نحوه استفاده از محصول تا تغییراتی عمیق‌تر در رفتار کاربران و افراد جامعه در حوزه‌هایی همچون تعاملات اجتماعی، نحوه استفاده از محصولات، محیط زیست، مقررات و ... را در بر می‌گیرد. در نگاهی دقیق‌تر به ظرفیت‌های طراحی رفتارگرا، می‌توان مطرح نمود که کنترل و حاکمیت بر جوامع نیز در این رویکرد قابل تعریف و دستیابی است. در این پژوهش برای تبیین این ظرفیت راهبردی این رویکرد طراحی، از نظریه سایبرنتیک، علم کنترل بر پدیده‌های زنده و غیرزنده، از طریق اشراف بر اطلاعات و ارتباطات پدیده‌ها، استفاده شده و بر اساس کدهای مشترک استخراج شده از این دو مفهوم و نحوه تعامل طراح و کاربر در این رویکرد، می‌توان گفت طراحی رفتارگرا مطابق با نظریه سایبرنتیک و در راستای آن، در طراحی محصول و خدمات، تعریف و استفاده می‌شود.

**کلمات کلیدی:** سایبرنتیک، سلطه، طراحی، طراحی رفتارگرا.

### ۱ مقدمه

در یک نگاه کلی به طراحی با تمام زیرمجموعه‌ها و شاخه‌های مختلف آن و گستردگی و عمق حضور آن در زندگی افراد، ظرفیت‌های مادی و غیرمادی آنچه طراحی می‌شود، و ابعاد مختلف این ظرفیت و نیز لزوم بررسی و شناخت هرچه بیشتر آن، ادراک می‌گردد. از میان سبک‌ها و رویکردهای مختلف طراحی، طراحی رفتارگرا، با هدف رفتارسازی در کاربر، از جمله زمینه‌هایی است که به نظر می‌رسد گستردگی و ظرفیت قابل توجهی برای مطالعه و فعالیت به خود اختصاص داده است. دغدغه‌ی طراحی رفتارگرا شکل دادن و اثرگذاری بر رفتارهای انسانی برای رسیدن به وضعیتی مطلوب‌تر است [۱]. اما سؤال اینجاست که وضعیت مطلوب‌تر، چه تعاریفی را در خود جای داده است؟ آیا هر محصول در حوزه طراحی رفتارگرا، تنها بر ارتباط کاربر و

محصول و رفتار مرتبط با آن تاثیر می‌گذارد؟ یا این تعامل، و به عبارتی این رفتارسازی، ابعاد، آثار و اهدافی فراتر از یک تعامل محدود در مدت زمان استفاده و حتی پس از استفاده‌ای که برای محصولات تعریف می‌شود، را دربر می‌گیرد؟

برای تبیین بیشتر این مساله و یافتن پاسخ مناسب به آن لازم است با نگاهی جامع‌تر بر طراحی رفتارگرا، چيستی و اهداف مطرح آن مروری کنیم و پاسخ به این سؤال را به کمک بررسی مفهوم سایبرنتیک، و آنچه سایبرنتیک می‌گوید و دنبال می‌کند، بدست آورده و از طریق پژوهشی توصیفی-تحلیلی بر اشتراکات و روابط مبحث سایبرنتیک و طراحی رفتارگرا، نگاهی عمیق‌تر به ظرفیت‌های طراحی رفتارگرا، داشته باشیم.

## ۲ مروری بر کارهای دیگران

خداوردی (۱۳۸۷) در مقاله‌ی «نظریه سایبرنتیک در جهان امروز» سایبرنتیک را مورد بررسی و معرفی قرار داده و ضمن اشاره به خطای محدود دانستن سایبرنتیک به علوم رایانه و یکی دانستن آن با مفهوم فضای سایبری قبل از ورود به مطالعه‌ی این مبحث، با بررسی ابعاد مختلف سایبرنتیک را نظریه و تئوری برای سایر علوم دانسته و عنوان می‌کند که مسئله اصلی در سایبرنتیک، گسترش رهیافت‌های غیر متعارف در زمینه‌های کنترل، داده پردازی، تکنولوژی رایانه‌ای و نرم افزاری و سیستم‌های خودکار در عرصه‌های مختلف علم، صنعت، اقتصاد و فرهنگ است.

شکوهیان‌راد (۱۳۹۸) در مقاله‌ی «نقش دانش شناخت در کنترل انسان» دانش شناخت را دانشی که به مطالعه ذهن و فرآیندهای ذهنی و نحوه‌ی اثرگذاری اطلاعات بر ذهن می‌پردازد، معرفی کرده و در بررسی دانش شناخت در هندسه قدرت به مفهوم سایبرنتیک می‌پردازد. در این پژوهش بیان می‌شود که مبنای تولید قدرت در عصر حاضر از منظر جهان‌بینی لیبرال، دانش سایبرنتیک است و سایر دانش‌های مولد قدرت، در نسبت با سایبرنتیک تنظیم می‌شوند. در ادامه نویسنده با تبیین بیشتر دانش سایبرنتیک و مفهوم دانش شناخت به این نتیجه دست می‌یابد که «دانش سایبرنتیک، مبنای طرح‌ریزی و تولید قدرت نرم برای کنترل پدیده‌های هوشمند است و دانش شناخت تبیین‌گر روش‌های اثرگذاری قدرت تولید شده توسط سایبرنتیک بر پدیده‌های هوشمند می‌باشد» [۲].

پانگرو (۲۰۱۹م) در مقاله «سایبرنتیک و طراحی: مکالماتی برای اقدام» به بیان نظریات رانولف گرانویل و تبیین آنها می‌پردازد. گرانویل، معمار و نظریه پرداز سایبرنتیک، سایبرنتیک و طراحی را دو روی یک سکه دانسته و آن‌را در قرن حاضر پایه‌ی ضروری طراحی می‌داند. در این پژوهش به مفهوم سایبرنتیک مرحله دوم (سایبرنتیک سایبرنتیک) نیز اشاره شده و بیان می‌کند که سایبرنتیک مرحله دوم به طراح چهارچوب‌های معرفتی داده و در واقع تمرکز اصلی خود را در بیان اهمیت سایبرنتیک در طراحی، بر سایبرنتیک مرحله دوم قرار می‌دهد.

مرتضایی (۱۳۸۹) در مقاله‌ی «بیان‌هایی پیرامون شناخت تعامل فرهنگ و طراحی (محصول)» به بررسی ارتباط طراحی و فرهنگ و تأثیر پذیری و تأثیرگذاری این دو بر یکدیگر پرداخته است. در این پژوهش با مروری بر منابع مرتبط با فرهنگ و طراحی، به ویژگی‌های نمادین و معانی و ابعاد اجتماعی محصولات اشاره داشته

و بیان می‌کند، محصول به خودی خود، برآورنده انتظارات معنایی نیست اما می‌تواند با جلب و جمع کردن تجربیات و مقایسه‌های مخاطب، معنا تولید کرده و تبدیل به شیء معنادار در بطن خود شود. نویسنده همچنین، فرهنگ و طراحی را دو طیف گسترده از معانی می‌داند که هر دو با خلق ارزش‌های مختلف عملکردی و ارزشی، تغییراتی اساسی در شکل و ماهیت زندگی ایجاد می‌کنند [۳].

مفهوم سایبرنتیک به جهت گستردگی و همان‌گونه که در مقاله‌ی خداوردی (۱۳۸۹) ذکر گردید، ارتباط وسیع و وجود آن در علوم مختلف، عنوان و مورد سؤال بسیاری از پژوهش‌ها در سالیان اخیر بوده به طوری که پژوهش‌هایی در بررسی تناوب و تکرار پرداخت به این موضوع در مقالات مختلف انجام شده است. به عنوان مثال، حسن‌زاده و همکاران (۱۳۹۵) در مقاله‌ی سایبرنتیک و الگوی مدیریت مد زودگذر با بررسی پژوهش‌های انجام شده، پیروی این کلیدواژه از الگوی مدیریت مد زودگذر را رد می‌کند [۴].

از بین پژوهش‌های فراوان در این حوزه، بسیاری از محققان تمرکز بیشتر را بر فضای سایبر و تکنولوژی رایانه‌ای داشته‌اند و بررسی سایبرنتیک با رویکرد مدیریت و کنترل و به عبارتی سلطه، به نسبت دیدگاه تکنولوژیکی به این مفهوم، کمتر مورد توجه قرار گرفته است، امر مهمی که در مقاله‌ی شکوهیان‌راد [۲] به آن اشاره شده و لزوم توجه به ابعاد حاکمیتی سایبرنتیک و علوم مرتبط با آن را یادآوری می‌کند. در مقالات مطرح‌شده‌ی بعدی، مبحث مهم طراحی و تأثیرات آن بر جوامع، ظرفیت طراحی و طراحان برای تأثیرگذاری بر حال و آینده و هویت و فرهنگ‌ها مورد بررسی قرار گرفته است. بر اساس مطالب ذکر شده در این مبحث نیز برای دستیابی بهتر به جایگاه و رابطه طراحی رفتارگرا و سایبرنتیک و پاسخ به سؤال پژوهش مفهوم سایبرنتیک را مورد تحلیل و تأمل قرار می‌دهیم.

### ۳ سایبرنتیک چیست؟ (واژه شناسی و تعاریف سایبرنتیک)

واژه‌ی سایبرنتیکس ریشه در زبان یونانی دارد، از واژه کوبرنان kubernan به مفهوم سکانداری و هدایت کشتی و کوبرنت kubernetes به معنی سکاندار کشتی و هدایت‌کننده‌ی کشتی برگرفته شده [۱۰] و از این ریشه‌ی یونانی، از سال ۱۸۳۰ در زبان فرانسوی واژه‌ی cybernétique به مفهوم «هنر حکومت‌داری» ایجاد شد [۵].

استفاده از واژه‌ی سایبرنتیک اولین بار در نوشته‌های افلاطون و نیز به طور جدی در قرن نوزدهم در نوشته‌های آمپر، در هر دو مورد، به عنوان علم دولت‌مداری اثربخش، بوده است. آمپر با عنوان «علم حاکمیت مدنی» از این واژه استفاده نمود و پس از او فلاسفه پیرو مکتب «اثبات‌گرایی» از این اصطلاح که معنی کنترل‌کننده و حکومت‌گر و هدایت‌کننده را دارد در زمینه‌های فلسفی و علوم اجتماعی و سیاسی وظایف دولت استفاده کردند [۶].

از سوی دیگر، واژه‌ی govern به معنای حکمرانی نیز با ریشه‌ی لاتین gubernare از واژه‌ی kubernan ریشه گرفته و از این روی سایبرنتیک با «حکومت کردن» و «حکمرانی» ریشه‌ی مشترکی دارد. بر این اساس می‌توان واژه سایبرنتیک را از منظر ریشه‌شناسی، معادل علم حکمرانی دانست. طرح مهم دیگر این واژه توسط دانشمندی به نام نوربرت وینر بوده است. او از لغت کاپرینیتز در تبیین

نقش کنترل و ارتباطات و توصیف معنای تبادل و تعامل و تعادل در سیستم‌ها استفاده کرد و آن را که به معنای سکندار و فرمانده و هدایت‌کننده بود، سایبرنتیک نامید؛ تا نقش کنترل و ارتباطات و انتقال اطلاعات را که چگونه حوادث پیچیده در ساختار موجودات زنده و ابزار ماشینی ساخت انسان و اعمال دستگاه‌های مکانیکی که در رهبری سیستم‌ها وجود دارد، کنترل می‌شوند نشان بدهد [۶]. مفهوم این واژه را متفکران متعددی مورد تعریف و تحلیل قرار داده‌اند و تعاریف کوتاه و بلندی از سایبرنتیک در دست است، همچون:

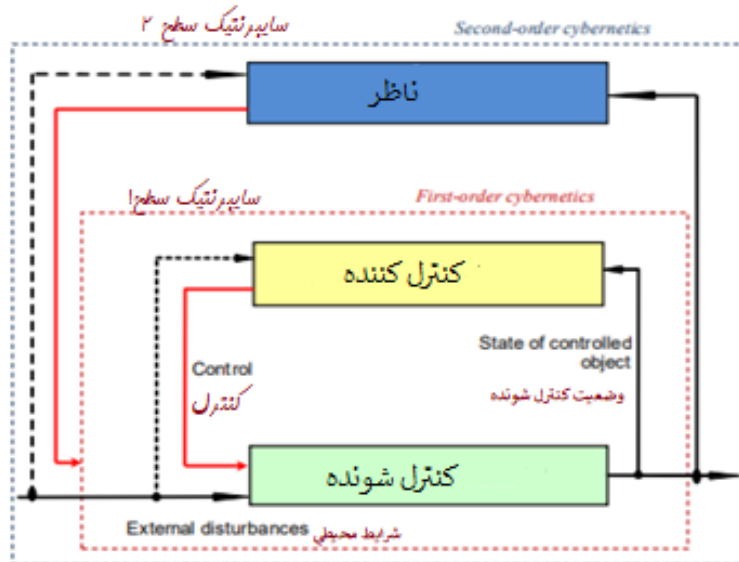
- علم ارتباط و کنترل در حیوان و ماشین (نوربرت وینر)
- یک معرفت‌شناسی تجربی که با برقراری ارتباط در درون مشاهده‌گر و بین مشاهده‌گر و محیطش می‌پردازد (وارن مک کلوچ).
- علم سازماندهی مؤثر (استافورد بیر)
- تأکید بر شکل و الگو به جای ماده و انرژی (آندره بیستون) [۷]

به‌عنوان یک تعریف جامع می‌توان گفت، علم سایبرنتیک مجموعه‌ای از علوم حکومت‌داری است که بر مبنای اطلاعات و ارتباط سیستم‌های هوشمند چه زنده و چه غیرزنده (انسان و ماشین)، این کنترل و حکومت را اعمال می‌کند. سایبرنتیک هنر هدایت است و به هم‌همی اشکال رفتاری تا جایی که منظم، یا معین یا قابل تکرار هستند سر و کار دارد: در مورد هوشمندهای طبیعی و یا الکترونیکی، روشی را برای رفتار علمی با سیستم ارائه می‌دهد که در آن پیچیدگی فوق‌العاده است و مهم‌تر از آن است که نادیده گرفته شود [۱۰]. سایبرنتیک پدیده‌های جهان را تحت مطالعه قرار می‌دهد، با تحلیل روابط بین یک پدیده با سایر پدیده‌های محیط اطراف، روش‌ها و نحوه‌ی کنترل آن را بررسی می‌نماید و این نکته را روشن می‌سازد که هر پدیده با محیط و درون خود ارتباطی ذاتی یا قراردادی دارد و شدت و ضعف این روابط، نقش، شکل و درجه پیچیدگی آن را مشخص می‌نماید. در یک جمله می‌توان گفت سایبرنتیک یک علم راهبردی است که از طریق اشراف و احاطه بر جریان اطلاعات، به کنترل اهداف مد نظر می‌پردازد [۵].

دانشمندان سایبرنتیک را به سه بخش و زمینه طبقه‌بندی می‌کنند: ۱. سایبرنتیک نظری، که با فرضیه‌سازی و نظریه‌های علمی سروکار داشته و در حوزه‌ی پژوهش و نه در حوزه‌ی عملی، حرکت می‌کند. ۲. سایبرنتیک تجربی یا کاربردی که عمل‌گرا بوده و به شبیه‌سازی می‌پردازد و از مدل‌ها در جهت استفاده‌ی عملی از سایبرنتیک بهره می‌گیرد؛ و ۳. سایبرنتیک مهندسی که ابزارسازی عرصه‌ی فنی و مکانیکی را ایجاد می‌کند [۷].

در کنار مفهوم سایبرنتیک، مبحث سایبرنتیک سطح ۲ و یا سایبرنتیک سایبرنتیک مطرح است. بر اساس این نظریه، که مبنایی تحلیلی فلسفی دارد، مجموعه‌ی کنترل‌شونده و کنترل‌کننده در یک سایبرنتیک سطح ۱ (آنچه تاکنون گفته شد) خود، تحت کنترل یک کنترل‌کننده‌ی بزرگتر در جریان است که به‌نوعی خود، کنترل کنترل را تحت نظارت اطلاعاتی و اقدام بر اساس اطلاعات گرفته است (شکل ۱).





شکل ۱: سایبرنتیک سطح ۱ و سطح ۲ (نویکوف، ۲۰۱۷)

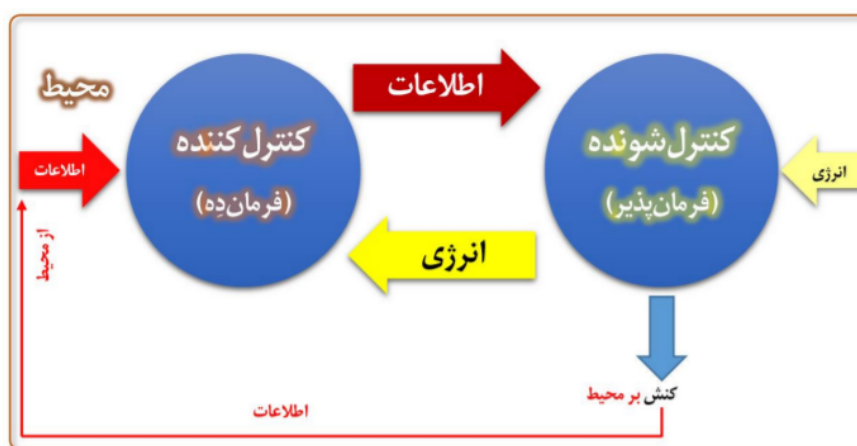
## ۴ طراحی رفتارگرا

طراحی رفتارگرا، با هدف ایجاد تغییر در رفتار کاربر، شکل می‌گیرد. در این رویکرد که ریشه در نظریات روان‌شناسی دارد باور عمومی بر آن است که از طریق طراحی محصولات و خدمات می‌توان رفتارهای انسانی را شکل داده یا دچار تغییر نمود. در طراحی رفتارگرا مباحث مرتبط با عادات و فعالیت‌های انسانی مورد تمرکز طراحان قرار می‌گیرد تا در نهایت منجر به ارتقا ارزش‌ها رفاه سلامت ایمنی و پایداری بیشتر در سطوح فردی و اجتماعی گردد [۱]. در طراحی رفتارگرا اگر چه تأکید بر توجه به عدم کنترل مخاطب وجود دارد اما با این وجود، بسیاری از محصولات، خدمات و محیط‌ها جنبه‌هایی دارند که در آن درجه‌ای از کنترل مورد نظر است [۱۱].

در واقع می‌توان گفت در طراحی رفتارگرا مبنای طراحی، بررسی جوامع هدف، نیازها و اطلاعات و در ادامه، ارائه‌ی طرح هدفمند با رویکرد ترغیب و یا جبر و تشویق به نوعی از رفتار است. مهم‌ترین اصل در طراحی رفتارگرا، تمرکز روی رفتار انسان و درک نیازهای او به عنوان کاربر نهایی محصول است، بهترین راه برای کشف نیازها، مشاهده‌ی محصولات هنگام استفاده‌ی طبیعی از آنها و ثبت رفتارهای کاربران هنگام کار با این محصولات است [۸]. بر این اساس طراح به کمک بازخوردهای کاربر، طرح محصول و خدمات را، با شرایط و تدبیری در اختیار کاربر قرار می‌دهد تا کاربر رفتار و عملکرد مد نظر طراح را در استفاده از محصول یا خدمات، داشته باشد. در حوزه‌ی محصول می‌توان به طراحی انواع «جای نشستن» که منجر به واکنش‌ها و رفتارهای مختلف و حتی ایجاد تغییر در نوع روابط اجتماعی و فرهنگ افراد شود را



شکل ۲: طراحی مبلمان برای فضا و افراد مختلف و ایجاد مدل‌های رفتاری متفاوت



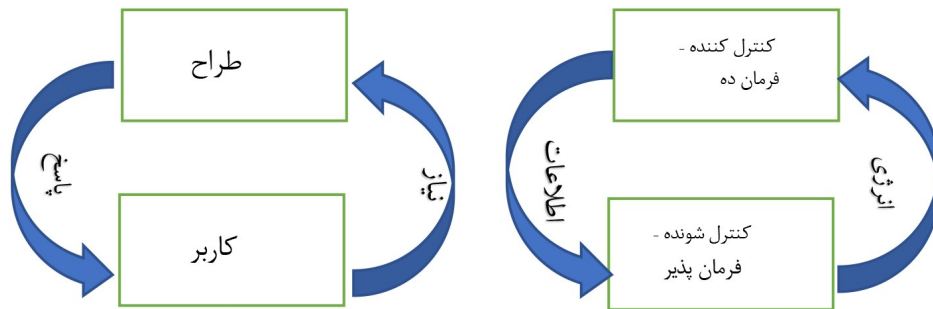
شکل ۳: کنترل در سایبرنتیک [۲]

مثال زد (شکل ۲).

در یک بیان ساده می‌توان گفت آنچه در سایبرنتیک به شکل رویه‌ی بازخورد و کنترل بین کنترل‌کننده و کنترل‌شونده وجود دارد در طراحی رفتارگرا میان طراح (به عنوان کنترل‌کننده) و کاربر (به عنوان کنترل‌شونده) مشاهده می‌شود (شکل ۳ و شکل ۴).

## ۵ نتیجه‌گیری

علم سایبرنتیک که معمولاً به نادرستی تنها محدود به فضای سایبر در نظر گرفته می‌شود، جایگاه مهمی در جهان بینی امروز دارد. علمی که با بررسی دقیق و جامع روابط و اشراف اطلاعاتی، به کنترل پدیده‌ها می‌پردازد. مفهوم مهم سایبرنتیک سایبرنتیک، تکمیل و تأییدکننده‌ی این سلطه و کنترل است. مشابه با



شکل ۴: رابطه کنترل کننده - طراح و کنترل شونده - کاربر

رویکرد بازخورد و کنترل در سایبرنتیک، طراحی رفتارگرا، رویکردی که اساساً هدف آن ایجاد و یا تغییر رفتاری در کاربر است، مورد استفاده قرار می‌دهد. در هر دوی این مفاهیم اهمیت چرخه‌ی اطلاعات و بازخورد و وجود هدف کنترل و ایجاد تغییر در رفتار کاربر، به چشم می‌خورد و البته با توجه به مفهوم سایبرنتیک سطح دوم، می‌توان چرخه‌ی طراحی رفتارگرا و طراح را در مفهوم سایبرنتیک سطح دوم نیز تعریف و طراحی رفتارگرا را، به عنوان سایبرنتیک کاربردی در حوزه‌ی طراحی مطرح کرده و آن را دارای ظرفیت استفاده به عنوان ابزار کنترل بر کاربران دانست.

## مراجع

- [۱] یکتاراد، محمد امین و همکاران. پرسمان دیزاین، نشر وارث، تهران، ۱۴۰۰.
- [۲] شکوهیان‌راد، محمدعلی. نقش دانش شناخت در کنترل انسان، فصلنامه آینده، شماره ۱۰، صفحات ۱۹-۱۴، ۱۳۹۸.
- [۳] مرتضایی، سیدرضا. بیان‌هایی پیرامون شناخت تعامل فرهنگ و طراحی (محصول)، هنرهای زیبا، شماره ۴۳، پاییز ۱۳۸۹، صفحات ۶۸-۵۷، ۱۳۸۹.
- [۴] حسن‌زاده، محمد؛ صدیقی، زینب؛ حسینی‌شعار، منصوره. سایبرنتیک و الگوی مدیریت مد زودگذر، فصلنامه دانش‌شناسی، دوره ۹، شماره ۳۳، شهریور ۱۳۹۵، صفحات ۳۷-۵۰.
- [۵] شکوهیان‌راد، محمدعلی. نظریه‌ی جنگ در عصر سیستم‌های فرماندهی - کنترل، انتشارات مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی، تهران، ۱۳۹۷.
- [۶] بیان، حسام‌الدین. نظریه سایبرنتیک، فرآیند مدیریت و توسعه، دوره ۶، شماره ۲، تهران، صفحات ۱۷-۱، ۱۳۷۱.
- [۷] نوکریزی، محسن؛ حسین‌قاسمی، علی. چشم‌اندازی بر ارتباطات و سیبرنتیک، کتابداری و اطلاع‌رسانی، شماره ۱۸، صفحات ۴۰-۲۵، تابستان ۱۳۸۱.
- [۸] مرتضایی، سیدرضا؛ دادخواه فرد، شیما. بکارگیری روش کاربرمحور مبتنی بر رفتارگرایی در طراحی محصول، نشریه هنرهای تجسمی، ۱۹-۰، ۱۳۹۳.
- [۹] خداوردی، حسن. نظریه سایبرنتیک در جهان امروز، نشریه ره‌آورد سیاسی، شماره ۹، بهار ۱۳۸۷.

- [10] Novikov, Dmitry A. Cybernetics, Control Philosophy and Control Methodology, 2016.
- [11] Lockton, Dan. Design, behavior change and the Design with Intent toolkit: Theories and Practices of Designing for Change, Design for Behavior Change, 2017.

## تهدیدات اکوسایبرنتیکی، چهارچوب نوین تهدیدات علیه زیست‌بوم

عاطفه نصیری<sup>۱</sup>، محمدعلی شکوهیان‌راد<sup>۲</sup>

<sup>۱</sup> کارشناس ارشد مهندسی منابع طبیعی، دانشگاه آزاد اسلامی، واحد تهران شمال  
nasiry.atefeh@gmail.com  
<sup>۲</sup> پژوهشگر ارشد آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران  
cm@shokoohian.ir

### چکیده

پژوهش حاضر در آمدی بر معرفی علمی و مصداقی تهدیدات اکوسایبرنتیکی است. اکوسایبرنتیک، دانشی است که موضوع اصلی آن، اعمال کنترل بر زیست‌بوم (و به تبع آن، تمامی اجزای وابسته به آن، زیستی و غیرزیستی موجود و به واسطه‌ی اعمال تغییرات بر این عناصر انجام می‌شود. تفاوت تهدیدات اکوسایبرنتیکی با تهدیدات مرسوم زیستی در آن است که در تهدیدات زیستی، عموماً هدف عامل، تخریب و تغییر است و اهداف ثانویه و مستمر را در بر ندارد. اما تهدیدات اکوسایبرنتیکی، به دنبال کنترل زیست‌بوم در مسیر مشخصی است که الزاماً از کانال تخریب و نابودسازی نمی‌گذرد؛ بلکه اتکا بر تغییر جریان اطلاعات زیست‌بوم دارد و می‌تواند به طرق مختلف صورت پذیرد. در رخدادهای اکوسایبرنتیکی، خودکنترلی و تعادل ذاتی از زیست‌بوم گرفته شده و نوعی دگرکنترلی توسط عامل مهاجم اعمال می‌شود که سیر طبیعی زیست‌بوم را تغییر می‌دهد. خرچنگ سبز خلیج ماین در آمریکا، شانه‌دار دریای مازندران و درخت کهور آمریکایی در استان‌های جنوبی کشور، از مصداق تهدیدات اکوسایبرنتیکی هستند. در زمان حاضر، توجه پدافندی به وجه کنترلی منابع طبیعی کشور در عرصه‌ی نبردهای اکوسایبرنتیکی، بسیار ضروری است؛ لذا تدوین راهبرد و برنامه‌ی ملی مبتنی بر پروتکل‌های بومی کنترل زیست‌بوم (و نه پروتکل‌های بین‌المللی) شاید یکی از ضروری‌ترین موضوعات در مجموعه‌ی محیط‌زیست کشور باشد. یکی از ابزارهای مهم در مطالعه و پیش‌بینی تهدیدات اکوسایبرنتیکی، طرح «طبقه‌بندی اثرات زیست‌محیطی گونه‌های مهاجم» است که می‌تواند از وقوع تهدیداتی مشابه کهور آمریکایی و یا شانه‌دار دریای مازندران جلوگیری نماید.

**کلمات کلیدی:** اکوسایبرنتیک، زیست‌بوم، کنترل زیست‌بوم، منابع طبیعی ایران، گونه‌های مهاجم، تهدیدات زیستی.

## ۱ مقدمه

یکی از مؤلفه‌های قدرت در هر کشور، منابع طبیعی و زیست‌بوم آن هستند. پیشتر، حکمرانان، در راستای کشورگشایی و با چشم‌داشت به منابع مهم طبیعی سایر کشورها، اقدام به لشکرکشی و جنگ می‌نمودند، تا در پس آن بتوانند از منابع طبیعی سایر کشورها، علی‌الخصوص آب و راه‌های دریایی، بهره‌مند گردند. امروزه، با توجه به تجربه‌ی بشر از دوران استعمار و نیز جنگ‌های جهانی اول و دوم، دیگر شاهد نبردهای مستقیم و رو در رو در میان کشورها نیستیم؛ بلکه یکی از راهبردهای اصلی، تصاحب منابع، تخریب منابع و جدیداً کنترل منابع و زیست‌بوم کشورهای رقیب در راستای تضعیف حکمرانی‌شان است. این اهداف با اتکا به تکنولوژی‌ها، روش‌ها و ابزارهای کاملاً جدید و عمدتاً اثبات‌ناپذیر یا سخت‌اثبات‌پذیر انجام می‌گیرد که امروزه ذیل دانش اکوسایبرنتیک مطالعه و تحلیل می‌شوند.

اهمیت دانش اکوسایبرنتیک و شناخت تهدیدات اکوسایبرنتیکی علیه زیست‌بوم کشور، از آن جهت مهم است که اولاً در کشورهای مختلف از جمله ایران، مصادیق چندی از آن تجربه شده و خسارات جدی و جبران‌ناپذیر به زیست‌بوم تحمیل نموده است و ثانیاً مجامع بین‌المللی نیز به گسترده شدن این قبیل تهدیدات اشاره نموده و نسبت به آن هشدار داده‌اند. برای نمونه، مطابق گزارش ریسک‌های جهانی مجمع اقتصاد جهانی در سال جاری (گزارش ریسک‌های جهانی، ۲۰۲۲)، از پنج ریسک اصلی که ایران با آنها روبرو است، دو مورد به زیست‌بوم‌های طبیعی مربوط می‌شود که شامل «بحران‌های منابع طبیعی» و «از دست دادن تنوع زیستی و فروپاشی زیست‌بوم»<sup>۱</sup> می‌باشد.

اینکه چرا تنوع زیستی مهم است و در حال حاضر، از دست دادن آن یکی از تهدیدات حیاتی در کشور محسوب می‌شود، به‌طور خلاصه باید گفت تنوع زیستی را می‌توان گوناگونی در شکل حیات یک منطقه دانست. تنوع زیستی، یک ثروت طبیعی است که نیاز بشر را در زمینه‌های پوشاک، خوراک، مسکن و حتی سلامتی روان تأمین می‌کند. در هر زیست‌بوم هرچه تنوع زیستی بیشتر باشد، زنجیره‌ی غذایی طولانی‌تر و شبکه‌ی حیاتی پیچیده‌تر می‌شود، در نتیجه محیط، پایدارتر و از شرایط خود تنظیمی بیشتری برخوردار می‌گردد. هر جزئی از یک زیست‌بوم، جایگاه خاص خود را دارد و دیگر اجزا قادر نیستند نقش آن را ایفا کنند. در یک کلام، تنوع زیستی، کلید پایداری و سلامت محیط‌زیست و زیست‌بوم است (کیان نجفی و همکاران، ۱۳۹۲).

پژوهش حاضر از این جنبه دارای نوآوری است که برای نخستین بار در زبان فارسی، دانش اکوسایبرنتیک را توضیح داده و با رویکرد سایبرنتیک به بررسی وضعیت برخی زیست‌بوم‌های کشور (اکوسایبرنتیک)<sup>۲</sup> و شناسایی مصادیق تهدیدات و تغییرات زیستی از نوع اکوسایبرنتیکی می‌پردازد؛ تهدیداتی که منتج به ناکارآمدسازی زیست‌بوم، انقراض گونه‌ها، کاهش کیفیت و کمیت برای استفاده‌ی انسانی و دریک کلام «اعمال کنترل غیر طبیعی بر حیات، محیط زیست و زیست‌بوم انسان» می‌شوند.

<sup>۱</sup> مطابق تعریف ارائه شده توسط این سازمان (مجمع جهانی اقتصاد)، از دست دادن تنوع زیستی و فروپاشی زیست‌بوم، به معنای پیامدهای برگشت‌ناپذیر برای محیط‌زیست، انسان و فعالیت‌های اقتصادی و نابودی دائمی سرمایه‌های طبیعی، در نتیجه انقراض و/یا کاهش گونه‌ها است.

<sup>۲</sup>Eco-cybernetics



ساختار پژوهش حاضر بدین صورت است که ابتدا مفهوم‌شناسی و ماهیت‌شناسی اکوسایبرنتیک ارائه می‌گردد؛ سپس رخدادهای اکوسایبرنتیکی بررسی شده و تفاوت آن با تهدیدات بیولوژیکی بیان می‌شود؛ در گام بعد مصادیق بین‌المللی و داخلی رخدادهای و تهدیدات اکوسایبرنتیکی مطرح می‌شود و در نهایت مشخص می‌شود که این قبیل تهدیدات را چگونه و با چه ابزاری می‌توان کشف، شناسایی، مطالعه و پیشگیری نمود.

## ۲ پیشینه پژوهش

یکی از نخستین مطالعاتی که به ارتباط اکولوژی و سایبرنتیک پرداخته، مطالعه‌ی وبستر<sup>۳</sup> و مکلوگین<sup>۴</sup> در سال ۱۹۷۰ میلادی است. در مطالعه‌ی مذکور عنوان شده که دانش اکولوژی در کنار سایبرنتیک می‌تواند برای جغرافی‌دانان و برنامه‌ریزان شهری به کار آید و سبب درک و شکلهی بهتر سیستم‌های شهری شود (وبستر و مکلوگین، ۱۹۷۰، صص ۳۶۹ تا ۴۰۸).

کلارک<sup>۵</sup> (۱۹۷۷) یک مدل «اکوسایبرنتیک» را معرفی می‌کند که در آن هر موجودیتی (مثلاً یک مدرسه یا یک درخت) را به عنوان سیستمی با اهداف، منابع، فرآیندها، سیگنال‌ها و فعال‌کننده‌ها در نظر می‌گیرد (کلارک، ۱۹۷۷).

از دیگر مقالاتی که آثار دانش سایبرنتیک بر زیست‌بوم را بررسی نموده، نوشتاری از مک‌ناگتن<sup>۶</sup> در ۱۹۸۱ میلادی است، با عنوان «ماهیت سایبرنتیک زیست‌بوم» که در آن بیان داشته **اساساً زیست‌بوم، یک سیستم سایبرنتیکی است**. مطابق نظر وی، جریان اطلاعات در ذات هر فرآیند سایبرنتیکی وجود دارد و آنچه یک زیست‌بوم را با سایبرنتیک منطبق می‌کند؛ وجود هماهنگی، تنظیم، ارتباط و کنترل در روابط موجود در یک زیست‌بوم است. هرگونه برهم‌کنش<sup>۷</sup> بوم‌شناختی، مشتمل بر رقابت، همزیستی<sup>۸</sup>، رابطه‌ی انگلی، شکارگری و هم‌سفرگی<sup>۹</sup>، با جریان اطلاعات سر و کار دارند و روابط منظمی مانند آنچه بر شمرده شد، فقط از طریق تنظیم و کنترل، قابل حفظ است و کنترل، خود مستلزم اطلاعات است (مک‌ناگتن، ۱۹۸۱).

در پژوهش نیلسن<sup>۱۰</sup> مورخ سال ۲۰۱۶ میلادی، تلاش شده تا برای سیستم‌های بسیار پیچیده‌ی زیست‌بوم‌های طبیعی و روابط موجود در آن، فرمول‌های محاسباتی ارائه شود، تا درک تعاملات موجود در زیست‌بوم، ساده‌تر گردد. مطابق نظر وی، جریان‌های تحمیلی که بر سیستم تأثیر می‌گذارند، سبب واکنش‌های نامشخصی می‌گردند که به سادگی قابل پیش‌بینی نیستند. هر نوع پاسخ و واکنش، در واقع یک تغییر سایبرنتیکی است که لزوماً تابع هدف مشخصی نیست و شناخت آن در طول زمان و با توسعه‌ی ویژگی‌های شناختی، سیستم‌های تفسیری، ذخیره‌سازی اطلاعات، دانش، تجربیات و آگاهی تغییر می‌کند. وی تلاش

<sup>3</sup>Webster

<sup>4</sup>McLoughlin

<sup>5</sup>Clark

<sup>6</sup>Mcnaughton

<sup>7</sup>Interaction

<sup>8</sup>Mutualism

<sup>9</sup>Commensalism

<sup>10</sup>Nielsen

کرده تا با استفاده از دانش سایبرنتیک، به مدل سازی روابط در زیست بومها بپردازد (نیلسن، ۲۰۱۶). نیمیک<sup>۱۱</sup> و همکارانش در سال ۲۰۱۸ به بررسی این موضوع پرداختند که برای مبارزه با گونه‌های مهاجم، علاوه بر عوامل اکولوژیکی، چه عوامل اقتصادی یا اجتماعی می‌تواند روند تهاجمی گونه‌ی مهاجم را کند کرده یا افزایش دهد و در نهایت توصیه‌های سیاستی را برای کاهش گسترش مهاجمان ارائه دادند. آنها عمدتاً به این موضوع پرداختند که فعالیت‌های انسانی، چه تأثیری بر روند تهاجمی یک گونه‌ی مهاجم دارد و این که چگونه ممکن است چندین محرک اجتماعی - اقتصادی بر پراکنش یک گونه‌ی مهاجم تأثیر بگذارد. در واقع آنچه مورد توجه آنها قرار گرفته است، عملکرد انسان‌ها، پس از ورود گونه‌های مهاجم به یک زیست بوم است و این که این عملکرد، چه تأثیری بر کنترل روند زیست بوم منطقه و تغییر آن از حالت طبیعی به سمت تغییر زیستگاه داشته است (نیمیک و همکاران، ۲۰۱۸، صص ۷۰ تا ۸۰).

در مطالعه‌ای دیگر که با استفاده از مدل سازی کامپیوتری انجام شد، دویزی<sup>۱۲</sup> و همکارانش در سال ۲۰۱۸ میلادی به بررسی این موضوع پرداختند که اثرات گونه‌های مهاجم در شبکه‌های بزرگ غذایی و اکولوژیکی چگونه خواهد بود و نتیجه گرفتند که خطر گونه‌های مهاجم در قبال گونه‌های بومی، بسیار بیشتر از آن چیزی است که عمدتاً تصور می‌شده است (دویزی و همکاران، ۲۰۱۸، ص ۷).

پودوالنی<sup>۱۳</sup> و همکارش نیز در مطالعه‌ی سال ۲۰۲۰ خود تلاش نموده‌اند تا ویژگی‌های حیات وحش را در قالب مفاهیم سایبرنتیک تعریف نمایند تا درک پیچیدگی‌های زیست بوم، ساده‌تر شود و این کار را برای مدیریت محیط زیست، الزامی دانسته‌اند؛ بدین ترتیب کنترل محیط زیست، ساده‌تر می‌گردد (پودوالنی و همکاران، ۲۰۲۰، ص ۱۴).

و در نهایت، مطابق نظر پترز<sup>۱۴</sup> و همکاران (۲۰۲۱)، از منظر فلسفه زیستی، در نقطه تاریخی خاصی قرار داریم که در آن، زیست شناسی و اطلاعات گرد هم می‌آیند تا با گسترش سیستم‌های اکوسایبرنتیکی، مسیرهای تکاملی - فرهنگی را در رابطه با حکومت زمین تعیین کنند (پترز و همکاران، ۲۰۲۱، ۳۷۰ تا ۳۸۸).

## ۳ ادبیات پژوهش

### ۱.۳ مفهوم شناسی و ماهیت شناسی اکوسایبرنتیک

اکوسایبرنتیک از تلفیق دو مفهوم «اکوسیستم»<sup>۱۵</sup> (که در سراسر متن حاضر به دلیل رعایت فارسی‌گزینی، از معادل زیست بوم برای آن استفاده شده) و «سایبرنتیک»<sup>۱۶</sup> حاصل شده است. مطابق تعریف بریتانیکا، «زیست بوم، مجموعه‌ای از موجودات زنده، محیط فیزیکی‌شان و تمام روابط متقابل آنها در یک واحد خاص

<sup>11</sup>Niemiec

<sup>12</sup>Doizy

<sup>13</sup>Podvalny

<sup>14</sup>Peters

<sup>15</sup>Ecosystem

<sup>16</sup>Cybernetics

مکانی است. یک زیست‌بوم از اجزای غیر زنده (از جمله مواد معدنی، آب و هوا، خاک، آب، نور خورشید و سایر عناصر غیر زنده‌ی دیگر) و اجزای زیستی آن که مشتمل بر همه‌ی اعضای زنده است، تشکیل شده است» (بریتانیکا، واژه‌ی Ecosystem).

همچنین طبق تعریف مارینسکو<sup>۱۷</sup>، کلمه‌ی سایبرنتیک از واژه‌ی یونانی Kybernetes گرفته شده و به معنای وسیله‌ای برای هدایت کشتی یا حمایت از حکومت انسانی است که در مجموع دلالت بر امر کنترل دارد. این کلمه، اولین بار توسط افلاطون، برای نشان دادن حکومت به کار رفت.

سایبرنتیک کاربردهایی در زمینه‌های مختلفی چون روانشناسی و نظریه‌ی کنترل، فلسفه و مهندسی مکانیک، معماری و زیست‌شناسی تکاملی، علوم اجتماعی و مهندسی برق دارد. البته فیلسوفان و دانشمندان، تعاریف متفاوتی از سایبرنتیک دارند. مثلاً ریاضیدان معروف آندری نیکولایویچ کولموگروف<sup>۱۸</sup>، سایبرنتیک را به عنوان «علمی که به مطالعه‌ی سیستم‌هایی - با هر ماهیتی - که قادر به دریافت، ذخیره و پردازش اطلاعات، برای استفاده در مقوله‌ی کنترل هستند» تعریف می‌کند (مارینسکو، ۲۰۱۷). لذا مهم‌ترین موضوع در سایبرنتیک، توان اعمال کنترل است.

با توجه به تعاریف فوق، اکوسایبرنتیک دانشی است که بحث اصلی آن، اعمال کنترل بر زیست‌بوم (و به تبع آن، تمامی اجزای وابسته به زیست‌بوم خصوصاً انسان) است. این امر از طریق کنترل جریان اطلاعات آن زیست‌بوم و با توجه به مؤلفه‌های زیستی و غیرزیستی زیست‌بوم و به واسطه‌ی اعمال تغییرات بر این عناصر انجام می‌شود.

اما تفاوت تهدیدات اکوسایبرنتیکی با تهدیدات زیستی (تهدیدات اکولوژیکی و بیولوژیکی) در چیست؟

**تهدیدات زیستی.** به انتشار عوامل زیست‌پایه یا غیرزیستی نظیر سموم که با قصد آسیب رساندن یا ارباب انجام می‌شود و بر انسان‌ها، حیوانات یا گیاهان اثر می‌گذارد، تهدیدات زیستی گفته می‌شود. در مقایسه با سایر انواع تهدیدات (متعارف، هسته‌ای، شیمیایی) در تهدیدات زیستی، روابط پیچیده‌ای وجود دارد. در بسیاری از تهدیدات زیستی؛ تغییرات محیطی، جزء عوامل تعیین‌کننده‌ی اصلی در مجموعه‌ی تهدیدات موجود هستند. محتمل‌ترین نوع و موضوع کلیدی تهدیدات زیستی، بیوتروریسم<sup>۱۹</sup> است (رادوساولیویچ، ۲۰۱۹، صص ۴۵۰ تا ۴۵۷).

<sup>17</sup>Dan C. Marinescu

<sup>18</sup>Andrey Nikolaevich Kolmogorov

<sup>19</sup>Bioterrorism

**تهاجمات زیستی.** تهاجمات زیستی<sup>۲۰</sup>، محرک اصلی تغییرات جهانی است. برخی گونه‌های مهاجم<sup>۲۱</sup>، بازخوردهای کلیدی زیست‌بوم را به نحوی تغییر می‌دهند که منجر به تغییر رژیم زیستی منطقه شده و پیامدهایی برای تنوع زیستی، خدمات زیست‌بوم، معیشت و رفاه انسان در پی دارد (شاکلتون، ۲۰۱۸، صص ۳۰۰ تا ۳۱۴). با این توضیحات مشخص می‌شود که مقوله‌ی کنترل، تهدیدات و تهاجمات زیستی، تقریباً مقوله‌ای هست که در دنیای امروز، شناخته شده و پیرامون آن، گفتنی‌های بنیادین و بسیار مهم وجود دارد.

## ۲.۳ بررسی رخدادهای اکوسایبرنتیکی و تفاوت آن با تهدیدات بیولوژیکی

تفاوت اصلی تهدیدات اکوسایبرنتیکی با تهدیدات مرسوم زیستی در این است که در تهدیدات زیستی، عموماً هدف عامل، تخریب است و اهداف ثانویه و مستمر را در بر ندارد. برای نمونه، انتشار عامل بیماری‌زا در پرندگان، به دنبال کاهش جمعیت آنهاست و احتمالاً موارد بعدی آن را لحاظ نکرده اما رخدادهای اکوسایبرنتیکی، به دنبال کنترل زیست‌بوم در مسیر مشخصی هستند که الزاماً از کانال تخریب و نابودسازی نمی‌گذرد؛ بلکه اتکا بر تغییر جریان اطلاعات زیست‌بوم دارد که می‌تواند به طرق مختلف صورت پذیرد. در نتیجه در رخدادهای اکوسایبرنتیکی، خودکنترلی و تعادل ذاتی از زیست‌بوم گرفته شده و نوعی دگرکنترلی توسط عامل مهاجم بر زیست‌بوم اعمال می‌شود که مسیر زیست طبیعی را برای مدتی طولانی تغییر می‌دهد. برای نمونه هر نوع تغییر تعادلی طبیعی یک زیست‌بوم، در منطقه‌ای مشخص، با علم به اینکه در روند «ورودی - پردازش - خروجی» اطلاعات زیستی آن منطقه، چه تغییراتی حاصل می‌شود و در بلند مدت چه نتایجی در بر دارد، از نوع اقدامات اکوسایبرنتیکی است. برای مثال گسترش گونه‌ء مهاجم کهور آمریکایی، اهداف بلند مدتی نظیر ایجاد خشک‌سالی را در بر دارد و کانونی است برای تغییر و کنترل جریان اطلاعات زیستی یک زیست‌بوم که هم‌اکنون مناطق جنوبی کشور مانند استان خوزستان را درگیر کرده است و از طریق آن می‌توان برای مدتی، رفتارهای زیست‌بوم و ساکنان آن را به دلیل ایجاد بحران محیطی کنترل نمود؛ زیرا خودکنترلی زیست‌بوم از سلب شده و دگرکنترلی از سوی درخت کهور بر محیط اطرافش اعمال می‌گردد.

از سویی با در نظر گرفتن گزارش ارائه شده از سوی مجمع جهانی اقتصاد در حوزه‌ی تهدیدات زیست‌بوم‌ها و از سوی دیگر به دلیل تخریب‌های روزافزون زیست‌بوم‌های طبیعی کشور، ضرورت پرداختن به علل و عوامل تخریب زیست‌بوم‌ها و ریشه‌یابی ایجاد بحران در زیست‌بوم کشور، کاملاً جدی و دارای اولویت است. اینکه چرا موضوع مذکور، محل تأمل است و جای نگرانی دارد -سوی مواردی که ممکن است در نگاه اول به چشم آیند، نظیر بیابان‌زایی یا تغییر چشم‌انداز طبیعی- باید گفت که تغییرات محیطی مشتمل بر تغییرات انسانی است که بر زیست‌بوم چشم‌انداز، زیست‌بوم انسانی و محیط‌های ایجاد شده توسط انسان و

### <sup>20</sup>Biological invasions

<sup>۲۱</sup>گروهی از گونه‌های غیربومی که به دلیل تغییرات شرایط زیست‌بوم یا پتانسیل ژنتیکی ویژه‌ی خود در زیستگاه طبیعی جمعیت‌های بارور گسترده‌ای تولید می‌کنند و غالباً سبب اختلالات و عدم تعادل زیست‌بوم خاص مانند کاهش جمعیت یا حذف گونه‌های بومی، اختلال در چرخه‌های هیدرولوژیکی و تغییر رژیم‌های آتش‌سوزی در زیستگاه‌ها می‌گردند (محرابیان و همکاران، ۱۴۰۰). همچنین در تعریف دیگری که توسط دولت ایالات متحده ارائه شده است، «گونه‌ی مهاجم، گونه‌ای است که موجودی غیربومی در زیست‌بوم مشخص باشد و معرفی آن، باعث آسیب اقتصادی یا زیست‌محیطی یا آسیب به سلامت انسان، حیوان یا گیاه شود» (Reaser et al., 2020).

همچنین آشفته‌گی‌ها و بلایای طبیعی تأثیر می‌گذارد.

ویژگی‌های محیطی، در قالب اجزای فیزیکی، شیمیایی، زیستی یا اجتماعی محیط‌ها از جمله جمعیت‌ها و صفات موجودات مربوطه که قابل اندازه‌گیری باشند، تعریف می‌شوند. هر نوع آشفته‌گی محیطی، بر تعادل زیست‌بوم و بافت درون جمعیت‌ها تأثیر گذارده، در آن بیماری بروز می‌کند که از این گذر می‌تواند کنترل زیست‌بوم را از خودکنترلی طبیعی خود به دیگرکنترلی غیرطبیعی تغییر دهد. بسیاری از شیوع‌ها با تغییرات جهانی یا محلی ناشی از تغییرات آب و هوا، تغییرات چشم‌انداز ناشی از اثرگذاری غیرمستقیم انسان یا تأثیر مستقیم فعالیت‌های انسانی مرتبط هستند. به علاوه با انتشار عوامل بیماری‌زا به مناطق جدید و تغییر فرآیند محیطی ممکن است بر چرخه‌ی انتقال پاتوژن‌های عفونی تأثیر بگذارد و منجر به شیوع بیماری شود (رادوساویویچ، ۲۰۱۹، صص ۴۵۰ تا ۴۵۷).

مطابق نظر میتن<sup>۲۲</sup>، گونه‌های مهاجم، منجر به استعمار ژنتیکی<sup>۲۳</sup> می‌شوند و در واقع به نظر وی، تهاجمات این چنینی به معنای استعمار ژنتیکی یک محیط توسط یک گونه‌ی غیربومی است. فعالیت‌های انسانی، سبب ایجاد استعمارهای متعدد ژنتیکی شده‌اند که اغلب نتایج فاجعه‌باری به همراه داشته‌اند. مثلاً، گربه‌های اهلی وارد شده به نیوزیلند و استرالیا، باعث انقراض پرندگان زمینی و انقراض محلی برخی از کیسه‌داران شدند. در مثالی دیگر، می‌توان به کشتی‌های اقیانوس‌پیما اشاره کرد. هنگامی که کشتی‌های اقیانوس‌پیما بار کامل ندارند، آب دریا را به مخازن خود پمپ می‌کنند تا تعادل خود را تنظیم کنند. با ورود به بندر جدید و محموله‌گیری، این آب را از مخازن خارج می‌کنند و هزاران لارو دریایی را وارد محیط جدید می‌نمایند که تعادل و کنترل بومی زیست‌بوم‌های محلی را تدریجاً مختل می‌سازد. برای نمونه، بیش از ۶۰ گونه‌ی دریایی از این طریق، خلیج سانفرانسیسکو را به قبضه‌ی خود درآورده‌اند (میتون، ۲۰۱۳، صص ۲۳۶).

اساساً بررسی اکوسایبرنتیک تهاجم‌های زیستی و زیست‌بومی، یک رشته‌ی نوپا اما به سرعت در حال پیشرفت است (پارسون، ۲۰۲۲). گونه‌های مهاجم، که با مقاصد برهم زدن خودکنترلی زیست‌بوم به یک زیست‌بوم وارد می‌شوند، می‌توانند آسیب‌های جبران‌ناپذیری به نظام‌مندی زیستی وارد کنند؛ در نتیجه تنوع زیستی را کاهش دهند و حتی سلامت انسان را تهدید نموده و بر آن تأثیر بگذارند. ۲۰ تا ۳۰ درصد از همه‌ی گونه‌های معرفی‌شده، آسیب‌های عمده‌ای به محیط‌های جدید خود وارد کرده‌اند که منجر به خسارت بیش از ۱۲۰ میلیارد دلار در سال می‌شود و راه‌حل‌های بالقوه، برای شناسایی مقرون‌به‌صرفه‌ترین روش برای ترمیم و پیشگیری از این آسیب‌ها هنوز در حال بررسی است [و در واقع هنوز راه حل خاصی برای آنها معرفی نشده است]. تشخیص زودهنگام گونه‌های مهاجمی که آثار اکوسایبرنتیکی دارند، برای حفظ تنوع زیستی و جلوگیری از آسیب‌های زیست‌بوم بسیار مهم است زیرا بسیاری از روش‌های ریشه‌کنی می‌تواند پرهزینه باشد و به حیات وحش بومی آسیب برساند (دنزیگر و همکاران، ۲۰۲۲، صص ۱۸۸۱ تا ۱۸۹۴). اما این در حالی است که هنوز دانش اکوسایبرنتیک و روش‌ها و ابزارهای مورد استفاده‌ی آن در کشور کاملاً ناشناخته است و در عین حال، تشخیص‌های فوق‌الذکر با روش‌ها و ابزارهای مرسوم و متداول زیستی، یا اساساً امکان‌پذیر نیست و یا بسیار مشکل است. بنابراین، یک روش قابل اعتماد برای شناسایی و ردیابی گونه‌های مهاجم بر

<sup>22</sup>J.B.Mitton

<sup>23</sup>Genetic Colonization

اساس نگاه و خط مشی علمی و فنی اکوسایبرنتیک، در شرایط امروز کشور کاملاً ضروری است.

### ۳.۳ مصادیق بین‌المللی و داخلی رخدادها و تهدیدات اکوسایبرنتیکی

#### ۱.۳.۳ خرچنگ سبز در خلیج ماین

یکی از گونه‌های مهاجم در خلیج ماین<sup>۲۴</sup> ایالات متحده، خرچنگ سبز<sup>۲۵</sup> است که منجر به آسیب‌دیدگی زیست‌بوم و تنوع زیستی آن شده است. این خرچنگ به مرور زمان از طریق نابود کردن علف مارماهی<sup>۲۶</sup> بر بخشی از کنترل طبیعی و درونی زیست‌بوم مسلط شده و تعادل درونی زیست‌بوم را برهم می‌زند. اما چرا نابودی علف مارماهی، تعادل زیست‌بوم منطقه را برهم می‌زند؟

علف مارماهی، گونه‌ی زیستی ضروری برای برخی گونه‌های ماهی، صدف و منبع غذایی پرندگان و سایر گونه‌های محلی است. همچنین علف مارماهی در صنایع غذایی و اقتصادی جنوب این خلیج، کاربرد دارد. این علف همچنین با تثبیت رسوبات پایین و تنظیم عملکرد موج، باعث طولانی کردن روند فرسایش ساحلی می‌شود. تمام این‌ها بدان معنا است که با افزایش تخریب این جامعه‌ی گیاهی، فرسایش ساحلی زیاد شده و این خود موجب از دست دادن زیست‌گاه سایر گونه‌های آبی - خاکی (ساحلی) و نزدیک به ساحل شده است (دنزیگر و همکاران، ۲۰۲۲، صص ۱۸۸۱ تا ۱۸۹۴).

از سوی دیگر چرا رخداد فوق، از منظر اکوسایبرنتیک قابل بررسی است و با قواره‌ی تهدیدات زیستی بررسی نشده است؟ با وجود اینکه در نهایت چنین به نظر می‌آید که صرفاً یک تهدید زیستی رخ داده است. پاسخ آن است که در این رخداد، عامل تهدید، اولاً جزئی از زیست‌بوم شده، در آن رشد کرده، تکثیر یافته و استمرار دارد؛ و ثانیاً کنترل درونی زیست‌بوم را در اختیار خود گرفته و دگرکنترلی بر زیست‌بوم اعمال کرده است؛ از این رو یک تهدید اکوسایبرنتیکی است. می‌توان همین نتایج را از طریق حذف مستقیم - و نه چرخه‌ای - علف مارماهی انجام داد؛ مثلاً سم خاصی در منطقه رها شود تا این علف حذف گردد. اما به دلیل توان ذاتی زیست‌بوم‌ها در بازسازی خود و برگشت به وضعیت تعادل، پس از مدتی، عامل تهدید از بین رفته و علف مارماهی به چرخه‌ی زیستی باز می‌گشت. عموماً تهدیدات زیستی به صورت دفعی ظاهر شده و پس از طی مدتی ولو چند سال، رفع می‌شوند اما تهدیدات اکوسایبرنتیکی به آرامی حاصل می‌شوند اما استمرار داشته و خود رژیم زیستی محلی را به خدمت می‌گیرند تا بقا یابند؛ و تا بقا داشته باشند، کنترل طبیعی زیست‌بوم نیز باز نخواهد گشت.

#### ۲.۳.۳ شانه‌دار دریای مازندران

یکی از مهم‌ترین مصادیق تهاجمات اکوسایبرنتیکی در ایران، مربوط به شانه‌دار دریای مازندران<sup>۲۷</sup>، است. این جاندار در اصل، بومی غرب اقیانوس اطلس است (قبولی و همکاران، ۲۰۱۳).

<sup>24</sup>Gulf of Maine

<sup>25</sup>Carcinus maenas

<sup>26</sup>Zostera marina L

<sup>27</sup>Mnemiopsis leidyi



این گونه‌ی مهاجم، اثرات مخربی بر زیست‌بوم طبیعی دریای مازندران داشته؛ برای مثال سبب کاهش ذخایر کیلکای آنچوی از ۱۸۵ هزار تن در سال ۱۳۷۵، به کمتر از ۲۰۰ تن در سال ۱۳۹۰ شده است. حذف کیلکای آنچوی می‌تواند سبب کاهش شدید در ذخایر آبزیان طبقات بالاتر یعنی ماهیان خاویاری و فک دریای مازندران بشود (فضلی، ۱۳۹۴). رقم خسارت وارده از این شانه‌دار به زیست‌بوم دریای مازندران، طی سال‌های ۱۳۷۹ تا ۱۳۸۳، بالغ بر ۵.۹۶۲ میلیارد ریال است (غفارزاده و همکاران، ۱۳۸۶). اساساً کیلکای آنچوی در چرخه‌ی غذایی این دریا بسیار مهم است و در سفره‌ی غذایی انسان هم سهم دارد.

برخلاف دریای سیاه و اقیانوس‌های اطراف آن، دریای مازندران محل پرترددی برای مقاصد کشتیرانی نیست، ولی به دلیل بسته بودن این زیست‌بوم، پتانسیل زیاد و ریسک خطرپذیری بالایی در تجمع گونه‌های آبی غیربومی دارد. برخی گونه‌های آبی، طی سال‌های اخیر از دریای سیاه به این دریا انتقال داده شده‌اند. شانه‌دار، ابتدا از طریق آب توازن کشتی‌ها به دریای سیاه و آروف و سپس به دریای مازندران وارد شده است و پس از ورود، سبب از بین رفتن برخی زئوپلانکتون‌های این دریا گردیده (روحی و همکاران، ۱۳۹۵). در دریای مازندران از زمان ورود این جانور، میزان پلانکتون‌های جانوری، ۷۵٪ کاهش داشته‌اند و از آنجا که این پلانکتون‌ها، غذای اصلی ماهی کیلکا و تمامی بچه ماهی‌ها هستند، و کیلکا نیز مهم‌ترین غذای بسیاری از جانوران این دریا، از جمله ماهیان خاویاری، ماهی آزاد و فک دریای مازندران است؛ به جمعیت این گونه‌ها نیز آسیب رسیده و به این ترتیب کل زنجیره‌ی غذایی دریای مازندران با اختلال مواجه شده است (فیض‌الله‌پور، ۱۳۹۳).

### ۳.۳.۳ کشور آمریکایی

از نمونه‌های دیگری که در زیست‌بوم طبیعی ایران وارد شده است، می‌توان به گونه‌ی گیاهی کشور آمریکایی<sup>۲۸</sup> اشاره کرد. کشور آمریکای، یکی از مسأله‌دارترین گونه‌های مهاجم در سطح دنیا بوده و تبعات اکوسایبرنتیکی حاصل از تهاجم زیستی آن، آثار زیان بار متعدد، دامنه‌دار و بلند مدت بر زیست‌بوم‌های طبیعی مناطق نیمه حاره‌ای تا خشک کره‌ی زمین وارد آورده است. این گونه در ابتدا در بسیاری از مناطق کره‌ی زمین، با هدف مهندسی زیست‌بوم از جمله حفاظت آب و خاک و مبارزه با بیابان‌زایی در مناطق گرم و خشک و همچنین تولید چوب معرفی گردید. کشور آمریکایی، بومی مناطق شمالی آمریکای جنوبی، آمریکای مرکزی و کشورهای همچون بولیوی، آرژانتین، کلمبیا، ونزوئلا و مکزیک است. تهدیدات مخرب آن، باعث نابودی سایر گونه‌های گیاهی بومی و هم‌بوم زیر تاج پوشش این گونه می‌گردد. به علت هجوم این گیاه به نخیلات و زمین‌های کشاورزی استان هرمزگان، آن را یک آفت مهم در منطقه به‌شمار می‌آورند (حشمتی و همکاران، ۱۳۹۹).

امروز تمام کشورهای خارجی و منطقه‌ای حتی کشورهای عربی و حاشیه‌ی خلیج فارس، سرمایه‌گذاری هنگفتی را برای نابودی این نوع درخت صورت داده‌اند و حتی اتحادیه‌ی اروپا این گونه‌ی گیاهی را خطرناک‌ترین موجود زنده‌ی دنیا نام‌گذاری کرده و در فهرست سیاه مهاجمان زیستی دنیا قرار داده است. درختان **کشور آمریکایی** فاقد رطوبت بوده و با خشک نگه‌داشتن هوای اطراف خود مانع تشکیل ابرهای باران‌زا می‌شوند و با خاصیت پوست‌ریزی برگ‌هایشان در زمان گرده‌افشانی، گرده‌هایشان را وارد هوا می‌کنند.

<sup>28</sup>Prosopis juliflora

این درختان با سفت کردن خاک و کم کردن پوشش گیاهی سبب می‌شوند آب‌های سطحی به زمین فرو نرود و در نتیجه سیلاب‌های ویرانگر ایجاد شود. با کم شدن گیاهان و بوته‌های اطراف، خاک حاصلخیز شسته شده و گیاهان خودرو رشد نمی‌کنند. کهور آمریکایی دارای سمی است که منجر به فلج اعصاب فک و صورت و لرزش فک و در نهایت مرگ دام می‌شود و مسمومیت دام‌های اهلی از نیام‌های باران خورده‌ی این گونه نیز گزارش شده است. این گونه‌ی گیاهی، زمین را غیرقابل استفاده می‌کند و به خاطر این موضوع در فهرست گونه‌های مهاجم اتحادیه‌ی جهانی حفاظت از طبیعت نیز قرار دارد. از طرف دیگر بر اساس برخی گزارش‌ها علت ۴۵ درصد آلودگی بیماران در امارات متحده عربی، وجود گیاه کهور است. عمق فاجعه آنجا است که بیش از ۹۰ درصد از پوشش گیاهی استان خوزستان از نوع کهور آمریکایی است. کاشت درختان کهور آمریکایی، در پی مطالعات انجام شده از سوی سازمان جنگل‌ها، مراتع و آبخیزداری به منظور مقابله با ریزگردها انجام شده و ۱۵۰ میلیون دلار نیز اعتبار بدان تخصیص داده شد (خبرگزاری مجلس شورای اسلامی، ۹ بهمن ۱۳۹۶). لذا همانطور که از دامنه‌ی اطلاعات و مستندات مشخص است، کهور آمریکایی صرفاً یک تهدید زیستی نیست بلکه یک پروژه‌ی اکوسایبرنتیکی است؛ زیرا خودکنترلی طبیعی و تعادل طبیعت را در حوزه‌های آب، دام، خاک، سایر گیاهان از اختیار طبیعت در آورده تا اولاً بقاء خود را تضمین کند و ثانیاً کنترل زیست‌بوم را در اختیار داشته باشد. این همان نکته‌ی مهم و راهبردی است که در اختلاف عمقی و عملکردی تهدیدات اکوسایبرنتیکی با تهدیدات زیستی مرسوم بیان شده بود.

به غیر از مصداق اکوسایبرنتیکی فوق که نمونه‌ی بسیار معروفی است؛ نتایج تحقیقات نشان می‌دهد که تا سال ۱۴۰۰ ه.ش، حدود ۲۷ گونه‌ی گیاهی بیگانه وارد پوشش گیاهی کشور ایران شده است که دست کم یازده گونه‌ی آنها، از منظر تهدیدات اکوسایبرنتیکی، مهاجم هستند (محرابیان و همکاران، ۱۴۰۰).

امروزه نیز که مبحث تغییرات آب و هوایی بسیار پررنگ شده است و آلودگی‌های هوا (به خصوص حاصل از ریزگردها و سوخت‌های فسیلی) بیش از پیش مطرح شده، ضرورت دارد توجه ویژه‌ای به کنترل منابع طبیعی کشور در راستای حفظ آنها و کمک به برطرف کردن آلودگی‌های زیست‌محیطی داشت؛ چرا که احتمال بسیار بالایی نسبت به آلودگی‌هایی که منشأ آنها طراحی تهدیدات اکوسایبرنتیکی است، وجود دارد. یکی از بخش‌هایی که در گزارش سال جاری مجمع اقتصاد جهانی مورد توجه قرار گرفته است، سرفصل «مقاوم‌سازی زیست‌بوم‌های ملی برای بحران‌های آینده» است. فارغ از اینکه ادعای فوق چقدر صحت دارد و دقیق است، باید این پرسش را مدنظر داشت که در کشور ما، چقدر به این قبیل موارد توجه می‌شود؟ آیا ما برای حفظ منابع خود در برابر طراحی‌های عامدانه‌ی اکوسایبرنتیکی که در تلاش هستند تا کنترل طبیعت کشور را به دست بگیرند، آمادگی راهبردی و عملیاتی لازم را داریم؟

به نظر می‌رسد که در سایه بی‌توجهی مسئولان امر از سویی و دخالت عوامل وابسته به دشمن در تصمیم‌سازی و مدیریت محیط‌زیست از سوی دیگر، ما با روند از دست دادن شدید و بسیار خطرناک منابع طبیعی کشور مواجه هستیم که استمرار آن، عمق فاجعه را بیشتر خواهد نمود.

## ۴.۳ سخت‌اثبات‌پذیر بودن تهدیدات اکوسایبرنتیکی

اساساً طبیعت، بستر لازم برای حیات انسانی و سایر گونه‌های زیستی است. پس بدیهی است زمانی که این بستر از بین رفته یا از حالت طبیعی خودکنترلی خود خارج شود، به نسبت حیات بشری دچار اختلال می‌گردد. مطالعات در خصوص گونه‌های مهاجم اکوسایبرنتیکی در اقصی نقاط جهان، فراوان است؛ اما نکته‌ی بسیار مهم آن است که معمولاً اکثر این مطالعات علمی و مستند در قبال اینکه ورود گونه‌های مهاجم و مخرب زیست‌بوم، عمدی بوده است؛ سکوت کرده‌اند. برخی از منابعی که در تلاش بوده‌اند عوامل طراحی تهدیدات نوین اکوسایبرنتیکی را شناسایی نمایند، اساساً توان اثبات عاملیت یا حتی تعمد در ورود گونه‌ی مهاجم را نداشته‌اند. به همین دلیل است که در ابتدای پژوهش حاضر بیان شد تهدیدات اکوسایبرنتیکی، تهدیداتی اثبات‌ناپذیر یا سخت‌اثبات‌پذیر هستند. زیرا هرچند که گزاره‌های عقلی و استدلالی برای تعیین تعمد و عاملیت موضوع داشته‌اند، اما استحصال شواهد علمی و حقوقی لازم برایشان مهیا نبوده است.

برای نمونه در مطالعه‌ای که ساکی و همکاران انجام داده‌اند، عنوان شده که برای ورود شانه‌دار مهاجم به دریای مازندران، دو روش اتفاقی (از طریق آب توازن کشتی‌ها) و عمدی مطرح است:

۱. **سناریوی ورود اتفاقی:** ورود اتفاقی شانه‌دار به دریای مازندران می‌تواند توسط آب توازن کشتی‌ها اتفاق افتاده باشد. بررسی‌ها نشان می‌دهد که کشتی‌ها برای ورود به دریای مازندران، در دریای سیاه بایستی از کانال ولگا دن عبور کنند. آنها ابتدا وارد رودخانه‌ی دن می‌شوند. کشتی‌ها در دریای سیاه قبل از ورود به رودخانه‌ی دن، مخزن آب توازن خود را تخلیه می‌کنند و چون تلاطمی در مسیر وجود ندارد، در طول مسیر ۶۰ کیلومتری خود با مخزن خالی حرکت می‌کنند. در این مدت می‌بایست شانه‌دار (اگر در مخزن باشد) با کم‌آبی کف مخزن و تکان‌های شدید آن خود را حفظ کرده باشد. وقتی کشتی به انتهای مسیر و ورودی دریای مازندران رسید، در آستاراخان و در دهانه‌ی رودخانه‌ی ولگا می‌رسد، برای ادامه‌ی دریانوردی در این دریا، آبیگیری مخزن توازن خود را انجام می‌دهد. آب رودخانه‌ی ولگا از نوع آب شیرین است که برای شانه‌دار کشنده است و اگر ورود اتفاقی انجام شده باشد، می‌بایست بعد از این عملیات، شانه‌دار از دریای سیاه به دریای مازندران انتقال داده شده باشد. شاید تا بدین جا، ورود اتفاقی یک فرضیه‌ی محتمل باشد اما نکته‌ی بسیار مهم و اثبات شده این است که حتی اگر شانه‌دار در طول مسیر زنده مانده باشد، زمانی که در دهانه ورودی دریای مازندران آبیگیری مخزن توازنی کشتی انجام می‌شود، بر اثر استرس ناشی از تغییر شوری آب از بین می‌رود. این ادعا در تحقیقات مربوط به سازگاری شانه‌دار با آب دریای مازندران نیز مشاهده شده که با ورود ناگهانی آب دریای مازندران به تانکر، این جانور می‌میرد. پس چنین به نظر می‌رسد که ورود اتفاقی شانه‌دار به دریای مازندران امکان نداشته باشد.

۲. **سناریوی ورود عمدی:** رهاسازی دستی و عمدی شانه‌دار در دریای مازندران توسط افراد یا سازمان‌ها و ... دومین احتمال مطرح شده است. تحقیقات نشان داده که برای رهاسازی شانه‌دار در دریای مازندران، سازگاری این جانور با زیست‌بوم مازندران الزامی است. بنابر این رهاسازی عمدی نمی‌تواند در آب‌های شمالی دریای مازندران که شوری کمی دارد، انجام شده باشد. در نتیجه این

رهاسازی عمدی می‌بایست بعد از تحقیقات علمی و میدانی در بلند مدت روی سازگاری زیستی و اولویت مکانی مناسب، انجام شده باشد. همچنین بلافاصله بعد از رهاسازی، تعداد شانه‌دار زیاد نمی‌شود و مدت قابل توجهی لازم است تا این جانور، حضور خود را در محیط تثبیت نموده، آشکار شود و آثار منفی تهاجمی خود را در اخلاص چرخه‌ی خودکنترلی زیست‌بوم نشان دهد. به نظر می‌رسد با توجه به عدم امکان ورود اتفاقی شانه‌دار مهاجم دریای مازندران به این دریا، این جانور می‌بایست به‌طور عمدی و توسط تجهیزات سازگارکننده‌ی زیستی و با اهداف و برنامه‌ی قبلی به دریای مازندران وارد شده باشد (ساکی و همکاران، ۱۳۹۵). در نتیجه با توجه به مجموع شواهد یاد شده، ورود این جاندار به پهنه‌ی دریای مازندران، عمدی ارزیابی می‌شود اما نسبت به فاعلیت آن، اسناد حقوقی در دست نیست.

بنابراین امروزه توجه پدافندی به وجه کنترلی منابع طبیعی کشور در عرصه‌ی نبردهای اکوسایبرنتیکی، بسیار ضروری است و ادامه‌ی عدم شناخت تهدیدات اکوسایبرنتیکی و عدم طرح‌ریزی راهبردی و فقدان برنامه‌ی عملیاتی ملی جهت مقابله با آنها که از دست رفتن کنترل طبیعی زیست‌بوم‌های کشور را در پی دارد، آینده‌ی بسیار خطیری را برای تمامی گونه‌های زیستی خصوصاً انسان ترسیم می‌نماید. لذا تدوین راهبرد و برنامه‌ی ملی مبتنی بر پروتکل‌های بومی کنترل زیست‌بوم (و نه پروتکل‌های بین‌المللی که اکثراً انطباق با زیست‌بوم کشورها ندارند) شاید حیاتی‌ترین عرصه در مجموعه‌ی محیط‌زیست کشور باشد. راهبردها و پروتکل‌هایی که ذیل آن، سیاست‌های عملی برای حفظ وضعیت طبیعی زیست‌بوم‌ها در نظر گرفته شود و در ادامه، به جبران خسارات حاصل از گونه‌های مهاجم نیز بپردازد.

نکته‌ی بسیار مهم این است که برخی محققان، روند ورود گونه‌های مهاجم را با پروژه‌های جهانی‌سازی<sup>۲۹</sup> مرتبط دانسته‌اند. برای نمونه کلر<sup>۳۰</sup> و همکاران بیان کرده‌اند «درست است که جهانی‌سازی، به‌واسطه‌ی جابجایی افراد و کالاها، مزایای بسیاری را به همراه دارد؛ اما منجر به انتقال عمد و غیرعمد موجودات در بین زیست‌بوم‌ها می‌شود. زیست‌بوم‌هایی که قبلاً از هم جدا بودند (کلر و همکاران، ۲۰۱۱).

## ۴ نتیجه‌گیری

مجموع مواردی که در پژوهش حاضر ارائه شد:

اولاً بدین منظور است که نشان داده شود رخداد‌های اکوسایبرنتیکی و آثار مخرب و پایدار آنها بر زیست‌بوم و به تبع آن، وقوع آسیب‌های مختلف غذایی، اقتصادی، سلامتی و ... مقوله‌ای است که در اقصی نقاط جهان سابقه دارد و سایر کشورها کم و بیش به آن پرداخته‌اند. پس اگر ادبیات و دانش آن در کشور ما ناشناخته و فاقد سابقه است، حاصل بی‌توجهی به این عرصه‌ی مهم است که البته ریشه در ناشناس بودن دانش سایبرنتیک و آثار و کارکردهای گسترده‌ی آن دارد.

<sup>29</sup>Globalization

<sup>30</sup>Keller

ثانیاً نباید تهدیدات اکوسایبرنتیکی را با تهدیدات زیستی سابق و مرسوم، یکسان پنداشت؛ هرچند که در نهایت تبعات زیستی داشته و قطعاً نظرات متخصصان زیست‌شناسی نسبت به این گونه تهدیدات نوین از اهمیت برخوردار است. اما صحیح و مؤثر آن است که از منظر روند کنترل طبیعی و چرخه‌مانند زیست‌بوم، درجه‌ی ورود تهدیدات و سپس محل اثرگذاری آن تحلیل و بررسی شود تا بتوان مانع از عملیاتی شدن تهدیدات اکوسایبرنتیکی شد.

به‌منظور شناسایی فوق‌الذکر، ضرورت دارد دقیقاً با رویکرد اکوسایبرنتیکی، گونه‌های مختلف گیاهی و حیوانی غیربومی در ایران شناسایی شده و آثار آنها بر چرخه‌ی خودکنترل زیست‌بوم‌های کشور مورد مطالعه قرار گیرد و در نهایت بر این اساس مشخص گردد ورود کدام گونه‌ها به بهبود روند خودکنترلی هر زیست‌بوم کمک کرده، کدام گونه‌ها تقریباً هیچ اثر بارزی نداشته و کدام گونه‌ها روند خودکنترلی زیست‌بوم را با اختلال و عدم تعادل مواجه می‌سازند. چنین پژوهشی هرچند گسترده و زمان‌بر است اما یکی از ضروری‌ترین نیازهای امروز کشور می‌باشد و مبنایی است برای تصمیمات آتی مسئولان کشور در حوزه‌های مختلفی که به نحوهای گوناگون بر زیست‌بوم‌های کشور اثرگذار هستند.

به‌منظور تهیه و تدوین فهرست تفصیلی و کیفی فوق، یکی از روش‌های پیشنهادی، استفاده از طرح «طبقه‌بندی اثرات زیست‌محیطی برای گونه‌های بیگانه»<sup>۳۱</sup> است که اثرات تنوع زیستی را از منظر اکوسایبرنتیک بر زیست‌بوم هدف ارزیابی می‌کند. طرح EICAT یکی از استانداردهای جهانی «اتحادیه‌ی بین‌المللی حفاظت از طبیعت»<sup>۳۲</sup> است<sup>۳۳</sup> که برای اندازه‌گیری شدت اثرات زیست‌محیطی ناشی از حیوانات، قارچ‌ها و گیاهانی است که در خارج از محدوده‌ی طبیعی زیستی خود، ظاهر می‌شوند (جشکه و همکاران، ۲۰۲۲، صص ۳۶۸ تا ۳۸۱). این ابزار سنجش به متخصصان، دست‌اندرکاران حفاظت و سیاست‌گذاران کشورها در حوزه‌های مختلف مرتبط با زیست‌بوم در مورد پیامدهای بالقوه‌ی گونه‌های بیگانه هشدار داده و راهنمایی‌هایی را برای گسترش اقدامات پیشگیرانه و کاهش آثار منفی آنها ارائه می‌دهد. همچنین به اولویت‌بندی اقدامات مدیریتی زیست‌بوم‌ها نیز کمک می‌نماید (IUCN، ۲۰۲۲).

این طرح در کنار طرحی دیگری با نام «طبقه‌بندی اثرات اجتماعی و اقتصادی گونه‌های بیگانه»<sup>۳۴</sup> که به ارزیابی گونه‌های غیربومی یک منطقه از حیث آثار اجتماعی و اقتصادی آنها می‌پردازد (جشکه و همکاران، ۲۰۲۲، صص ۳۶۸ تا ۳۸۱)، کمک می‌کند تا با توجه به پوشش جانوری (: فون) و پوشش گیاهی و نباتی (: فلور) منطقه، گونه‌های مهاجمی که به هر زیست‌بومی وارد می‌شوند، قابل شناسایی گردند. نکته‌ی دیگری که می‌تواند حائز اهمیت باشد، در نظر گرفتن ردیف بودجه‌ی خاص برای مبارزه با گونه‌های مهاجم است. مثلاً آفریقای جنوبی، سالانه حدود ۱۱۵ میلیون دلار، برای مبارزه با گونه‌های مهاجم اختصاص می‌دهد و یکی از مواردی که در این هزینه کرد، بسیار پررنگ است، آموزش دادن عامه‌ی جامعه در این خصوص است (نوباس و همکاران، ۲۰۲۱، صص ۱۵).

<sup>31</sup>EICAT: The Environmental Impact Classification for Alien Taxa

<sup>32</sup>IUCN: The International Union for Conservation of Nature

<sup>33</sup>اعضای این اتحادیه، منحصرأ از دولت‌ها و سازمان‌های جامعه‌ی مدنی تشکیل شده‌اند.

<sup>34</sup>SEICAT: Socio-economic Impact Classification of Alien Taxa



## سیاس گزاری

از راهنمایی‌های استاد ارجمندم، جناب آقای دکتر حسین نگارستان، برای نوشتن این مقاله، متشکرم.

## مراجع

- [۱] کیان نجفی تیره شبانکاره و رحمان اسدپور، «گونه‌ی غیربومی و مهاجم کهور آمریکایی (*Prosopis juliflora*) تهدیدی برای تنوع زیستی بوم‌نظام‌های سواحل و جزایر خلیج فارس و دریای عمان»، همایش ملی پدافند غیر عامل در بخش کشاورزی، ۱۳۹۲.
- [۲] حسن فضل‌ی، «اثر شانه دار مهاجم دریای مازندران (*Mnemiopsis leidyi*) بر ذخایر پنج گونه ماهی مهم تجاری در سواحل جنوبی دریای مازندران»، زیست‌شناسی دریا (بیولوژی دریا)، بهار ۱۳۹۴، دوره‌ی ۷، شماره ۲۵، صفحات ۲۳ تا ۳۴.
- [۳] حمیدرضا غفارزاده و نازلی هنریخش، «بررسی تبعات اقتصادی عدم مبارزه با گونه مهاجم شانه‌دار در سواحل ایرانی دریای مازندران»، فصلنامه علوم و تکنولوژی محیط‌زیست، دوره‌ی ۹، شماره‌ی ۴، اسفند ۱۳۸۶، صفحات ۱۱۷ تا ۱۲۸.
- [۴] ابوالقاسم روحی و همکاران، «بررسی روند تغییرات شانه‌دار و اثرات آن بر روی زئوپلانکتون‌های حوضه‌ی جنوبی دریای مازندران»، مجله‌ی آبریان دریایی مازندران، سال یکم، شماره‌ی ۱، تابستان ۱۳۹۵، صفحه‌ی ۲۴ تا ۳۶.
- [۵] م. فیض‌الله‌پور، «مخاطرات زیست محیطی دریای مازندران، در ارتباط با تأثیر گونه‌ی شانه دار مهاجم به جمعیت کیلکا و فک مازندران»، اولین همایش ملی ارزیابی و مدیریت و آمایش محیط زیستی در ایران، آذر ۱۳۹۳.
- [۶] ا. حشمتی، ن. خراسانی، ب. ش. اسفندآباد، ب. ریاضی، «ارزیابی اثر تغییر اقلیم بر ریسک تهاجم زیستی کهور آمریکایی در زیست بوم‌های طبیعی ایران»، فصل‌نامه‌ی علمی - پژوهشی محیط‌زیست جانوری، سال ۱۲، بهار ۱۳۹۹.
- [۷] خبرگزاری مجلس شورای اسلامی، «درخت کهور آمریکایی، دیوی سیاه در لباس فرشته‌ای سبز / پروژه ویران‌سازی زیست محیطی از کجا آب می‌خورد»، سرویس اجتماعی، ۹ بهمن ۱۳۹۶، پیوند به: <http://www.icana.ir/Fa/News/367692>
- [۸] ر. محرابیان و همکاران، «الگوهای انتشار گیاهان معرفی شده به ایران»، فصل‌نامه‌ی علمی زیست‌شناسی کاربردی دانشگاه الزهراء(س)، دوره‌ی ۳۵، شماره‌ی ۳، صفحات ۱۱۵ تا ۱۵۷، پاییز ۱۴۰۰.
- [۹] ا. ساکی، ح. نگارستان، م. غلامی، «بررسی نحوه‌ی ورود شانه‌دار مهاجم دریای مازندران به زیست‌بوم این دریا»، همایش ملی آبی‌پروری و زیست‌بوم آبی پایدار، ۵ صفحه، مهر ۱۳۹۵.
- [10] World Economic Forum, "The Global Risks Report 2022," 17th Edition, P 101.
- [11] J. B. McLoughlin, J. N. Webster, "Cybernetic and general-system approaches to urban and regional research: a review of the literature," Environment and Planning, 1970, vol. 2, Pages 369-408
- [12] J.W. Clark, "General systems perspectives," Journal of Creative Behavior, 1977, vol. 11. Pages 36-46.
- [13] Samuel J Mcnaughton, "The Cybernetic Nature of Ecosystems," The American Naturalist, vol. 117, No. 6 June 1981, Pages 985-990.
- [14] S. N. Nielsen, "Second order cybernetics and semiotics in ecological systems—Where complexity really begins," Ecological Modeling, vol. 319, January 2016, Pages 119-129.



- [15] R.M. Niemiec, G.P. Asner, P.G. Brodrick, J.A. Gaertner, N.M. Ardoin, "Scale-dependence of environmental and socioeconomic drivers of albizia invasion in Hawaii," *Landscapes and Urban Planning*, vol. 169, January 2018, Pages 70-80.
- [16] A. Doizy, E. Barter, J. Memmott, K. Varnham, T. Gross, "Impact of cyber-invasive species on a large ecological network," *Scientific reports*, vol. 8, 2018.
- [17] S. L. Podvalny, E. M. Vasiljev, "The cybernetic concept of multialternativity in the evolution of biological systems," *Journal of Physics: Conference Series*, 2020.
- [18] 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.
- [19] Britannica, Branch Science, Concept Ecosystem, Link: <https://www.britannica.com/science/ecosystem>.
- [20] Dan C. Marinescu, "Complex Systems and Clouds," Elsevier: *Computer Science Review and Trends*, 2017.
- [21] V. Radosavljevic, "Environmental Health and Bioterrorism," *Encyclopedia of Environmental Health (Second Edition)*, Year 2019, Pages 450-457.
- [22] Ross T. Shackleton, "Social-ecological drivers and impacts of invasion-related regime shifts: consequences for ecosystem services and human wellbeing," *Environmental Science & Policy*, Volume 89, November 2018, Pages 300-314.
- [23] J. B. Mitton, Brenner's, "Genetic Colonization," *Encyclopedia of Genetics (Second Edition)*, 2013, Page 236.
- [24] Dean E. Pearson, "Biological Invasions: An Overview," *Reference Module in Life Sciences*, 2022.
- [25] A. M. Danziger & M. Frederich, "Challenges in eDNA detection of the invasive European green crab, *Carcinus maenas*," *Biological Invasions*, vol. 24, Pages 1881-1894, 2022.
- [26] Sara Ghabooli and Tamara A. Shiganova, "Invasion Pathway of the Ctenophore *Mnemiopsis leidyi* in the Mediterranean Sea," *Plos One*, November 26, 2013.
- [27] Reuben P Keller, Juergen Geist, Jonathan M Jeschke & Ingolf Kühn, "Invasive species in Europe: ecology, status, and policy," *Environmental Sciences Europe*, Volume 23, Article number 23, June 2011
- [28] Jonathan M. Jeschke and Coworks, "Biological Invasions: Impact and Management," *Encyclopedia of Inland Waters (Second Edition)*, Volume 4, 2022, Pages 368-381
- [29] IUCN, "Environmental Impact Classification for Alien Taxa (EICAT)," Link: <https://www.iucn.org/resources/conservation-tool/environmental-impact-classification-alien-taxa-eicat>
- [30] N. Jubase, R. T. Shackleton, J. Measey, "Public Awareness and Perceptions of Invasive Alien Species in Small Towns," *Biology*, vol. 10, December 2021.



# بهینه‌سازی ماژول NTT در الگوریتم رمزنگاری پسا کوانتوم CrystalsKyber

محمد غفاری<sup>۱</sup>، حاتم عبدلی<sup>۲</sup>

<sup>۱</sup> دانشجوی کارشناسی ارشد مهندسی معماری سیستم‌های کامپیوتری  
mohammad.g7777@gmail.com

<sup>۲</sup> استادیار، گروه کامپیوتر، دانشکده مهندسی، دانشگاه بوعلی سینا، همدان  
abdoli@basu.ac.ir

## چکیده

با توجه به اینکه کامپیوترهای کوانتومی توان محاسباتی خیلی بیشتری نسبت به کامپیوترهای کلاسیک دارند، این مسئله باعث ایجاد چالش در حوزه رمزنگاری شده است، به طوری که پیش‌بینی می‌شود در سال‌های آتی کامپیوترهای کوانتومی به اندازه‌ای قدرتمند شوند که بتوانند الگوریتم‌های رمزنگاری کلید عمومی را بشکنند. به منظور حل این مشکل الگوریتم‌های رمزنگاری پسا کوانتوم مطرح شده و در حال تکامل هستند. یکی از الگوریتم‌های راه یافته به مراحل نهایی انتخاب الگوریتم‌های پسا کوانتوم، الگوریتم CRYSTALSKYBER است. یکی از ماجول‌های پیچیده این الگوریتم واحد NTT است که می‌توان با بهینه‌سازی آن زمان اجرای الگوریتم را کاهش داد. در این پژوهش، برای پیاده‌سازی واحد NTT که قبلاً با پایه دو صورت می‌گرفت، از پایه چهار استفاده شده است و این امر باعث کاهش زمان اجرا شده است. برای پیاده‌سازی NTT پایه چهار متناسب با Kyber لازم است تغییراتی در NTT رخ دهد، به طوری که در واحد حافظه روش پیشنهادی، تولید آدرس و همچنین تعداد ماجول‌های حافظه جهت خواندن و نوشتن همزمان تغییر کرده است. نتایج پیاده‌سازی روش پیشنهادی روی دو تراشه متفاوت FPGA با استفاده از نرم افزار Vivado نشان می‌دهد که در ازای افزایش جزیی منابع مورد نیاز، زمان اجرا در Artix7 در مقایسه با پیاده‌سازی‌های مشابه بیش از ۲۸ درصد کاهش یافته است.

**کلمات کلیدی:** رمزنگاری پسا کوانتوم، CrystalsKyber، NTT، پایه چهار، ضرب چند جمله ای، بهینه‌سازی سخت‌افزار.

## ۱ مقدمه

کامپیوترهای کوانتومی، کامپیوترهایی هستند که برای انجام محاسبات از خاصیت‌های فیزیک کوانتوم استفاده می‌کنند که این ویژگی باعث شده عملکرد خارق العاده‌ای نسبت کامپیوترهای کلاسیک که در حال حاضر استفاده می‌شوند، داشته باشند و این عملکرد شگفت‌انگیز باعث جلب توجه بسیاری شده است. در

کامپیوترهای کلاسیک از بیت استفاده می‌شود در حالی که کامپیوترهای کوانتومی مبتنی بر کیوبیت است [۱].

امروزه مؤسسات تحقیقاتی و شرکت‌های بزرگی مانند گوگل، IBM، NVIDIA و میکروسافت روی کامپیوترهای کوانتومی سرمایه‌گذاری کرده‌اند و IBM، Q System One و گوگل، Sycamore و USTC، Jiuzhang 2 را معرفی کرده‌اند. پیش‌بینی شده‌است که حدوداً تا سال ۲۰۳۰ کامپیوترهای کوانتومی به قدری قدرتمند می‌شوند که می‌توانند الگوریتم‌های رمزنگاری کلید عمومی را بشکنند [۱]، [۲]. برای حل این مشکل می‌بایست از الگوریتم‌هایی استفاده شود که در مقابل حملات کوانتومی مقاوم باشند. انجمن ملی استاندارد و تکنولوژی آمریکا (NIST) یک فراخوانی در رابطه با این موضوع در اواخر سال ۲۰۱۶ منتشر کرد و به این صورت الگوریتم‌های رمزنگاری پساکوانتوم (PQC)<sup>۱</sup> و امضای دیجیتال پساکوانتوم به وجود آمدند.

در دور سوم این رقابت، در سال ۲۰۲۰ چهار الگوریتم رمزنگاری کلید عمومی Saber، Classic، NTRU، McEliece و CRYSTALSKYBER به عنوان فینالیست پذیرفته شده‌اند و پنج الگوریتم Bike، FrodoKEM، NTRUprime، SIKE و HQC به عنوان الگوریتم‌های جایگزین در نظر گرفته شده‌اند. سه الگوریتم Saber، NTRU و CRYSTALSKYBER مبتنی بر lattice و الگوریتم Classic McEliece مبتنی بر کد هستند. همچنین سه الگوریتم امضای دیجیتال Rainbow، CRYSTALSDILITHIUM و Falcon به عنوان فینالیست پذیرفته شده‌اند و سه الگوریتم امضای دیجیتال GeMSS، Picnic و SPHINCS+ به عنوان الگوریتم امضای دیجیتال جایگزین انتخاب شده‌اند. دو الگوریتم امضای دیجیتال Rainbow و CRYSTALSDILITHIUM مبتنی بر lattice هستند و الگوریتم امضای دیجیتال Falcon مبتنی بر چندمتغیره است.

در پیاده‌سازی سخت افزاری الگوریتم‌های رمزنگاری پساکوانتوم به دو موضوع توجه شده است: ۱ زمان اجرا و ۲ منابع موردنیاز. به طور کلی برای بهبود پیاده‌سازی سخت‌افزاری الگوریتم‌های رمزنگاری پساکوانتوم از دو رویکرد اصلی استفاده می‌شود:

- بهبود کارایی بخش‌های پیچیده الگوریتم مانند بهینه‌سازی بخش ضرب چندجمله‌ای با استفاده از روش‌های حساب کامپیوتری
- استفاده از تکنیک‌های مختلف طراحی در سطح معماری کامپیوتر (مانند pipelining) با هدف افزایش کارایی سخت‌افزار الگوریتم

در کارهایی که تاکنون انجام شده‌است در بعضی از مقالات به چگونگی کاهش زمان اجرا توجه کرده‌اند، عده‌ای دیگر تمرکزشان بر کاهش منابع است و برخی به هر دو رویکرد توجه داشته‌اند. در این مقاله با اعمال تغییراتی در واحد NTT، به عنوان یکی از بخش‌های پیچیده الگوریتم Kyber، بهبود زمان اجرای الگوریتم Kyber حاصل شده است که جزییات این تغییرات در ادامه مقاله توضیح داده شده‌است.

<sup>1</sup>Post Quantum Cryptography

## ۱.۱ آشنایی با Kyber

Kyber یک سازوکار کیسوله‌سازی کلید (KEM) است که امنیت آن براساس سختی حل کردن مسئله یادگیری با خطا در lattice است [۳]. ساختار Kyber از دو نوع پیروی می‌کند، یکی CPA و دیگری CCA است. CPA نوعی حمله است که در آن فرد مهاجم هم به متن رمز شده و هم به متن آشکار دسترسی دارد و سعی می‌کند که متوجه شود که متن چگونه رمز شده است و CCA نوعی حمله است که فرد مهاجم می‌تواند با متن رمز شده انتخابی به متن آشکار دست پیدا کند. برای نمایش حلقه چندجمله‌ای  $Z[X]/(Xn + 1)$  از  $R$  و برای نمایش حلقه  $Zq[X]/(Xn + 1)$  از  $Rq$  استفاده می‌شود و به طوری که  $n = 256$ ،  $n' = 9$  و  $q = 3329$  است. از حروف بزرگ برای نشان دادن ماتریس‌ها و حروف کوچک برای نشان دادن بردارهایی با ضرایبی در  $R$  و  $Rq$  استفاده می‌شود. در ادامه با اجزای Kyber آشنا می‌شویم.

## ۲.۱ آشنایی با NTT

NTT شباهت‌هایی با FFT دارد؛ پیچیدگی محاسباتی NTT برابر با  $O(n \log n)$  است در حالی که پیچیدگی محاسباتی  $FFT$  برابر  $O(n^2)$  است و از  $N$  امین ریشه واحد  $\omega$  استفاده می‌شود و  $N$  توانی از دو است. می‌توان گفت NTT روشی بهینه برای ضرب است.

$$A_i = NTT(a_i) = \int_{j=0}^{N-1} a_j \omega_N^{ij} \pmod{q} \quad i = 0, 1, 2, \dots, N-1 \quad (1)$$

برای به دست آوردن INTT کافی است، عبارت در  $1/N$  ضرب شود و به جای  $\omega$ ، از  $\omega^{-1}$  استفاده شود.

$$a_j = INTT(A_j) = \frac{1}{N} \int_{i=0}^{N-1} A_i \omega_N^{-ij} \pmod{q} \quad j = 0, 1, 2, \dots, N-1 \quad (2)$$

میزان خطا از توزیع دوجمله‌ای متمرکز  $B\eta$  (CBD) نمونه‌برداری می‌شود و  $f$  به عنوان خروجی طبق  $B\eta$  نمونه‌برداری می‌شود. در Kyber نمونه‌برداری به ازای  $\eta = 2$  یا  $\eta = 3$  انجام می‌شود. در الگوریتم Kyber تعدادی تابع درهم‌سازی وجود دارد مانند SHAKE128, 256 و SHA3256, 512 که مبنای این توابع الگوریتم Keccak می‌باشد که وظیفه آن درهم‌سازی دیتا است و این باعث می‌شود که دیتا غیرقابل تشخیص باشد. در جدول ۱ مجموعه پارامترهای الگوریتم Kyber نشان داده شده است.

ساختار این مقاله به این صورت است که در بخش بعدی پیشینه پژوهش بررسی می‌شود؛ در بخش ۳ روش پیشنهادی بیان می‌شود و سپس در بخش ۴ نتایج حاصل از پیاده‌سازی روش پیشنهادی مورد مقایسه و ارزیابی قرار می‌گیرد. در نهایت بخش ۵ شامل جمع‌بندی و نتیجه‌گیری است.

## ۲ پیشینه پژوهش

تاکنون بهینه‌سازی‌های بسیاری برای Kyber ارائه شده است که در ادامه برخی از موارد که با NTT مرتبط هستند را ذکر می‌کنیم. در [۴] و [۵] برای کاهش منابع مورد نیاز از واحد پروانه یک‌پارچه شده استفاده شده

جدول ۱: مجموعه پارامترها برای الگوریتم Kyber

Algorithm	Level	Parameters ( $n/k/q$ )	Public key/ Secret key/ Cipher- text size $p/s/c$ (in Bytes)
Kyber512	۱	۲۵۶/۲/۳۳۲۹	۸۰۰/۱۶۳۲/۷۳۶
Kyber768	۳	۲۵۶/۳/۳۳۲۹	۱۱۸۴/۲۴۰۰/۱۰۸۸
Kyber1024	۵	۲۵۶/۴/۳۳۲۹	۱۵۶۸/۳۱۶۸/۱۵۶۸

است که کار واحد پروانه CT و GS را انجام می‌دهد. در [۶]، [۷] و [۵] با اعمال تغییراتی در modular reduction توانستند طراحی خود را بهبود ببخشند. برای مثال در [۶] از Modified Barrett Reduction استفاده شده است، در [۷] با استفاده از عملیات منطقی AND، OR و XOR و تغییر جایگاه بیت‌ها توانستند واحد modular reduction را بهبود دهند و در [۵] از Montgomery Reduction استفاده شده است. در [۴] و [۵] با افزایش تعداد واحد پروانه توانستند زمان اجرا را کاهش دهند. در [۵] از ویژگی قابلیت پیکربندی در زمان اجرا یا (RTC) استفاده شده است که موجب انعطاف‌پذیری طراحی شده است.

در [۷] و [۸] برای بهبود عملکرد، تغییراتی را در حافظه اعمال کردند. در [۸] پهنای باند حافظه را دو برابر کردند تا مشکل دسترسی به RAM حل شود و تغییر در الگوی دسترسی به حافظه باعث افزایش سرعت و بهره‌وری شده است و در [۷] برای اطمینان از ذخیره داده و افزایش سرعت از شانزده بلوک SRAM استفاده کردند.

در [۶] و [۹] برای پیاده‌سازی NTT از DIT و برای پیاده‌سازی INTT از DIF استفاده شده است. در [۸] NTT را طراحی کرده‌اند که از مبنای چهار استفاده می‌کند و حافظه‌ی آن بدون برخورد<sup>۲</sup> است و از روش‌هایی استفاده کردند که تعداد حافظه موردنیاز آن کم بود.

در مقالاتی که اولویت کاهش منابع بوده زمان اجرای آنها نسبتاً طولانی بوده و در مقالاتی که اولویت کاهش زمان اجرا بوده و برای کاهش زمان اجرا تعداد زیادی واحد پروانه اضافه کرده‌اند، به منابع خیلی بیشتری احتیاج داشته‌اند. در روش پیشنهادی می‌خواهیم یک NTT مبنای چهار که برای Kyber مناسب‌سازی شده است را به گونه‌ای بهینه کنیم که زمان اجرای کمی داشته باشد و در عین حال به منابع خیلی زیادی احتیاج نداشته باشد.

## ۳ روش پیشنهادی

تاکنون در پیاده‌سازی‌هایی که برای الگوریتم‌های پساکوانتوم انجام شده است از NTT مبنای دو استفاده شده است، یعنی دو ضریب وارد شده، محاسبات آن انجام شده و سپس خارج می‌شوند. حال اگر بتوان در NTT از مبنای چهار استفاده کرد، عملکرد NTT به‌طور محسوسی بهبود می‌یابد، که برای تحقق آن لازم است

<sup>2</sup>Conflict



تغییراتی در NTT رخ دهد.

در این معماری، باید به طول دیتا و تعداد واحدهای پروانه توجه کنیم و همین طور باید بررسی شود که آیا در حافظه ممکن است با برخوردی در حافظه روبه‌رو شویم، چون باید مطمئن شد که دیتا به موقع فراخوانی و در زمان و جای مناسب ذخیره می‌شود.

در طراحی‌های گذشته چون براساس مبنای دو بودند واحد تولید آدرس<sup>۳</sup>، دو آدرس را تولید می‌کرد و حافظه هم دو ضریب را می‌خواند یا می‌نوشت که برای مبنای چهار مناسب نبودند، پس در کد تغییراتی انجام شد، که این واحد با مبنای چهار سازگار باشند. با داشتن NTT مبنای چهار می‌توان انتظار داشت که عملکرد و زمان اجرای الگوریتم Kyber بهبود یابد چون حداقل، زمان اجرای NTT کاهش می‌یابد. پیش‌تر FFT مبنای چهار طراحی شده بود و این تغییر مبنای تأثیر زیادی بر عملکرد داشت [۱۰]، [۱۱]. FFT و NTT هم شباهت‌هایی نسبت به هم دارند، در [۸] نحوه‌ی محاسبات NTT مبنای چهار توضیح داده شده است. برای اجرای NTT از DIT و برای INTT از DIF استفاده می‌شود. در ادامه نحوه‌ی تبدیل DIT و DIF معمولی به DIT و DIF مبنای چهار توضیح داده می‌شود. فرمول NTT که با پیش‌پردازش<sup>۴</sup> ترکیب شده است به‌صورت زیر است:

$$A_i = \sum_{j=0}^{N-1} a_j \phi_{\sqrt{N}}^j \omega_N^{ij} \quad \text{mod } q \quad i = 0, 1, 2, \dots, N-1 \quad (3)$$

عبارت بالا را به چهار قسمت برابر تبدیل می‌کنیم:

$$A_i = \sum_{j=0}^{\frac{N}{4}-1} a_{4j} \phi_{\sqrt{N}}^{4j} \omega_N^{i \cdot (4j)} + \sum_{j=0}^{\frac{N}{4}-1} a_{4j+1} \phi_{\sqrt{N}}^{4j+1} \omega_N^{i \cdot (4j+1)} + \quad (4)$$

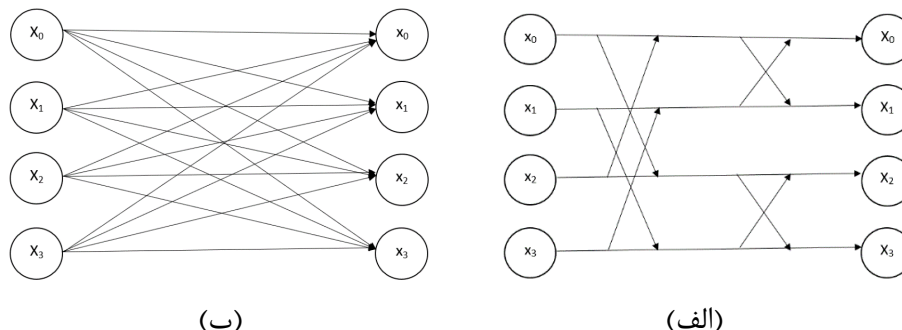
$$\sum_{j=0}^{\frac{N}{4}-1} a_{4j+2} \phi_{\sqrt{N}}^{4j+2} \omega_N^{i \cdot (4j+2)} + \sum_{j=0}^{\frac{N}{4}-1} a_{4j+3} \phi_{\sqrt{N}}^{4j+3} \omega_N^{i \cdot (4j+3)} \quad \text{mod } q \quad i = 0, 1, 2, \dots, N-1$$

در ادامه twiddle factor های  $\omega$  و  $\phi$  را ساده می‌کنیم. برای پیاده‌سازی واحد پروانه به‌طور معمول از مبنای ۲ استفاده می‌شود شکل ۱ (الف) نحوه محاسبات در مبنای ۲ را نشان می‌دهد. با استفاده از روش‌هایی می‌توان تعداد ضرب، تفریق و جمع را کاهش داد. شکل ۱ (ب) نمایی از واحد پروانه چهار نقطه‌ای در مبنای ۴ را نشان می‌دهد. همان‌طور که مشخص است محاسبات در مثال چهار نقطه‌ای، در مبنای ۴ در یک مرحله انجام می‌شود ولی در مبنای ۲، در دو مرحله انجام می‌شود که این موضوع نشان می‌دهد که استفاده از مبنای ۴ می‌تواند باعث کاهش زمان شود.

اگر به صورت مستقیم معادلات NTT مبنای ۴ را محاسبه کنیم، به پنج ضرب، شش تفریق و شش جمع نیاز داریم ولی می‌توان مقادیر را دوباره استفاده کرد که با استفاده از این روش به چهار ضرب، چهار تفریق و چهار جمع نیاز داریم.

<sup>3</sup>Address generator

<sup>4</sup>Preprocessing



شکل ۱: نحوه محاسبات ماجول NTT: (الف) مبنای ۲ و (ب) مبنای ۴

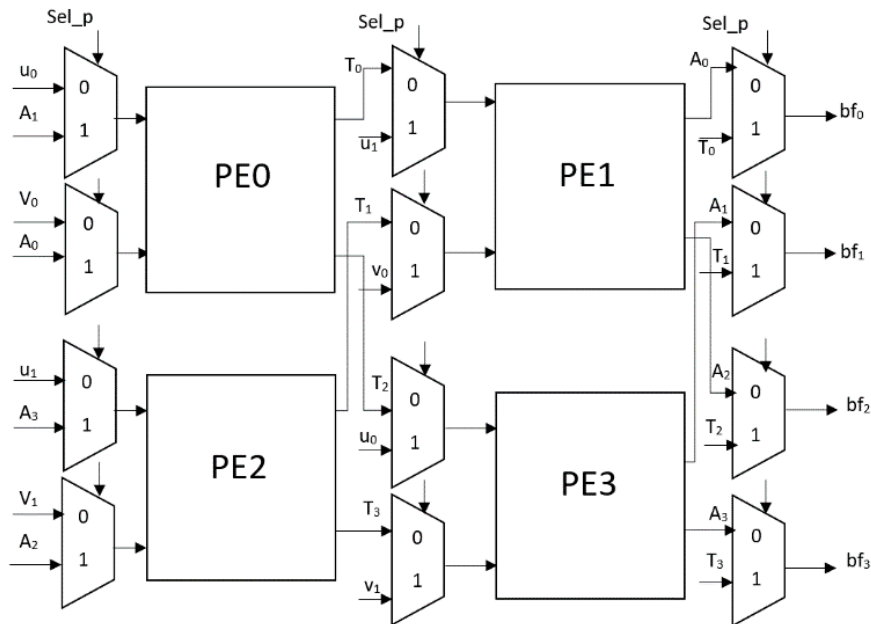
در شکل ۲ از چهار PE<sup>۵</sup> یا عنصر پردازشی استفاده شده است، هنگامی که sel\_p یک باشد، دیتای مرتبط به  $A_i$  را فراخوانی می کند و محاسبات آن در ستون اول PEها انجام می شود و مقادیر میانی تولید می شود و در ادامه، محاسبات در PE های ستون دوم انجام می شود و در نهایت مقدار خروجی مشخص می شود. زمانی که sel\_p صفر باشد، از دیتای جایگزین استفاده می شود.

به منظور جلوگیری از هرگونه مشکل احتمالی و بالا بردن سرعت در خواندن و نوشتن از هشت حافظه RAM استفاده شده که چهارتا از آنها برای خواندن و چهارتای دیگر برای نوشتن به کار گرفته شده اند که این موضوع باعث تغییراتی در بخش آدرس دهی شده است. شکل ۳ ساختار حافظه را نشان می دهد. در پیاده سازی Kyber به صورت مستقیم نمی توان از NTT مبنای چهار استفاده کرد و NTT مبنای چهار نیاز به تغییراتی دارد تا به گونه ای شود که برای پیاده سازی الگوریتم Kyber مناسب باشد. به طور مثال مقدار  $n$  و  $q$  باید تغییر کنند، مقدار  $n$  برابر با ۲۵۶ باشد و مقدار  $q$  برابر با ۳۳۲۹ باشد.

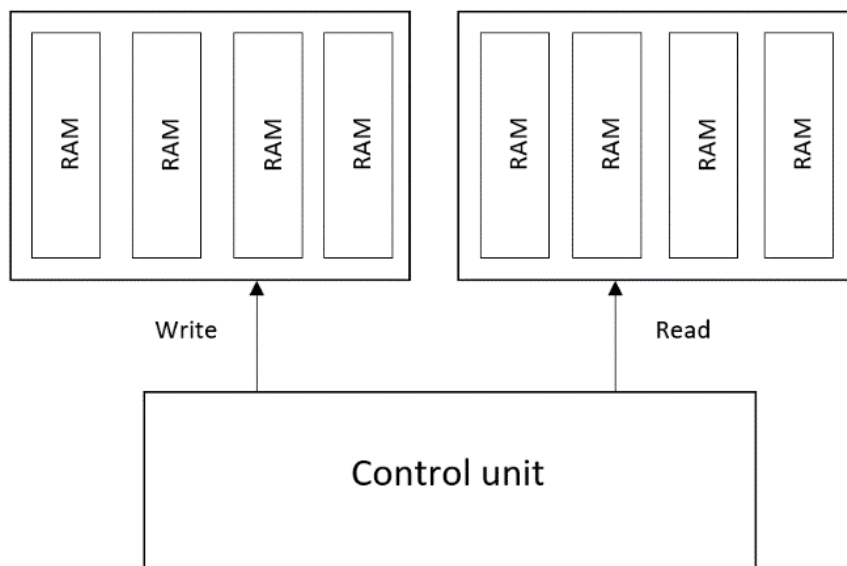
## ۴ ارزیابی نتایج پیاده سازی

با استفاده از روش پیشنهادی، NTT مبنای چهار مورد نظر را روی FPGA های Artix-7 (xc7a200tffg11563) و Virtex-7 (xc7vx690tffg17612) توسط Vivado 2019.1 پیاده سازی شده است. نتایج به دست آمده طبق گزارشهای Vivado می باشد و کد روی FPGAها پروگرام نشده است. واحد پروانه را به صورت جداگانه روی Artix-7 و Virtex7 پیاده سازی کرده ایم که طبق گزارشهای به دست آمده روی Artix-7 به ۶۷۶ فلیپ فلاپ، ۱۱۳۲ LUT و ۴ DSP روی فرکانس ۱۸۵/۱۸ مگاهرتز نیاز است و توان مصرفی آن ۰/۲۷۱ وات می باشد و روی Virtex-7 به ۶۷۶ فلیپ فلاپ، ۱۱۵۶ LUT و ۴ DSP روی فرکانس ۲۳۴/۷۴ مگاهرتز نیاز است و توان مصرفی آن ۰/۵۰۲ وات می باشد. در شکل ۴ زمان اجرای روش پیشنهادی با سایر پیاده سازیها روی Artix-7 مشابه، مقایسه شده است و همان طور که دیده می شود پیاده سازی روش پیشنهادی ما توانسته زمان خوبی را ثبت کند و زمان اجرای ۱/۱۳۴ میکرو ثانیه

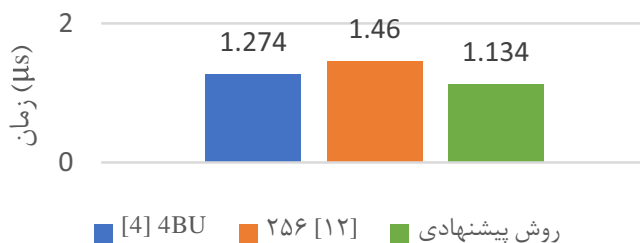
<sup>5</sup>Processing element



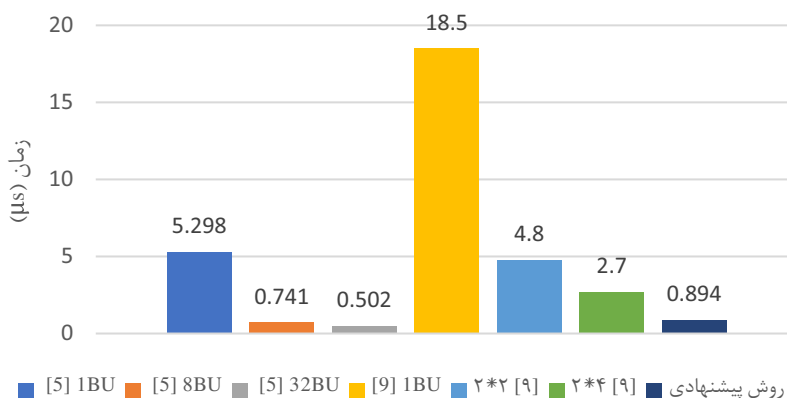
شکل ۲: ساختار مسیره‌دهی در مبنای چهار



شکل ۳: ساختار حافظه در روش پیشنهادی



شکل ۴: مقایسه پیاده‌سازی‌ها روی Artix-7



شکل ۵: مقایسه پیاده‌سازی‌ها روی Virtex-7

است (منظور از BU واحد پروانه می‌باشد).

زمان اجرای روش پیشنهادی روی Artix7 نسبت به [۴] 4 BU ۱۲/۳۴ درصد سریع‌تر و نسبت به [۱۲] ۲۵۶ ۲۸/۷۴ درصد سریع‌تر و نسبت به [۴] 4 BU ۱۲/۳۴ درصد سریع‌تر است. در شکل ۵ زمان اجرای روش پیشنهادی با سایر پیاده‌سازی‌ها روی Virtex-7 مقایسه شده است که توانسته سریع‌تر از اکثر پیاده‌سازی‌ها باشد. با توجه به اینکه پیاده‌سازی مشابهی برای Virtex-7 وجود نداشت، بناچار روش پیشنهادی با همه پیاده‌سازی‌های روی Virtex-7 مقایسه شده است.

زمان اجرای روش پیشنهادی روی Virtex-7 نسبت به [۹] 4\*2 ۳/۰۲ برابر سریع‌تر، نسبت به [۹] 2\*2 ۵/۳۶ برابر سریع‌تر، نسبت به [۹] 1 BU ۲۰/۶۹ برابر سریع‌تر، نسبت به [۵] 32 BU ۱/۷۸ برابر کندتر، نسبت به [۵] 8 BU ۱/۲ برابر کندتر و نسبت به [۵] 1 BU ۵/۹۲ برابر سریع‌تر است.

پیاده‌سازی‌های گوناگونی برای NTT وجود دارد برخی از آنها از طراحی همزمان سخت‌افزار/ نرم‌افزار استفاده کرده‌اند و برخی از طراحی تمام سخت‌افزاری یا برخی از پیاده‌سازی‌ها از تعداد واحد پروانه بیشتری

جدول ۲: مقایسه نتایج پیاده سازی روی Artix-7

Design	n	BU	LUTs	FFs	DSPs	BRAMs	Freq. (MHz)	NTT (CCs)	INTT (CCs)	Time ( $\mu$ s)
[۴]	۲۵۶	۴	۲۵۴۳	۷۹۲	۴	۹	۱۸۲	۲۳۲	۲۳۳	۲۷۴.۱
[۱۲]	۲۵۶	۲*۲	۸۰۱	۷۱۷	۴	۲	۲۲۲	۳۲۴	۳۲۴	۴۶.۱
روش پیشنهادی	۲۵۶	۲*۲	۲۳۰۱	۹۲۵	۴	۹	۱۸.۱۸۵	۲۱۰	۲۱۰	۱۳۴.۱

استفاده کرده‌اند یا در مواردی مقدار  $n$  متفاوت بوده است (معمولاً مقدار  $n = ۲۵۶$  است) که همه‌ی موارد بالا روی سرعت و منابع موردنیاز اثرگذار می‌باشد ولی در جدول ۲ پیاده‌سازی‌های مشابه با روش پیشنهادی روی Artix-7 مقایسه شده‌اند. با مقایسه نتایج، می‌توان متوجه شد که روش پیشنهادی توانسته بهترین زمان اجرا را ثبت کند ولی در مقایسه با [۱۲]، روش پیشنهادی به منابع بیشتری نیاز دارد به طوری که  $۲/۸۷$  برابر LUT بیشتر،  $۱/۲۹$  برابر فلیپ فلاپ بیشتر،  $۴/۵$  برابر BRAM بیشتر نیاز دارد و روش پیشنهادی در مقایسه با [۴] به LUT کمتر و فلیپ فلاپ بیشتر نیاز دارد.

## ۵ نتیجه‌گیری

به علت قدرت بالای محاسباتی کامپیوترهای کوانتومی، در آینده این کامپیوترها می‌توانند الگوریتم‌های رمزنگاری کلید عمومی فعلی را بشکنند؛ برای مقابله با این موضوع الگوریتم‌های رمزنگاری پساکوانتوم به وجود آمدند. پیاده‌سازی الگوریتم‌های رمزنگاری پساکوانتوم با چالش‌های مختلفی، همچون منابع مورد نیاز و زمان اجرا روبه‌رو بودند و هستند، برای حل این چالش‌ها روش‌های مختلفی پیشنهاد شده‌است. یکی از پیچیده‌ترین و پرهزینه‌ترین ماجول‌های محاسباتی الگوریتم Kyber ماجول NTT است و در روش پیشنهادی از مینای محاسبه NTT از ۲ به مینای ۴ تغییر کرده که باعث تغییرات در سایر قسمت‌های NTT شده است و توانسته زمان اجرا کوتاهی در مقایسه با سایر پیاده‌سازی‌ها داشته‌باشد درحالی‌که به منابع موردنیاز متعادلی نیاز دارد. روش پیشنهادی با تغییر مینا در NTT توانست زمان اجرا را بهبود دهد و در مقایسه با پیاده‌سازی‌های مشابه توانست  $۲۸/۷۴$  درصد زمان اجرای کوتاه‌تری را ثبت کند.

## مراجع

- [1] F. Farahmand, D. T. Nguyen, V. B. Dang, A. Ferozpuri and K. Gaj, "Software/Hardware Codesign of the Post Quantum Cryptography Algorithm NTRUEncrypt Using High-Level Synthesis and Register-Transfer Level Design Methodologies," *2019 29th International Conference on Field Programmable Logic and Applications (FPL)*, 2019, pp. 225-231, doi: 10.1109/FPL.2019.00042.
- [2] J. Xie, K. Basu, K. Gaj and U. Guin, "Special Session: The Recent Advance in Hardware Implementation of Post-Quantum Cryptography," *2020 IEEE 38th VLSI Test Symposium (VTS)*, 2020, pp. 1-10, doi: 10.1109/VTS48691.2020.9107585.

- [3] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J.M. Schanck, P. Schwabe, G. Seiler and D. Stehlé, “CRYSTALS-Kyber algorithm specifications and supporting documentation,” 2017, NIST PQC Round 2, vol. 9, pp. 11.
- [4] F. Yaman, A. C. Mert, E. Öztürk and E. Savaş, “A Hardware Accelerator for Polynomial Multiplication Operation of CRYSTALS-KYBER PQC Scheme,” *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2021, pp. 1020-1025, doi: 10.23919/DATE51398.2021.9474139.
- [5] K. Derya, A.C. Mert, E. Öztürk and E. Savaş, “CoHA-NTT: A Configurable Hardware Accelerator for NTT-based Polynomial Multiplication,” *Microprocessors and Microsystems*, 2022, vol. 89, p.104451.
- [6] Y. Xing and S. Li, “A Compact Hardware Implementation of CCA-Secure Key Exchange Mechanism CRYSTALS-KYBER on FPGA,” *TCHES*, vol. 2021, no. 2, pp. 328–356, Feb. 2021.
- [7] W. Guo, S. Li and L. Kong, “An Efficient Implementation of KYBER,” in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 3, pp. 1562-1566, March 2022, doi: 10.1109/TCSII.2021.3103184.
- [8] C. Zhang *et al.*, “Towards Efficient Hardware Implementation of NTT for Kyber on FPGAs,” *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2021, pp. 1-5, doi: 10.1109/ISCAS51556.2021.9401170.
- [9] X. Chen, B. Yang, S. Yin, S. Wei, and L. Liu, “CFNTT: Scalable Radix-2/4 NTT Multiplication Architecture with an Efficient Conflict-free Memory Mapping Scheme”, *TCHES*, vol. 2022, no. 1, pp. 94–126, Nov. 2021.
- [10] M. Garrido, J. Grajal, M. A. Sanchez and O. Gustafsson, “Pipelined Radix-2k Feedforward FFT Architectures,” in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 1, pp. 23-32, Jan. 2013.
- [11] E. E. Swartzlander, W. K. W. Young and S. J. Joseph, “A radix 4 delay commutator for fast Fourier transform processor implementation,” in *IEEE Journal of Solid-State Circuits*, vol. 19, no. 5, pp. 702-709, Oct. 1984, doi: 10.1109/JSSC.1984.1052211.
- [12] M. Bisheh-Niasar, R. Azarderakhsh and M. Mozaffari-Kermani, “High-Speed NTT-based Polynomial Multiplication Accelerator for Post-Quantum Cryptography,” *2021 IEEE 28th Symposium on Computer Arithmetic (ARITH)*, 2021, pp. 94-101.



## دیپلماسی سایبری؛ توئیپلماسی ایالات متحده آمریکا

فریده محمدعلی پور<sup>۱</sup>، محمدرضا نوروزپور<sup>۲</sup>

<sup>۱</sup> استادیار گروه روابط بین الملل دانشگاه خوارزمی  
fm.alipour@khu.ac.ir

<sup>۲</sup> دکترای روابط بین الملل دانشگاه خوارزمی  
noroozpoor@gmail.com

### چکیده

رشد و گسترش چشمگیر فناوری‌های اطلاعاتی و ارتباطی و شبکه‌های اجتماعی در سراسر جهان، سبب تسهیل و تسریع ارتباطات دوسویه و چند سویه شده است. استفاده از این ظرفیت در برقرار کردن ارتباط مستقیم و سریع با میلیون‌ها مخاطب و جمع‌آوری اطلاعات از تعاملات رایج در شبکه‌های اجتماعی، از جمله توئیتر، در دستور کار دولت‌ها قرار گرفته است که به آن «دیپلماسی سایبری» می‌گویند. توئیتر در شبکه‌های اجتماعی از لحاظ سرعت دسترسی، انتشار سریع اطلاعات و محدودیت به کارگیری واژگان از اهمیت و جایگاه ویژه‌ای برخوردار شده است و همین موضوع سبب شده است که از این شبکه اجتماعی برای پیشبرد اهداف سیاست خارجی استفاده شود که «توئیپلماسی» نامیده می‌شود. سؤال اساسی در این است که جایگاه توئیپلماسی در سیاست خارجی آمریکا چیست؟ نتایج پژوهش نشان می‌دهد که دستگاه سیاست خارجی آمریکا توانسته است قدرت فضای سایبری را به منزله مصداق بارز قدرت هوشمند به خدمت گیرد و در کشورهای هدف تأثیرگذار باشد. همچنین استفاده وسیع وزارت خارجه آمریکا از دیپلماسی دیجیتال و توئیپلماسی در سراسر جهان سبب شده است تا دیپلمات‌های این کشور بتوانند با انبوهی از مخاطبان خود مستقیماً ارتباط برقرار کنند و از قابلیت‌های شبکه‌های اجتماعی برای تعقیب منافع خود به خوبی بهره‌گیرند.

**کلمات کلیدی:** دیپلماسی سایبری، دیپلماسی توئیتری، توئیپلماسی، شبکه‌های اجتماعی، سیاست خارجی آمریکا.

## ۱ مقدمه

واژه سایبر از لغت یونانی Kybernetes به معنی سکان‌دار یا راهنما مشتق شده است. نخستین بار اصطلاح «سایبرنتیک» را ریاضی‌دانی به نام نوربرت وینر در کتابی با عنوان سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین در سال ۱۹۸۴ به کاربرد. فضای سایبر در معنا به مجموعه‌هایی از ارتباطات درونی انسان‌ها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود [۹].

در سال ۱۹۸۴ ویلیام گیبسون واژه «فضای سایبری» را در یک رمان علمی - تخیلی به نام نورومانسر رونمایی کرد. از آن پس استفاده از پیشوند «سایبر» به موازات رشد و توسعه اینترنت استفاده شد. در اواخر دهه ۱۹۹۰ تقریباً هر آنچه به اینترنت مربوط می‌شد یک پیشوند «سایبر» با خود همراه داشت. واژگان «اجتماع سایبر»، «امنیت سایبر»، «قانون سایبر»، «جنایت سایبر» همگی از این نوع عبارات ساخته شده با استفاده از پیشوند «سایبر» هستند که خواننده را متوجه ارتباط موضوع اصلی با فضای سایبری می‌کنند.

در اوایل قرن بیستم، به تدریج واژه «سایبر» مهجور شد و از ادبیات رایج عمومی کنار رفت، اما در ادبیات تخصصی مرتبط با امنیت و جنگ باقی ماند. از این سال‌ها به تدریج ادبیات تخصصی درباره «امنیت سایبری» و «جنگ سایبری» تقویت شد. شاید یکی از دلایل اصلی آن، رشد چشمگیر «جنایت سایبری» در سراسر جهان بود؛ به طوری که تا سال ۲۰۱۳ از هر سه نفری که در دنیا به اینترنت دسترسی داشتند، یک نفر قربانی «جنایت سایبری» شده است [۱۰].

از آغاز قرن بیست و یکم و شدت گرفتن استفاده گروه‌های تروریستی از اینترنت و پیدایش «تروریسم سایبری» سبب شد تا واژه «سایبر» بیش از گذشته به موضوعات امنیتی و جنگ و صلح مرتبط شود. در سال ۲۰۰۱ شورای اروپا «کنوانسیون جنایت سایبری» را منعقد ساخت. این کنوانسیون در رواج این واژه در ادبیات دانشگاهی و ادبیات روابط بین‌الملل تأثیرگذار بوده است. امروزه بسیاری از کشورها «استراتژی‌های امنیت سایبری» خاص خود را اعلام کرده‌اند. اتحادیه بین‌المللی ارتباطات راه دور «برنامه جهانی امنیت سایبری» خود را دارد و پیمان آتلانتیک شمالی (ناتو) نیز برای خود «سیاست‌های دفاع سایبری» تدوین کرده است. بنا به تعریف کلار، دیپلماسی سایبری به آن دسته از تکنیک‌ها و فنونی اطلاق می‌شود که دستگاه سیاست خارجی هر کشور به منظور کنترل خطرات و تهدیداتی که اینترنت می‌تواند متوجه منافع ملی کشورش کند و قوف داشته باشد. دیپلماسی سایبری مکانیسم رویارویی با تهدیدهای امنیتی، نفوذ هکرها، جلوگیری از وقوع جنگ سایبری یا کنترل آن در صورت وقوع، یا هرگونه عمل متقابل در مورد دشمن و عامل نفوذکننده علیه منافع ملی است [۱۱].

دیپلماسی در طول تاریخ تکامل یافته است و با الزامات ملت‌ها، شخصیت رهبران، درگیری‌ها، ائتلاف‌ها و تغییرات پارادایمی منطبق شده است. با وجود این، مهارت‌های مورد نیاز برای انجام دادن مأموریت دیپلمات‌ها، به طور قابل توجهی به همان صورت باقی مانده است. در این زمینه، تغییری اساسی در نحوه تعامل افراد و جوامع، به شدت در هنر دیپلماسی تأثیر گذاشته است. رسانه‌های اجتماعی در فضای سایبری نه تنها نوع جدیدی از رابطه را در سطحی شخصی ایجاد کرده‌اند، بلکه راه جدیدی را برای رسیدن به مخاطبان گسترده‌تر پدید می‌آورند. بنابراین دیپلماسی سایبری و ابزارهای آن مانند توئیپلماسی، پی‌آمد طبیعی تکامل ارتباطات در قرن بیست و یکم است. در این میان، قدرت‌های بزرگ از این ابزارها به خوبی بهره برده‌اند. پژوهش حاضر به این سؤال پاسخ می‌دهد که جایگاه توئیپلماسی در سیاست خارجی آمریکا چیست؟ برای این منظور ابتدا با مروری بر ادبیات پژوهش، به تشریح دیپلماسی سایبری و قدرت‌سازی در شبکه‌های اجتماعی پرداخته می‌شود و سپس توئیپلماسی و اهمیت شبکه‌های اجتماعی در سیاست داخلی آمریکا بررسی می‌گردد.

## ۲ ادبیات پژوهش

واژه دیپلماسی سایبری دیرزمانی نیست که وارد ادبیات روابط بین‌الملل و علوم سیاسی شده است. برخی از واژه «دیپلماسی دیجیتال» که بار معنایی مشابهی دارد برای اشاره به این حوزه استفاده می‌کنند بنابراین در پیشینه به آثار با هر دو عنوان اشاره می‌شود. در زبان فارسی نخستین کتابی که در این حوزه منتشر شده «دیپلماسی دیجیتال (نظریه و عمل)» [۱] نام دارد. این کتاب ممزوجی از تبیین وضعیت، نظریه پردازی و ارائه نمونه است و دیپلماسی دیجیتال را به منزله تغییر مدیریت در سیاست‌های بین‌المللی مورد بررسی قرار داده است. در کتاب «دیجیتالی شدن دیپلماسی عمومی» [۲]. مولف اذعان می‌دارد این نوع دیپلماسی دارای فرایندی طولی‌المدت است که در آن بازتعریف هنجارها، ارزش‌ها، روال‌ها و اهداف دیپلماسی عمومی انجام می‌شود. نویسنده، محقق دانشگاه آکسفورد است که چگونگی بهره‌گیری از دیپلماسی دیجیتال در بحران را موضوع مطالعه خود قرار داده است. کتاب «حکمرانی در عرصه پنجم: گذار به دیپلماسی سایبری» [۳] تنها کتابی است که در عنوان خود با موضوع پژوهش حاضر اشتراک دارد. این کتاب با طرح چالش‌های سیاست‌گذاری و دستور کار روابط سایبری بین‌المللی، کشورهای بازیگر جهانی و نهادهای بین‌المللی را توضیح می‌دهد. این کتاب برای مطالعه اقدامات بازیگران خاص در این عرصه، آمریکا، چین، روسیه، ژاپن، اتحادیه اروپا، مالزی و دیپلماسی شرکتی مفید است. تنها مقالات فارسی با عنوان دیپلماسی سایبری نیز به روسیه و آمریکا اختصاص دارند در زبان انگلیسی منابع متعددی منتشر شده‌اند که از دسترسی مخاطب ناآشنا به این زبان خارج هستند. از این رو پژوهش حاضر می‌تواند بخشی از خلأ ادبیات را در این حوزه رفع کند.

## ۳ دیپلماسی سایبری و قدرت‌سازی در شبکه‌های اجتماعی

واژه دیپلماسی در اصل از فعل یونانی دیپلم گرفته شده که به معنای «تاکردن» است. کلمه دیپلماسی نیز از همین فعل مشتق شده و حاکی از نوشته یا طومار ماندنی است که به هرکسی اعطا می‌شد، از امتیازات خاصی برخوردار می‌شد [۴]. دیپلماسی، دربرگیرنده مجموع اقداماتی است که از برنامه‌ریزی تا اجرای سیاست خارجی کشورها در عرصه جهانی را دربرمی‌گیرد. دیپلماسی سایبری به این اقدامات در فضای سایبر اشاره دارد.

دیپلماسی سایبری از وجوه قدرت سایبری و مبتنی بر کنترل ارتباطات و اطلاعات در فضای سایبر است. از منظر کاستلز، صاحب‌نظر عرصه ارتباطات، «قدرت در وهله اول از طریق معناسازی در ذهن انسان و به کمک فرایندهای ارتباطی اعمال می‌گردد که در شبکه‌های چندرسانه‌ای جهانی یا محلی با رویکرد ارتباط جمعی، از جمله ارتباط جمعی خود انگیز اجرایی می‌شوند» [۵]. «با نفوذ روزافزون اینترنت، شکل جدیدی از ارتباطات تعاملی پدید آمده است و به این ترتیب ظرفیت ارسال پیام‌های چند به چند، در زمان حال یا زمانی انتخاب شده و با امکان استفاده از ارتباطات نقطه به نقطه، پخش محدود یا گسترده، با توجه به اهداف و ویژگی‌های معطوف به کنش ارتباطی در نظر گرفته شده، مشخص می‌شوند. این شکل تازه ارتباطات را به لحاظ تاریخی ارتباطات جمعی خودانگیز می‌نامم» [۶].

کاستلز با بیان این که قدرت در جامعه شبکه‌ای از طریق شبکه‌ها جریان می‌یابد چهار شکل از قدرت را

در این اوضاع فناورانه و اجتماعی ارائه می‌دهد: قدرت شبکه‌بندی<sup>۱</sup>، قدرت شبکه‌ای<sup>۲</sup>، قدرت شبکه‌ای شده<sup>۳</sup> و قدرت شبکه‌سازی<sup>۴</sup>. کاستلز بر اهمیت برنامه‌ریزان در جامعه شبکه‌ای مبتنی بر ارتباطات جمعی چندرسانه‌ای تأکید می‌کند [۷]. دولت‌ها با در اختیار داشتن هر چهار نوع قدرت، امکانات گسترده‌ای برای دیپلماسی سایبری و پیشبرد منافع خود در اختیار دارند. در دیپلماسی سایبری، حوزه فعالیت دیپلمات‌ها به درون وزارت خارجه، سفارت‌خانه، کشور محل مأموریت و نهادهای بین‌المللی محدود نمی‌شود. سرعت در تصمیم‌گیری و اقدام از مشخصات بارز این دیپلماسی است. در این دیپلماسی مخاطبان به مقامات، دیپلمات‌های دیگر، صاحبان جراید و رسانه‌ها و گروه‌های ذی‌نفوذ محدود نمی‌گردد، بلکه هر فرد یا گروهی از هر نقطه جهان در حوزه اقدام دیپلمات قرار می‌گیرد [۸]. استفاده از ظرفیت فضای سایبر برای پیشبرد اهداف دیپلماسی به ضرورت تبدیل شده است از این‌رو، دیپلمات عصر فناوری ارتباطات و اطلاعات با دیپلمات نسل قبل خود تفاوت‌های ماهوی پیدا کرده است. یکی از مهم‌ترین شبکه‌های اجتماعی که در دیپلماسی سایبری اهمیت دارد، توئیتر است. دیپلماسی توئیتری یا توئیپلماسی در خدمت دیپلماسی سایبری قرار گرفته است و مسیر جدیدی را پیش روی سیاستمداران گشوده است.

## ۴ دیپلماسی سایبری و قدرت توئیتر؛ توئیپلماسی

قدرت و نفوذ شبکه‌های اجتماعی بسیار جدی و مؤثر است. توئیتر یکی از محبوب‌ترین و کارآمدترین شبکه‌های اجتماعی در جهان شناخته شده است. تحقیقات نشان داده است که کاربران شبکه‌های اجتماعی توئیتر را به دیگر شبکه‌های اجتماعی از جمله فیس‌بوک ترجیح می‌دهند و یکی از عمده دلایل آن کارآمدی و درجه بالای تأثیرگذاری آن است [۱۲]. این شبکه اجتماعی تا آوریل سال ۲۰۲۲ بالغ بر ۷۶۹ میلیون عضو و ۳۲۸ میلیون کاربر فعال داشته است [۱۳].

توئیپلماسی شکل آنلاین به‌کارگیری دیپلماسی عمومی در فضای سایبری از طریق توئیتر است که دیپلمات‌ها، سیاستمداران، وزارتخانه‌های امور خارجه و دیگر شخصیت‌های عمومی و بازیگران ذی‌نفع از آن استفاده می‌کنند. توئیپلماسی به معنی افزایش بهره‌وری، هم‌افزایی و تعامل از طریق توئیت‌های هدفمند است. نخستین وجه بارز توئیپلماسی وجه ارتباط برقرارکردن بی‌واسطه با انبوه مخاطبانی است که هر یک نه مخاطبی عادی، بلکه مخاطبی کنشگر محسوب می‌شوند که آن‌ها نیز مخاطبان کنشگر دیگری را دارند. هر فرد در توئیتر کنشگری سیاسی، اجتماعی، مذهبی، یا بین‌المللی است. کشورها برای حل مسائل بین‌المللی از «دیپلماسی چندمسیره» استفاده می‌کنند که تمامی ویژگی‌های آن در توئیتر نمایان است. مخاطب این توئیت‌ها افراد معمولی یا کاربران خاص هستند و این کار می‌تواند با انتشار موضع رسمی، تعامل با ذی‌نفعان و اعضای دیگر، یا از طریق «دنبال کردن» شخصی کاربران یا ارتباط بی‌واسطه از طریق ارسال پیام مستقیم یا خصوصی برای کاربران صورت گیرد. از آنجاکه هرکسی از هر جای دنیا می‌تواند کاربران عمومی شبکه‌های

<sup>1</sup>Networking Power

<sup>2</sup>Network Power

<sup>3</sup>Networked Power

<sup>4</sup>Network-making Power

اجتماعی را دنبال کند، توئیپلماسی می‌تواند وسیله‌ای برای افزایش مخاطبان پیام یک کشور باشد [۱۴]. فارغ از این که نام این روند جدید در دیپلماسی را توئیپلماسی یا دیپلماسی چندمسیره یا شاخه‌ای از دیپلماسی عمومی بگذاریم، ابزارهای پدید آمده با شبکه‌های اجتماعی خصوصاً توئیتر دیپلمات‌ها، سیاستمداران و ارتباط گیرندگان دیگر را (بازیگران دیگر بین‌المللی یا کسانی که به آن‌ها توئیپلمات می‌گویند) مجبور کرده است تا با وجود این ساختار و زمینه جدید، دیپلماسی را مورد بازطراحی و بازاندیشی قرار دهند.

مطالعه‌ای درباره توئیپلماسی در سال ۲۰۱۷ که تحقیقی سالیانه درباره حضور فعالانه رهبران و سران حکومت‌های جهان، وزرای خارجه و مؤسسات زیرمجموعه آن‌ها در توئیتر است، ۶۶۹ حساب کاربری توئیتر را بررسی کرده و دریافته است که تقریباً همه دولت‌های ۱۹۳ کشور عضو سازمان ملل به جز چند کشور در آفریقا در توئیتر حضور دارند. در همین حال، مشخص شده است دولت‌ها و وزارت خارجه بیش‌تر کشورهای جهان از طریق توئیتر برخی از برنامه‌ها، سیاست‌ها و اهداف سیاست خارجی خود را دنبال می‌کنند [۱۵].

بر اساس یافته‌های منتشرشده در وبسایت توئیپلماسی، شبکه‌های اجتماعی از جمله توئیتر به یکی از اصلی‌ترین و حیاتی‌ترین ابزارهای ارتباطی برای دولت‌ها تبدیل شده‌اند و توئیتر مشخصاً کانال و مسیر اصلی اجرای دیپلماسی دیجیتال است. در واقع، حتی تفاوت‌های دنیای واقعی نیز در توئیتر نقش ایفا می‌کنند و برخی مواقع به وقوع جنگ هشتگ‌ها بین سفارت‌خانه‌ها و وزارت خارجه‌های کشورهای مختلف منتج می‌شوند [۱۶].

وبسایت توئیپلماسی هم‌چنین لیست جامعی از تمامی سفارت‌خانه‌ها و رهبران و وزرای خارجه کشورهای مختلف دنیا را که در توئیتر حضور فعال دارند به صورت سالیانه منتشر می‌کند. بیش از پنج هزار سفارت‌خانه در سراسر دنیا از کشورهای مختلف در توئیتر حضور فعال دارند، حال آن که به غیر از هزاران سفیر که روزانه در توئیتر مأموریت‌های خود را انجام می‌دهند، نزدیک به دو هزار سیاستمدار برجسته - از جمله رئیس‌جمهور آمریکا، نخست‌وزیران و وزرای خارجه کشورها و حتی دیگر شخصیت‌های برجسته مذهبی، اقتصادی و اجتماعی جهانی مانند پاپ - در توئیتر فعالانه حضور دارند. به نظر می‌رسد، توئیپلماسی به طریقی دی.ان.ای دیپلماسی را دگرگون کرده است: نوعی سازگاری ژنتیکی با فناوری‌های جدید [۱۷]. بنابراین می‌توانیم نتیجه بگیریم که دیپلماسی توئیتری نه تنها ماهیت، اهداف و ارزش‌های دیپلماسی عمومی را حفظ کرده و تغییر نداده است، بلکه همه آن‌ها را ارتقاء بخشیده و به تحقق آن‌ها کمک کرده است.

#### ۱.۴ اهمیت شبکه‌های اجتماعی در سیاست خارجی آمریکا

در استراتژی بین‌المللی ایالات متحده برای فضای مجازی، بر تعهد ایالات متحده بر تلاش‌های بین‌المللی تأکید شده است که برای ارتقای زیرساخت‌های اطلاعاتی و ارتباطی باز، بر خوردار از تعامل متقابل، امن و قابل اعتماد که حامی تجارت و بازرگانی بین‌المللی است؛ امنیت بین‌المللی را تقویت می‌کند و موجب نوآوری و تقویت آزادی بیان در سراسر جهان می‌شود، ویکتوریا اسر در تشریح و تأیید استراتژی‌های دیجیتالی آمریکا می‌گوید: «نوآوری یکی از بزرگ‌ترین دارایی‌های ایالات متحده است و ما با به‌کارگیری آن در حال بازتعریف برنامه‌های دیپلماتیک و توسعه‌ای خود هستیم. دیپلمات‌ها و متخصصان توسعه ما چه در حال کمک به پیشرفت آزادی اینترنت باشند یا در حال ارتباط‌گیری با پیشگامان زن در غرب آفریقا یا درگیر زلزله ویرانگری که ژاپن را

تکان داده است همگی در حال استفاده از شبکه‌های دیجیتالی و فناوری‌هایی هستند که در خدمت سیاست خارجی آمریکا قرار دارد. وزارت خارجه آمریکا گوی بلورین ندارد. بنابراین ما به درستی می‌دانیم که نوآوری مداوم ما را در خط مقدم دیپلماسی دیجیتال حفظ خواهد کرد و این برتری به معنی ایجاد امکان بیش‌تر برای به اشتراک‌گذاری اطلاعات بیش‌تر و غنی‌تر در داخل و خارج از کشور برای ماست. ما هم‌چنین می‌دانیم که ضرب‌المثل قدیمی نوآوری کن یا بمیر، همچنان ما را روی پای خود نگه خواهد داشت» [۱۸].

وزارت خارجه ایالات‌متحده آمریکا در سال ۲۰۰۲ گروه عملیات ویژه ای. دیپلماسی را تشکیل داد. این گروه هم‌اکنون به اداره ای. دیپلماسی تغییر نام‌یافته است که در ادارات و دفاتر مختلف در سراسر جهان کار می‌کنند. اداره آمریکا در ارتباط برقرار کردن و به اشتراک گذاشتن اطلاعات ایجاد شد و اکنون آرشیو آن از ۲۰ ژانویه ۲۰۰۹ تا ۱۰ ژانویه ۲۰۱۷ در دسترس عموم قرار دارد [۱۹]. وزارت خارجه ایالات‌متحده آمریکا به جز این، یک نسخه داخلی از ویکی‌پدیا دارد که نام آن دیپلوپدیا است. هم‌چنین، برای تشویق افراد به شبکه‌سازی داخلی یک نسخه معادل فیس‌بوک در اداره راه‌اندازی شده است که نام آن را کریدور گذاشته‌اند. بنابراین، می‌توان ادعا کرد که جدی‌ترین گام در بهره‌برداری از فناوری‌های نوین و ظرفیت‌های مبتنی بر اینترنت در پیشبرد سیاست خارجی بعد از حوادث یازده سپتامبر برداشته شد و پس‌از این حملات بود که وزارت خارجه آمریکا برنامه مستمر و جدی دیپلماسی دیجیتال خود را آغاز کرد [۲۰].

در سال ۲۰۱۴، مویرا ولان، جانشین دستیار جان کری در استراتژی‌های دیجیتال و در اداره امور عمومی وزارت خارجه آمریکا، وضعیت دیپلماسی دیجیتال را چنین تبیین کرده است: «اکنون تقریباً تمام سفرای آمریکا از فیس‌بوک و توئیتر برای برقراری ارتباط مستقیم با مردم دنیا استفاده می‌کنند. شبکه‌های اجتماعی اکنون در حال تغییر دادن مسیر برقراری رابطه میان آمریکا و دیگر مردمان جهان هستند که هم جنبه شخصی دارد و هم جنبه عمومی. ما داریم تلاش می‌کنیم تا به جای پس‌زدن مخالفت‌ها، از ابزارهای شبکه‌های اجتماعی برای مدیریت سیاست‌های آمریکا و انتقادهای موجود استفاده کنیم. شبکه‌های اجتماعی، تلاش‌های دیپلماسی ما را ادامه داده است و ما را تبدیل به شفاف‌ترین وزارت خارجه جهان کرده است. ما اکنون روزانه بیش از هزار توئیتر در روز داریم و اگر به فرض در ماه یک توئیتر اشتباه در دسرساز هم داشته باشیم آن قدر در قبال دستاوردهای مثبت آن به چشم نمی‌آید» [۲۱].

## ۲.۴ توئیپلماسی وزارت خارجه آمریکا

وزارت خارجه ایالات متحده آمریکا از توئیپلماسی برای پیشبرد اهداف متفاوتی در سراسر جهان بهره برده است و همواره آن را منبع جدیدی از قدرت دانسته است. دیپلمات‌های آمریکایی نیز در دوره دولت باراک اوباما و هیلاری کلینتون در وزارت خارجه از توئیتر برای اهداف سیاسی، انسان‌دوستانه، یا کمک به برخی کشورها برای رسیدن یا قرارگرفتن در مسیر توسعه استفاده کرده‌اند. در بخش سیاسی اهداف وزارت خارجه آمریکا شامل نفوذ در جوانان مسلمان به‌منظور تغییر نگرش آن‌ها به سیاست‌های آمریکا در خاورمیانه و دیگر نقاط جهان در خصوص مسلمانان، رصد و پایش و جمع‌آوری اطلاعات درباره فعالیت‌های تروریستی مرتبط با القاعده و دیگر افراط‌گرایان مسلمان، تأثیرگذاری در جنبش‌های دموکراسی‌خواه مانند آنچه در ایران و در ناآرامی‌های پس از انتخابات ریاست‌جمهوری این کشور در سال ۲۰۰۹ رخ داد، تأثیرگذاری در روند دموکراسی‌سازی در



خاورمیانه - هرچند نمی‌توان مستقیماً دخالت وزارت خارجه آمریکا را در ایجاد انقلاب‌های عربی اثبات کرد - تأثیرگذاری در فعالیت‌های سیاسی کشورهای رقیب از جمله روسیه و چین بوده است. در دوران ریاست جمهوری ترامپ، استفاده افراطی وی از توئیتر به تضعیف بهره‌برداری سایر نهادهای این کشور انجامید، امری که با روی کار آمدن بایدن، به سمت و سوی اولیه خود گرایش یافت.

یکی از مثال‌های بارز دیپلماسی توئیتری به سیاست خارجی آمریکا در قبال کوبا مربوط است. در سال ۲۰۰۹ دولت آمریکا در پوشش برنامه‌های اجتماعی و بهداشتی که تحت نظارت آژانس توسعه بین‌الملل آمریکا، یو.اس.اید<sup>۵</sup> بود، تلاش کرد باعث تحریک مردم این کشور برای تغییر سیاسی در کوبا شود. خبرگزاری آسوشیتدپرس در گزارشی تحقیقی افشا کرد که دولت باراک اوباما براساس یک برنامه مخفی از طریق شبکه‌های اجتماعی طرح جامعی را برای اغتشاش و به‌خیابان‌کشاندن مردم در برخی از کشورهای آمریکای لاتین از جمله کوبا دنبال می‌کرده است. در پروژه «یو.اس.اید» یک شبکه رسانه‌ای اجتماعی درست مانند توئیتر در کوبا راه‌اندازی شد که «زون زونئو»<sup>۶</sup> نام گرفت و توانست در سال‌های ۲۰۰۹ تا ۲۰۱۱، چهل هزار کاربر کوبایی را به خود جذب کند. نکته جالب این بود که هیچ‌یک از این کاربران نمی‌دانستند که عضو شبکه اجتماعی‌ای شده‌اند که گرداننده و تأمین‌کننده مالی آن، دولت آمریکاست. هم برنامه توئیتر کوبایی «زون زونئو» و هم برنامه سفر جوانان آمریکای لاتین به کوبا برای جذب فعالان سیاسی کوبا، بخشی از تلاش چندمیلیون دلاری «یو.اس.اید» برای تأثیرگذاری در کشورهایی بوده است که از لحاظ سیاسی بی‌ثبات بودند. «یو.اس.اید» هم در پاسخ به انتقادات صورت‌گرفته از این برنامه مخفی اعلام کرد که «دولت باراک اوباما متعهد است از علاقه مردم کوبا به آزادی برای تعیین آینده‌شان حمایت کند. یو.اس.اید با گروه‌های مستقل جوانان در کوبا در خدمات اجتماعی مثل بهداشت عمومی، هنر، و دیگر فرصت‌ها همکاری می‌کند تا مطابق با برنامه‌های دموکراسی با این جوانان ارتباط برقرار کند.» گزارش آسوشیتدپرس نشان می‌دهد که طبق برنامه قرار بود که اگر این جوانان دستگیر شوند، به‌صورت رمزی پیامی ارسال کنند و بگویند «من سردرد دارم». منظور از این جمله این بود که آن‌ها تحت نظارت مقامات کوبا هستند. یا جمله رمزی دیگر این بود که «خواهر شما بیمار است». ارسال این جمله در واقع دستور به این جوانان برای ترک کشور کوبا و پایان دادن به سفرشان بود. طبق قوانین کوبا همکاری با برنامه‌های یو.اس.اید غیرقانونی است [۲۲].

به‌نظر می‌رسد که اساس دکتترین «کشورداری در قرن بیست و یکم» وزارت امور خارجه آمریکا به‌منظور ایجاد قدرت در سیاست خارجی از طریق به‌کارگیری شبکه‌های اجتماعی و ابزارهای نوین ارتباطی شکل گرفته است. به غیر از نمونه به‌کارگیری این دیپلماسی در کوبا، موارد مشهور توئیلماسی آمریکا در مولداوی، اوکراین، روسیه، یا حتی بهار عربی وجود دارد. فارغ از این که وزارت امور خارجه آمریکا تا چه اندازه با به‌کارگیری این دیپلماسی موفق بوده است، روش‌ها و تلاش‌های این وزارت‌خانه در به‌کارگیری هر چه بهتر از فرصت شبکه‌های اجتماعی از جمله توئیتر به‌مثابه نماد و مؤلفه جدید از قدرت اعمال نفوذ و شکل‌دهی به افکار عمومی است.

<sup>5</sup>US Aid<sup>6</sup>ZunZuneo

## ۵ نتیجه گیری

تحولات عظیم عرصه فناوری ارتباطات و اطلاعات موجب شده است تا دیپلماسی نوین با عبور از دیپلماسی سنتی به عرصه دیپلماسی فوق مدرن وارد شود. در گستره بی کران فضای مجازی که امروزه بستر و جولان گاه شبکه های اجتماعی محبوب، از جمله توئیتر، شده اند و صدها میلیون انسان را به یکدیگر مرتبط کرده اند، استفاده از توئیپلماسی یا دیپلماسی توئیتری جایگاه مهمی پیدا کرده است؛ چراکه یکی از بهترین ابزارها برای کنترل و مدیریت آن چیزی است که کاستلز به آن ها «برنامه نویسی» و «راه گزینی» جامعه شبکه ای می گوید و معتقد است دو مکانیسم اصلی قدرت سپاری در شبکه ها هستند. دیپلماسی سایبری سبب می شود تا قدرت های بزرگ چون ایالات متحده آمریکا، عملکرد سیاست های رسانه ای خود را آن گونه که کاستلز تبیین می کند از طریق ایمن سازی دسترسی رسانه ها توسط بازیگران سیاسی و اجتماعی درگیر در راهبردهای قدرت سازی، بسط و گسترش پیام ها و تولید تصاویری که به بهترین وجه به منافع هر یک از بازیگران عرصه قدرت یاری می رساند، ارسال و پخش پیام را با استفاده از فناوری های خاص و چارچوب های ارتباطاتی مطلوب و سرمایه گذاری مالی مناسب بر روی ابزارهای ارتباطاتی بهبود ببخشد. به همین علت، استفاده مقامات سیاسی عمده کشورهای جهان در سالیان اخیر از رسانه های اجتماعی و خصوصاً توئیتر برای پیشبرد دیپلماسی رشد فراوانی داشته است. امروزه دیپلمات ها و سفارت خانه های کشورهای و در رأس آن ها آمریکا در سراسر دنیا به شبکه توئیتر متصل هستند. توئیتر فضایی به وجود آورده است که مسئولان کشورها و دیپلمات ها یا خود کنشگران فعالی در این شبکه شده اند و زنجیره حمایتی برای موضوع های مورد نظر خود را فراهم می کنند یا تحت تأثیر کنشگران دیگر اینترنتی اعم از سازمان های غیردولتی یا حتی اشخاص و گروه ها قرار گرفته اند و سیاست های خود را اصلاح می کنند یا تغییر می دهند. اگر هدف اصلی از دیپلماسی عمومی که دولت ها به کار می گیرند ایجاد تغییر در باور و تصور و ادراک افکار عمومی در کشورهای دیگر باشد، امروزه این مهم را کنشگران شبکه های اجتماعی خصوصاً توئیتر و از طریق دیپلماسی دیجیتال و توئیپلماسی به دست می دهند.

## مراجع

- [۱] کورنلیو بیولا و مارکوس هلمز، دیپلماسی دیجیتال (نظریه و عمل)، ترجمه رعنا کاظمی مهرآبادی، تهران: بنگاه ترجمه و نشر کتاب پارسه، ۱۳۹۵.
- [۲] ایلان مانور، دیجیتالی شدن دیپلماسی عمومی، ترجمه بابک دربیکی، تهران: سروش، ۱۴۰۰.
- [۳] عبدالحسین کلانتری، عباس قنبری باغستان، حکمرانی در عرصه پنجم: گذار به دیپلماسی سایبری، تهران: پژوهشگاه فضای مجازی، ۱۴۰۰.
- [۴] علیرضا توتونچیان، دیپلمات و دیپلماسی، تهران: دفتر مطالعات سیاسی و بین المللی وزارت امور خارجه، شماره ۱۳، ص ۱۲۴، ۱۳۷۲.
- [۵] مانوئل کاستلز، قدرت ارتباطات، ترجمه حسین بصیریان جهرمی، تهران: شرکت انتشارات علمی و فرهنگی، ص ۷۴۳، ۱۳۹۶.
- [۶] مانوئل کاستلز، قدرت ارتباطات، ترجمه حسین بصیریان جهرمی، تهران: شرکت انتشارات علمی و فرهنگی، ص ۸، ۱۳۹۶.

- [۷] مانوئل کاستلر، قدرت ارتباطات، ترجمه حسین بصیریان جهرمی، تهران: پژوهشگاه فرهنگ، هنر و ارتباطات، ص ۳۲۱، ۱۳۹۳.
- [۸] محمود بیات، دیپلماسی دیجیتالی: پژوهشی در تحولات دیپلماسی معاصر، تهران: وزارت امور خارجه، مرکز چاپ و انتشارات، ۱۳۸۵.
- [9] N. Wiener. Cybernetics or Control and Communication in the Animal and the Machine. Cambridge: MIT Press. 1964.
- [10] Willie D. Jones, This Week in Cybercrime: Cybercrime's Industrial Revolution, 2013, available at: <https://spectrum.ieee.org/this-week-in-cybercrime-cybercrimes-industrial-revolution>.
- [11] Tiirmaa-Klaar, H. Cyber Diplomacy: Agenda, Challenges and Mission. Peacetime Regime for State Activities in Cyberspace, 2013.
- [12] M. S. Dinata, Twiplomacy: How Twitter Affects Contemporary Public Diplomacy. Paramadina University, 2014.
- [13] Statista, Retrieved from Number of social media users worldwide 2022 (in billions), available at: <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users>.
- [14] C. Bjola, & M. Holmes, Digital Diplomacy: Theory and Practice, Routledge, 2015.
- [15] S. Adesina, Olubukola "Foreign policy in an era of digital diplomacy". Cogent Social Sciences, Volume 3, Issue 1, 2017.
- [16] Andra Alexandru, Twiplomacy, report: Twitter is the channel of choice for digital diplomacy, 2015. Retrieved from digitaldiplomacy: <http://digitaldiplomacy.ro/twiplomacy-2015-report-twitter-is-the-channel-of-choice-for-digital-diplomacy/?lang=en>.
- [17] A. Sandre, Twitter for Diplomats: A Guide to the Fastest Growing Digital Diplomacy Tool. 2013, 02 10. Retrieved from diplo: <https://www.diplomacy.edu/blog/twitter-diplomats-guide-fastest-growing-digital-diplomacy-tool>.
- [18] V. Esser, 21st Century Statecraft: Forging U.S. Digital Diplomacy, 2012, 03. 27. Retrieved from huffingtonpost: [https://www.huffingtonpost.com/victoria-esser/us-diplomacy-technology\\_b\\_1223638.html](https://www.huffingtonpost.com/victoria-esser/us-diplomacy-technology_b_1223638.html).
- [19] US department of state, ARCHIVEDCONTENT, 2022, Available at: <https://2009-2017.state.gov/m/irm/ediplomacy/index.htm>.
- [20] US department of state, Major Programs of IRM's Office of eDiplomacy, 2022, Available at: <https://2009-2017.state.gov/m/irm/ediplomacy/index.htm>.
- [21] M. Whelan, Social media is changing diplomacy, State Department official tells class, 2014, 10, 07. Retrieved 2017 from penn state: <http://news.psu.edu/story/329204/2014/10/07/academics/social-media-changing-diplomacy-state-department-official-tells>

- [22] AP (Associated Press) (2014). US secretly created 'Cuban Twitter' to stir unrest and undermine government. Retrieved 2017 from theguardian: <https://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest>.

## بایوسایبرنتیک، مبنای کنترل‌های نوین در حوزه‌ی زیستی

محمدعلی شکوهیان‌راد<sup>۱</sup>، امیرحسین منتظر<sup>۲</sup>

<sup>۱</sup>پژوهشگر ارشد آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران

cm@shokoohian.ir

<sup>۲</sup>دانشجوی دانشگاه علوم پزشکی تهران

### چکیده

متأثر از تحولاتی که دانش سایبرنتیک در سایر دانش‌ها ایجاد نمود، منطق کنترل پدیده‌ها مبتنی بر اصالت جریان اطلاعات به اکثر دانش‌ها راه یافت و الگوی منطقی آنها را تغییر داد. زیست‌شناسی، یکی از مهم‌ترین حوزه‌های متأثر از سایبرنتیک است که حاصل آن از اواخر دهه‌ی ۱۹۷۰ با عنوان بایوسایبرنتیک شناخته می‌شود. منظور از بایوسایبرنتیک، دانش جدیدی است که در هر سه حوزه‌ی مفاهیم، نظریات و روش‌شناسی، به‌دنبال شناسایی و شناخت سیستم‌های فرماندهی و کنترل موجودات زیستی از درون و بیرون آنهاست تا بتواند از این طریق، کنترل را بر آن پدیده‌ی زیستی اعمال نماید. بایوسایبرنتیک علاوه بر بررسی منطق فیزیکی و کارکرد فرماندهی و کنترل در موجودات زیستی، به بررسی هویت متافیزیکی و علل ترنس‌فیزیکی پدیده‌های زیستی نیز می‌پردازد. یکی از مهم‌ترین نقاط اتکای علمی و عملی بایوسایبرنتیک، حوزه‌ی دانش‌های همگرا است که از چهار دانش نانو، بیولوژی، تکنولوژی اطلاعات و دانش‌شناختی تشکیل شده است. ساخت مصنوعی پدیده‌های زیستی، ساخت مسیرهای زیستی جدید، ایجاد بیماری‌های نوین و کاملاً متفاوت، طرح‌ریزی انسان از حیث فرماندهی و کنترل مبتنی بر ژنوم نمونه‌هایی از دستاوردهای دانش بایوسایبرنتیک در حوزه‌ی فرماندهی و کنترل زیستی هستند.

**کلمات کلیدی:** بایوسایبرنتیک، سایبرنتیک، زیست‌کنترل اطلاعاتی، سایبرنتیک زیستی، کنترل اطلاعاتی، کنترل شناختی.

## ۱ مقدمه

دهه‌ی ۱۹۵۰ تا ۱۹۸۰ میلادی را می‌توان دهه‌ی تحول دانش‌ها و شکل‌گیری منظومه‌ی نوین دانش در نظر گرفت؛ سال‌هایی که دانشمندان و متخصصان در هر رشته، متأثر از ادبیاتی که دانش سایبرنتیک رواج داد به بازنگری در منطق پایه‌ی تخصص خود پرداخته و نسخه‌ی به‌روز شده‌ای از دانش خود را ارائه نمودند. به‌طور کل، منطق سایبرنتیک بیان می‌دارد که برای کسب سلطه می‌توان از کنترل جریان اطلاعات مؤثر بر پدیده‌ها استفاده نمود؛ به‌گونه‌ای که ادراک آن پدیده‌ها منطبق با معیارهای کنترل‌کننده شود. در نتیجه تصمیم و سپس اقدام پدیده‌های مدنظر نیز در راستای مطلوبات و ترجیحات کنترل‌کننده قرار خواهد گرفت.

منطق فوق در حوزه‌ی کنترل، ده‌ها دانش کلان و جامعه‌ساز نظیر اقتصاد، روانشناسی، جامعه‌شناسی، تاریخ، فیزیک و ... را تحت تأثیر قرار داد که محتوای پایه‌ی هر کدام از آنها موجود است. زیست‌شناسی نیز از این شرایط مستثنی نشد و با عنوان دانش بایوسایبرنتیک، نسخه‌ی سایبرنتیکی خود را عرضه نمود. لذا مبنای دانش بایوسایبرنتیک، کنترل پدیده‌های زیستی از طریق کنترل جریان اطلاعات توسط متغیرهای مختلف کنترلی است که موجودات زیستی از آنها تأثیر می‌پذیرند که حوزه‌ی موسع و گسترده‌ای شامل ژنتیک تا ذهن را در بر می‌گیرد.

بر این اساس بیش از نیم قرن است که بسیاری از روش‌ها و تکنولوژی‌های نوین کنترل پدیده‌های زیستی، بر اساس دانش بایوسایبرنتیک طراحی و عملیاتی شده است. از این رو ضرورت دارد متخصصان در کشور، به دو دلیل مهم به دانش بایوسایبرنتیک روی آورند:

۱. بسیاری از کاربردهای مفید امروزی در نسبت با گیاهان، حیوانات و انسان، ریشه در بایوسایبرنتیک دارد که امروزه در کشور برای مقاصد مختلف، به آنها نیاز داریم؛

۲. تهدیدات نوین نسبت به پدیده‌های زیستی نیز بر اساس مبانی بایوسایبرنتیک طراحی می‌شود. لذا برای شناخت و مقابله با تهدیدات و مخاطرات نوین نیز باید دانش مذکور را مطالعه و بر آن مسلط شویم.

نوآوری پژوهش حاضر از آن جنبه است که اولاً نخستین متن علمی در زبان فارسی است که به تعریف و تبیین جامع دانش بایوسایبرنتیک می‌پردازد، ثانیاً دانش‌های پایه‌ی آن را معرفی می‌نماید و ثالثاً دستاوردهای نوینی که از آن حاصل شده را شرح می‌دهد.

بدین منظور، پژوهش حاضر ابتدا دانش سایبرنتیک را بررسی می‌کند، سپس به معرفی تأثیرات سایبرنتیک بر حوزه‌ی زیست پرداخته و بایوسایبرنتیک را معرفی می‌نماید. در نهایت نیز به تشریح جدیدترین دستاوردهای بایوسایبرنتیک می‌پردازد.

## ۲ پیشینه‌ی پژوهش

به استناد جستجو در سه پایگاه علمی مقالات علمی معتبر فارسی زبان شامل نورمگز، مگیران و پایگاه مرکز اطلاعات علمی جهاد دانشگاهی، تنها دو مقاله که در آن از عنوان بایوسایبرنتیک (با نگارش بیوسایبرنتیک) استفاده شده است، یافت شد.

نخست، حمید هادیان در مقاله‌ای با عنوان «روحیه‌ی جنگی در پروژه‌ی گذار ارتش آمریکا به قرن بیست و یکم» اشاره‌ای کوتاه به یکی از کاربردهای بایوسایبرنتیک در حوزه‌ی تجهیزات نظامی نموده و بیان داشته: «امروزه جنگجویان جدید، شامل منابع انسانی متخصص و دارنده‌ی دانش برتر نظامی و نیز هوش مصنوعی ربات‌های جنگی موسوم به سیستم‌های جدید جنگی است که با یکدیگر کنش شبکه‌ای دارند.

جنگجویان جدید معطوف به سیستم‌های جدید جنگی با فناوری‌های تأثیرپذیر از مهندسی عملکرد انسانی و شبکه‌ی به تعامل بین سیستم و انسان برای پردازش داده‌ها و تبدیل آنها به اطلاعات و نیز انتقال آنها



می‌پردازند. بدین ترتیب نوعی ارتباط بهینه بین روحیه‌ی انسان‌افزایی جنگی و روحیه‌ی سیستمی جنگی مبنی بر تعامل بین انسان و سیستم، تحت عنوان بیوسایبرنتیک چندرسانه‌ای چندبعدی دینامیک با عملکرد طبیعی و واقعیت‌های مجازی برای توسعه‌ی محیط‌های همکاری انسان و سیستم به وجود می‌آید.»

سپس محمد علی شکوهیان‌راد در مقاله‌ای با عنوان «اخلاق در سیستم‌های فرماندهی و کنترل، مبنای چهارچوب نوین طراحی تهدیدات و بحران‌ها» در خصوص بیوسایبرنتیک چنین ذکر نموده: «سیستم‌های فرماندهی و کنترل، محدود به سیستم‌های ماشینی نیست بلکه در دانش نوین، برای سیستم‌های فرماندهی - کنترل طبیعی نیز امکان برنامه‌ریزی و به تبع اخلاق وجود دارد. مهم‌ترین نمونه‌ی سیستم فرماندهی و کنترل طبیعی که با عنوان سیستم‌های بیوسایبرنتیک شناخته می‌شود انسان است که فرایند درک ذهنی و پردازش اطلاعاتی وی، همانند سیستم‌های هوشمند ماشینی است زیرا فرماندهی و کنترل ماشین از فرماندهی و کنترل انسان الگو پذیرفته است و دانش هوش مصنوعی روند مطالعات تکمیلی آن را دنبال می‌نماید.»

اما اصل پیشینه‌ی پژوهش‌های بیوسایبرنتیک را می‌توان در دو زبان انگلیسی و آلمانی ملاحظه نمود. بر اساس جستجوی پایگاه‌های علمی انگلیسی زبان، حدود ۲۳۷۰ مقاله در پایگاه ساینس دایرکت و ۱۳۷ مقاله در پایگاه گوگل اسکولار فقط برای سال ۲۰۲۲ میلادی نمایه شده که در عنوان آنها بیوسایبرنتیک به کار رفته است. همچنین به طور ویژه دو مجله‌ی علمی بین‌المللی برای این حوزه وجود دارد که عبارتند از «مهندسی بیوسایبرنتیک و بیومدیکال»<sup>۱</sup> و «بیولوژی‌یکال سایبرنتیک»<sup>۲</sup> که به صورت تخصصی مقالات مرتبط با حوزه‌ی بیوسایبرنتیک را از سراسر جهان پذیرش نموده و منتشر می‌سازند.

قطعاً نمی‌توان در این مجال به بررسی بسیاری از مقالات پرداخت اما رصد عناوین مقالات نوین حاکی از آن است که بخش چشمگیری از مقالات در حیطه‌ی کنترل انسان یا بخشی از اندام انسان توسط سیستم‌های سایبرنتیک تمرکز دارند.

همچنین بخش دیگری از مقالات اخیر در حوزه‌ی بیوسایبرنتیک به بررسی انواع مسائل بیماری‌زا یا روش‌های تشخیص بیماری‌ها در انسان از منظر سایبرنتیک پرداخته‌اند که در این خصوص، مقالات مرتبط با کرونا از تعداد قابل توجهی برخوردار است. برای نمونه مارتا کوزون و همکارانش در مقاله‌ای با عنوان «شناسایی خودکار بیماری‌های تنفسی از طریق سیگنال‌های صوتی ریه استتوسکوپی با استفاده از طبقه‌بندی کننده‌های گروهی»<sup>۳</sup> ذکر کرده است: «در این مطالعه، ما تأثیر آترواسکلروز را بر رفتار ناهمسانگرد و تراکم‌ناپذیر دیواره‌ی آئورت قفسه‌ی سینه‌ی انسان، تحت بارهای مکانیکی تجزیه و تحلیل کردیم. این مطالعه تنها مطالعه‌ای است که تاکنون تغییراتی را در خواص مکانیکی در تمام مراحل رشد آترواسکلروتیک ارائه کرده است. تعداد زیادی از آماده‌سازی‌ها در مطالعه گنجانده شد که برای نتایج به دست آمده به دلیل علت چند عاملی توسعه آترواسکلروز مهم است.»

در مقاله‌ای دیگر با عنوان «تجزیه و تحلیل سیگنال‌های EEG صرعی با استفاده از تجزیه حالت پویا و

<sup>1</sup>Biocybernetics and Biomedical Engineering

<sup>2</sup>Journal "Biological Cybernetics"

<sup>3</sup>Influence of atherosclerosis on anisotropy and incompressibility of the human thoracic aortic wall

طیف»<sup>۴</sup>، اوزلم کارابیر کورا<sup>۵</sup> تلاش نموده از طریق تشخیص و تحلیل سیگنال‌های نوار مغزی به وقوع حملات صرع، الگوریتم وقوع و زمان بندی آن پی ببرد.<sup>۶</sup>

ولادیمیر کودکین در مقاله‌ای با نام «شناسایی دیجیتالی شرایط انسانی به عنوان پیش نیاز اثربخشی عملیات سیستم‌های اتوماسیون سازمانی (بایوسایبرنتیک)» تلاش نموده کنترل انسان از طریق تعامل با ماشین را ارتقاء بخشد. وی اذعان داشته: «این مقاله به مشکلات بهبود سیستم‌های تعامل انسان و ماشین مدرن می‌پردازد. چنین سیستم‌هایی را سیستم‌های بایوسایبرنتیک می‌نامند که نشان داده شده است با تثبیت کار آنها بر اساس نظریه‌ی کنترل اتوماسیون می‌توان به افزایش قابل توجهی در کارایی انسان دست یافت. تجزیه و تحلیل طرح‌های ساختاری سیستم‌ها نشان داد که یکی از مهم‌ترین عوامل تأثیرگذار در این سیستم‌ها «دیجیتال سازی» ضعیف شرایط انسانی است. «دیجیتالی سازی» در اینجا شناسایی یک فرد به عنوان مشارکت کننده در تعامل با یک سیستم سایبرنتیک یا سایبری-فیزیکی است.

مشکل اصلی ساخت یک سیستم بایوسایبرنتیک، ثابت نبودن ویژگی‌های انسانی مانند زمان واکنش به اختلالات خارجی، خستگی فیزیکی یا عصبی، توانایی انجام مقدار مورد نیاز کار و ... است. در عین حال، به عنوان یک قانون، هیچ ارزیابی عینی از این غیر ایستایی وجود ندارد. تحت این شرایط، اطمینان از کنترل پذیری و کارایی سیستم‌های بایوسایبرنتیک کاری بسیار دشوار است.

برای حل این مشکل با کمک سیگنال‌های الکتروکاردیوگرام پیشنهاد شده است: در دسترس‌ترین و دقیق‌ترین اطلاعات در مورد وضعیت فعلی یک انسان گزارش شود. در این مقاله به چند نمونه از راه‌حل‌ها و نتایج مطالعات و آزمایشات نظری پرداخته می‌شود.

تمایز اصلی پژوهش حاضر با سایر پژوهش‌های داخلی و خارجی که تاکنون در زمینه‌ی بایوسایبرنتیک منتشر شده است در این است که تلاش نموده تا برای نخستین بار، اساس مبانی و منطق حاکم بر بایوسایبرنتیک را از منظر دانش سایبرنتیک تشریح نموده و مشخص سازد چه تحولاتی متأثر از سایبرنتیک در زیست‌شناسی ایجاد شد که منتج به پدید آمدن بایوسایبرنتیک گشت. همچنین تلاش بر این است تا بر اساس شاخصه‌های کاربردی و تعاریف عملیاتی مشخص شود وجه تمایز بایوسایبرنتیک با زیست‌شناسی در چیست و این دانش نوین چه جایگاه و نگاهی به پدیده‌های زیستی دارد؟ در نهایت میدان‌های نظری و فنی که امروزه تحت تأثیر بایوسایبرنتیک هستند مورد اشاره، معرفی و تشریح قرار خواهند گرفت.

لذا در یک جمله می‌توان اذعان داشت پژوهش حاضر در تلاش است تا برای نخستین بار، یک متن علمی پایه، مدون و نسبتاً جامع برای معرفی دانش بایوسایبرنتیک و آثار آن در حوزه‌ی فرماندهی و کنترل پدیده‌های زیستی ارائه نماید.

<sup>4</sup>Analysis of epileptic EEG signals by using dynamic mode decomposition and spectrum

<sup>5</sup>Ozlem Karabiber Cura

<sup>6</sup>44 تا 28 صفحات هم‌ان،

## ۳ ادبیات پژوهش

### ۱.۳ دانش سایبرنتیک

بر اساس منابع موجود، پایه‌گذاری سایبرنتیک به‌عنوان یک دانش، به اوایل قرن نوزدهم میلادی بازمی‌گردد. تاکنون اولین مرجع شناخته شده‌ای که از سایبرنتیک با عنوان **دانش** یاد کرده است، مبحث «دانش آینده‌ی حکومت»<sup>۷</sup> به قلم «آندره ماری آمپر»<sup>۸</sup> فیزیک‌دان معروف فرانسوی است که در سال ۱۸۴۳ میلادی نگاشته شده است. آمپر در اثر خود، سایبرنتیک را (با تلفظ فرانسوی سیبِنتیک)<sup>۹</sup> به حوزه‌ی علوم سیاسی مرتبط کرده و آن را «**دانش حکومت‌داری مدنی**»<sup>۱۰</sup> به‌معنای «دانش سیاست‌های جاری و اداره‌ی عملی در یک دولت یا جامعه» تعریف نموده است. همچنین نظر آمپر درباره‌ی کارکرد و جایگاه دانش سایبرنتیک چنین بوده که همان «**حکومت و شعبه‌ای از علم سیاست**» است. پس از آمپر، ترنتوسکی<sup>۱۱</sup> سایبرنتیک را «**هنر چگونگی حکمرانی بر مردم**» تعریف نموده که مؤید دیدگاه آمپر می‌باشد.

اما مهم‌ترین منابع فلسفی و نظری در خصوص دانش سایبرنتیک، توسط نوربرت وینر<sup>۱۲</sup> و در قرن بیستم میلادی تألیف و منتشر شده است؛ به‌همین دلیل وی را پدر دانش سایبرنتیک می‌نامند. وینر در سال ۱۹۴۸ میلادی برای اولین بار به زبان انگلیسی در کتابی با عنوان «سایبرنتیک: یا کنترل و ارتباط در حیوان و ماشین»<sup>۱۳</sup> واژه‌ی سایبرنتیک را به کار برد.

وینر در خصوص انتخاب واژه‌ی سایبرنتیک چنین بیان می‌دارد: «تا دوران اخیر، واژه‌ای که مبین این گروه از افکار [منظور، کنترل پدیده‌ها از طریق 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». 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».

بنابر تعریف وینر، سایبرنتیک دانش کنترل پدیده‌ها از طریق جریان اطلاعات است و ابعاد آن مطابق شکل ۱ است.

لذا از سویی بر کنترل هر پدیده در جای خود تمرکز دارد و از سویی دیگر ارتباطات پدیده‌ها را با یکدیگر کنترل می‌نماید. این یعنی اعمال کنترل هم در سطح فردی و هم در سطح اجتماعی صورت می‌پذیرد. همچنین کنترل فردی و اجتماعی، هم نسبت به موجودات زیستی انجام می‌شود و هم پدیده‌های غیرزیستی. از تلفیق و ضرب ماتریسی گزاره‌های فوق، چنان نتیجه می‌شود که سایبرنتیک، کنترل تمام جامعه را مدنظر قرار داده است.

<sup>7</sup>The Future Science of Government

<sup>8</sup>André-Marie Ampère

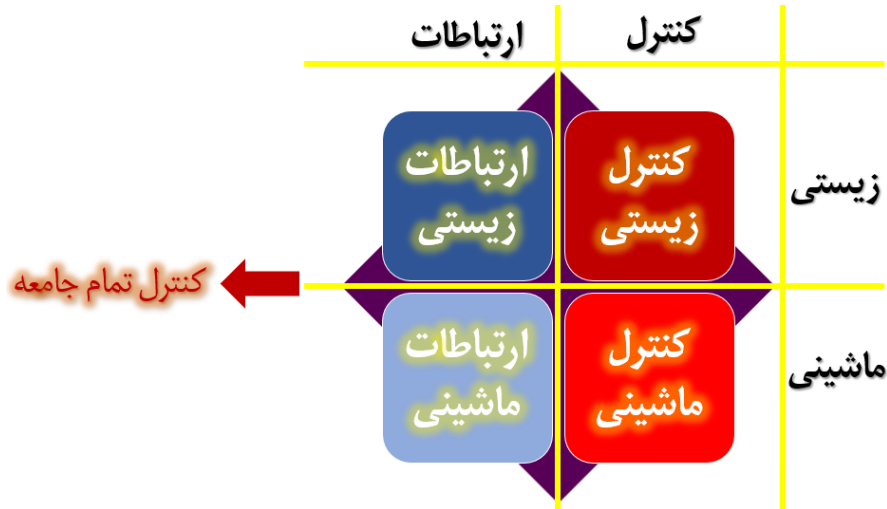
<sup>9</sup>Cybernétique

<sup>10</sup>The Science of Civil Government

<sup>11</sup>Trentowsky

<sup>12</sup>Norbert Wiener

<sup>13</sup>Cybernetics: Or Control and Communication in the Animal and the Machine



شکل ۱: ابعاد دانش سایبرنتیک مطابق تعریف وینر

لذا در یک جمله می‌توان سایبرنتیک را دانش کنترل تمامی پدیده‌ها در سطوح فردی و اجتماعی از طریق جریان اطلاعات تعریف نمود.

### ۲.۳ سایبرنتیک، مبنای تحول دانش‌ها در عصر حاضر

بررسی قیاسی دانش‌های پیش از سایبرنتیک و همچنین دانش‌هایی که پس از آن ایجاد شده‌اند حاکی از آن است که منطق کنترل از طریق جریان اطلاعات، به مبنای اکثر دانش‌ها راه یافته و بر آنها عمیقاً اثر گذاشته است. لذا با صدها رشته‌ی علمی مواجه هستیم که اهداف سابق خود را با شیوه‌های جدید سایبرنتیکی پیگیری می‌نمایند. در این میان، از مهم‌ترین حوزه‌های متأثر از دانش سایبرنتیک، منظومه‌ی دانش‌های زیست‌شناسی است که مسیری بسیار جدی و متفاوت را نسبت به گذشته‌ی خود رقم زده است. به عبارت دیگر، میزان اثرگذاری سایبرنتیک به‌عنوان یک نقطه‌ی عطف در دانش زیست‌شناسی، از سایر دانش‌ها عمیق‌تر و ملموس‌تر می‌باشد.

بایوسایبرنتیک یک رویکرد نوآورانه است که هدف آن، درک عمیق‌تر سیستم‌های پیچیده‌ی دارای حیات است. این توصیف ریاضی و ساختاری، مقوله‌ی پردازش اطلاعات در موجودات زنده و اکوسیستم‌ها را پوشش می‌دهد.

نخستین ریشه‌های بایوسایبرنتیک را می‌توان در آثار «هانس دریشل»<sup>۱۴</sup> دانشمند آلمانی مشاهده کرد که اثری با عنوان «درآمدی بر بایوسایبرنتیک»<sup>۱۵</sup> به زبان آلمانی تألیف نموده است. وی در کنار جمعی از دانشمندان که همگی بر حوزه‌ی بایوسایبرنتیک تمرکز داشته‌اند، از محققین اصلی «انستیتو بایوسایبرنتیک

<sup>14</sup>Hans Drischel

<sup>15</sup>Einführung in die Biokybernetik

ماکس پلانک»<sup>۱۶</sup> به‌شمار می‌آید که اساساً برای مطالعه‌ی آثار و عملکرد کنترل‌های سایبرنتیکی بر حوزه‌های زیستی تأسیس شده بود.

ادامه‌ی روند مطالعات بایوسایبرنتیک، امروز بدان‌جا رسیده که چندین ژورنال علمی نظیر «مهندسی بایوسایبرنتیک و بیومدیکال»<sup>۱۷</sup> و «بیولوژیکال سایبرنتیک»<sup>۱۸</sup> و همچنین آزمایشگاه‌های معتبر مانند «آزمایشگاه بایوسایبرنتیک دانشگاه یوسی‌ال‌ای»<sup>۱۹</sup> با تعریف ده‌ها پروژه‌ی مطالعاتی - عملیاتی راه‌اندازی شده و به‌طور عمیق و گسترده‌ای بر سیستم‌های فرماندهی و کنترل زیستی تمرکز نموده‌اند.

### ۳.۳ بایوسایبرنتیک: چیستی، چرایی و چگونگی

بقاء تمامی موجودات زنده، متشکل از یک سری امور است که اگر هر کدام از آنها دچار اختلال شود، در حداقل زمان، مشکلات جدی و حتی مرگ را برای آن موجود پدید می‌آورد. از سوی دیگر این امور حیاتی و سایر امور زیستی وابسته به آنها بر پایه‌ی مجموعه‌ای از دستورالعمل‌ها و اطلاعات در بدن موجودات تعریف می‌شوند، به‌گونه‌ای که اولاً تعیین‌کننده‌ی چیستی و چگونگی اقدامات و امور حیاتی می‌باشند و ثانیاً به‌صورت کامل، تحت کنترل سیستم‌های فرماندهی بالادستی هستند تا هماهنگی، یکپارچگی، به‌هنگام بودن، روند تکامل و سایر ملزومات را فراهم نماید.

مهم‌ترین قسمت دستورالعمل‌های مذکور در دو بخش:

۱. سیستم اعصاب مرکزی به‌عنوان مرکز فرماندهی و کنترل موجودات زیستی؛
  ۲. ژنوم (به دو صورت DNA و RNA) به‌عنوان عاملیت فرماندهی و کنترل صفات و ویژگی‌های بنیادین موجودات زیستی و منتقل‌کننده‌ی آنها به نسل‌های آینده؛
- وجود دارد و قابل بررسی است.

پیشرفت‌های اخیر در حوزه‌ی بایوسایبرنتیک، دانشمندان را قادر به کنترل و جهت‌دهی هر دو بخش به‌صورت متمرکز، توده‌ای، گسترده و از راه‌دور نموده به‌گونه‌ای که از طریق کنترل اعصاب مرکزی، کلیات ادراکات و واکنش‌های موجودات زیستی را و از طریق تولید توالی‌های جدید ژنوم از ابتدای طراحی تا انتهای عملیاتی نمودن آن، ویژگی‌ها و صفات بنیادین موجودات زیستی و نسل آتی آنها را کنترل می‌نمایند. با کمک بایوسایبرنتیک، می‌توان از کوچکترین واحد حیات در سطح میکرو ارگانیسم‌های نانومتری تا موجودات در سطح ماکرو را تحت کنترل درآورد و از آنها موجودیت‌هایی نوین ایجاد نمود که دارای قابلیت‌های کاملاً جدید و متفاوت از موجودات سابق هستند. همچنین می‌توان از موجودات زیستی، کاربردهای جدید و مورد نیاز به‌دست آورد؛ برای نمونه می‌توان با کنترل ویژگی‌های زیستی برخی حیوانات، از پتانسیل آنها قابلیت‌هایی نظیر تولید سوخت‌های زیستی و ترشح پیش‌سازهای داروهای پزشکی را به‌دست آورد که سابق بر این میسر

<sup>16</sup>Max Planck Institute for Biological Cybernetics

<sup>17</sup>Biocybernetics and Biomedical Engineering

<sup>18</sup>Journal "Biological Cybernetics"

<sup>19</sup>UCLA Biocybernetics Laboratory

نبوده است. از سوی دیگر می‌توان با الحاق ترانه‌های سایبری به موجودات زیستی، انواع فعالیت‌های عصبی، ارگانی و سیستمی آنها را به سمت دلخواه سوق داد؛ یعنی می‌توان مجموعه‌ای از فعالیت‌های خودآگاه و ناخودآگاه موجودات زیستی را از طریق دانش و تکنولوژی‌های بایوسایبرنتیک به کنترل در آورد. چنین دستاوردهای نوینی بر اساس نگاه بایوسایبرنتیک به پدیده‌های زیستی است که آنها را به مثابه کامپیوترهای زیستی در نظر می‌گیرد که نیازمند یک سیستم‌عامل کنترلی برای بهره‌برداری از توان سخت‌افزاری این کامپیوترها است. لذا تلاش دارد تا با خروجی‌های نوینی که از دانش بایوسایبرنتیک حاصل می‌شود، سیستم‌های عامل متناسب با این کامپیوترهای زیستی را طراحی و روی آنها نصب نماید. از آنجا که نگاه، اهداف و روش‌های اقدام بایوسایبرنتیک در شاخه‌های مختلف بایولوژی مطرح نبوده است، لذا نباید این دانش نوین را معادل بایولوژی و حوزه‌ی متریقی آن نظیر سینتتیک بایولوژی در نظر گرفت. وقتی صحبت از بایوسایبرنتیک می‌شود، منظور از آن دانش کاملاً جدیدی است که در هر سه حوزه‌ی مفاهیم، نظریات و روش‌شناسی، از طریق تلفیقی کاملاً هماهنگ میان دانش سایبرنتیک و بایولوژی به دنبال شناسایی و شناخت سیستم‌های فرماندهی و کنترل موجودات زیستی از درون و بیرون از آنها بوده تا بتواند از این طریق، کنترل سایبرنتیک بر آن پدیده‌ی زیستی را اعمال نماید. به همین دلیل است که یک آزمایشگاه و فضای کاری پیشرفته‌ی بایوسایبرنتیک، نه شباهتی به آزمایشگاه کاملاً الکترونیکی و کامپیوتری دانشمندان حوزه‌ی سایبر دارد، و نه فضایی است کاملاً زیستی با شمایل آزمایشگاه‌های زیستی که زیست‌شناسانی با روپوش سفید در آن مشغول به کار بر روی گونه‌های زیستی هستند؛ بلکه یک زیرساخت پیچیده و نوین است برای تحقق انواع کنترل‌ها بر پدیده‌های مختلف زیستی که حوزه‌هایی مثل مهندسی ژنتیک طبیعی و مصنوعی با تمام توان و پیچیدگی‌هایش، صرفاً یکی از زیربخش‌های آن می‌باشد.

در چنین فضایی، طراحی و آزمایش سیستم‌های عصبی مصنوعی، بازشناسی الگوریتم‌های محاسباتی موجودات زیستی برای فهم چگونگی تولید کدهای امور حیاتی‌شان، بازشناسی و بازسازی الگوی کنترل ژنوم، کشف الگوریتم‌های شناختی موجودات زنده به منظور کنترل شناخت آنها، اتصال و ارتباط عملیاتی و یکپارچه میان الگوهای زیستی از طریق یکسان‌سازی اطلاعات ارائه شده به آنها، آزمایش‌های مختلف بر سیستم‌های فرماندهی و کنترل زیستی و ... به عنوان نمونه‌هایی از حوزه‌ی مطالعاتی بایوسایبرنتیک انجام می‌پذیرد. همچنین از نکات بسیار مهم در تمایز بایوسایبرنتیک نسبت به شاخه‌های مختلف بایولوژی، آن است که بایولوژی دانشی است که عموماً مبتنی بر تجربیات آزمایشگاهی است و در سطح فیزیک هستی تعریف می‌شود. اما بایوسایبرنتیک، دامنه‌ی گسترده‌ای دارد که هر سه سطح فیزیک، متافیزیک و ترانس فیزیک هستی را مورد بحث، بررسی و مطالعه و کنترل قرار می‌دهد. سطح فیزیکی هستی، سطح طبیعیات است. متافیزیک، سطحی است که درباره‌ی موجودات «بما هو موجودات» به بحث و بررسی علمی می‌پردازد و سطح ترانس فیزیک یا ماوراء طبیعت، سطحی است که دانش‌های آن پیرامون پدیده‌های فرامادی صحبت می‌کنند. لذا رابطه‌ی بین فیزیک و متافیزیک، مصداق رابطه‌ی میان جزء و کل است و رابطه‌ی میان فیزیک با ترانس فیزیک، از نوع روابط علت و معلولی است.

پس در واقع، بایوسایبرنتیک علاوه بر بررسی منطق و کارکرد فرماندهی و کنترل در موجودات زیستی، به بررسی هویت متافیزیکی و علل ترانس فیزیکی پدیده‌های زیستی نیز می‌پردازد. حاصل چنین نگاهی است که



برخی مراکز پیشرفته‌ی علمی در سال‌های اخیر به تعریف پروژه‌هایی نظیر «ژن مقدس»<sup>۲۰</sup> می‌پردازند. ژن مقدس پروژه‌ای علمی است که یک ژن با نام ترا برنده ویزیکولی مونوآمین-۲۱۲ موجب تمایل انسان به سمت امور روحانی و عرفانی می‌شود که نخستین بار توسط «دین هیمر»<sup>۲۱</sup> (متخصص ژنتیک) بیان شده است. هدف پروژه‌ی مذکور چنین است که در نهایت بتوان با تغییرات ژنتیکی یا ایجاد ژنومی جدید که سابقاً وجود نداشته، ابعاد ایدئولوژیک انسان را دستخوش تغییرات مدنظر نموده و از این طریق حوزه‌ی معرفتی انسان را پیش از تولد وی تحت سیطره و کنترل در آورد که مصداق کنترل انسان به‌عنوان یک پدیده‌ی زیستی در سطوح متافیزیک و ترانس‌فیزیک است.

به‌طور کل، بایوسایبرنتیک را می‌توان از یک سو دانشی برای طراحی و ساخت مسیرهای نوین کنترل زیستی که در طبیعت وجود ندارند؛ و از سوی دیگر بازتعریف‌کننده‌ی مسیرهای کنترل زیستی موجود در طبیعت دانست. به‌عبارت دیگر خلق نوین ساز و کارهای کنترل زیستی و همچنین طراحی و ساخت گونه‌ای از موجودات با قابلیت‌های متفاوت شناختی، ادراکی و محاسباتی و حتی طراحی مجدد اکوسیستم‌های بایولوژیکی طبیعی (که در حال حاضر وجود دارند) به‌نحوی که مد نظر طراح است (حالتی که در حال حاضر وجود ندارد) در دانش بایوسایبرنتیک به‌واقعیت بدل شده است.

## ۴.۳ دستاوردهای بایوسایبرنتیک در حوزه‌ی فرماندهی و کنترل زیستی

بر اساس آنچه بیان شد، اهم مصادیقی که به‌عنوان دستاوردهای بایوسایبرنتیک در زمینه‌ی تحقق فرماندهی و کنترل پدیده‌های زیستی قابل طرح است عبارتند از:

۱. **ساخت مصنوعی پدیده‌های زیستی:** یعنی ساخت یک موجود زنده، بدون حضور خود آن موجود و صرفاً با ساخت اطلاعات DNA آن. به‌عنوان مثال، ژنوم یک باکتری از طریق اتصال قطعات کوچک DNA به یکدیگر ساخته می‌شود حتی اگر در آن محیط، هیچ باکتری‌ای به‌عنوان مولد وجود نداشته باشد. این امر برای گیاهان، ویروس‌ها، سلول‌ها، حیوانات، انسان‌ها و حتی موجودات جدید زیستی که تاکنون به‌صورت طبیعی وجود نداشته‌اند میسر است.

۲. **ساخت مسیرهای زیستی جدید:** ایجاد مسیرهای زیستی که در دنیای طبیعی وجود ندارند یا اگر وجود دارند، فعالیت ویژه‌ای که مد نظر ما است را انجام نمی‌دهند. برای نمونه، آنزیمی شناسایی و تولید می‌شود که در تولید ماده‌ی A کاربرد دارد، در حالی که ماده‌ی A در هیچ موجود زنده‌ای تولید نمی‌شود. سپس ژن این آنزیم در موجودی قرار می‌گیرد که پیش‌ماده‌ی A در آن وجود دارد تا از این طریق ماده‌ی A تولید گردد. پایه‌ی چنین مبحثی در سینتتیک بایولوژی مطرح است اما دریافت کاربردهای کنترلی، اتکا بر بایوسایبرنتیک دارد. برای مثال به‌صورت سنتتیک، آنزیمی تولید شود که

<sup>20</sup>God Gene

<sup>21</sup>VMAT2

<sup>22</sup>Dean Hamer

پدیده‌های زیستی نظیر انسان را با کنترل‌گرهای مغناطیسی یا اپتیکی هماهنگ سازد تا از طریق بتوان رفتارها و کنش‌های اجتماعی افراد را کاملاً تحت کنترل و نظارت درآورد.

به عبارت دیگر می‌دانیم که جهان سایبری از دنباله‌های دودویی متشکل از ۰ و ۱ تشکیل شده است، در نتیجه محاسبات آن در دستگاه لگاریتمی با مبنای ۲ انجام می‌شود. از سوی دیگر جهان زیستی از دنباله‌های چهارتایی شامل آدنین<sup>۲۳</sup>، تیمین<sup>۲۴</sup>، سیتوزین<sup>۲۵</sup> و گوانین<sup>۲۶</sup> که به ترتیب با اختصار A، C، T و G نمایش داده می‌شوند، ساخت یافته است. لذا انجام محاسبات مربوطه در دستگاه لگاریتمی با مبنای ۴ صورت می‌پذیرد. از سوی دیگر تبدیل دستگاه‌های لگاریتمی از مبنایی به مبنای دیگر، امری میسر است. این به معنای تبدیل محاسبات اطلاعاتی سایبرنتیک و بیولوژیک به یکدیگر است که می‌تواند زمینه‌ساز فضای یکپارچه‌ی کنترل اطلاعات و گامی در راستای کنترل پدیده‌های زیستی مبتنی بر زیرساخت سایبرنتیک می‌باشد.

لذا ظرفیت علمی و امکان عملیاتی نگارش و سنتز کدهای زیستی، بدون هیچگونه محدودیتی و از طریق ساز و کار سایبرنتیکی وجود دارد. این مهم توسط «پل دیویس»<sup>۲۷</sup>، فیزیک‌دان دانشگاه ایالتی آریزونا در فصل دوم کتاب «شیطان در ماشین»<sup>۲۸</sup>، چنین بیان شده است: «با اندکی توجه در می‌یابیم که تحلیل کلود شانون، کاربرد مستقیمی در زیست‌شناسی دارد. اطلاعات با استفاده از رمزهای ژنتیکی همگانی در دی‌ان‌ای ذخیره شده‌اند. محتوای اطلاعاتی ژن‌ها از طریق mRNAها به ریبوزومها ارسال می‌شود و در آنجا پس از رمزگشایی، برای ساختن پروتئین‌ها از رشته‌ای از اسیدهای آمینه مورد استفاده قرار می‌گیرد. اما کانال اطلاعاتی mRNA، ذاتاً شلوغ، پرهیاهو و مستعد خطا است. بنابر این کتاب راهنمای حیات به‌طور منطقی، معادل با تحلیل شانون از اطلاعات رمزگذاری شده‌ای است که از کانال ارتباطی پراشویی ارسال می‌شود».

۳. توسعه و تعمیق فرماندهی و کنترل موجودات زیستی در مقیاس گسترده و کلان: به‌طور کلی، محل فرماندهی و کنترل در یک موجود تک سلولی، اندامک هسته‌ای آن موجود محسوب می‌شود و در صورتی که یک موجود پر سلولی بوده و دارای سیستم عصبی باشد، شبکه‌ای درهم پیچیده از سلول‌های عصبی آن موجود تحت عنوان مغز، مرکز فرماندهی و کنترل آن موجود به‌شمار می‌آید.

عوامل بیوسایبرنتیک می‌توانند با در دست گرفتن مرکز فرماندهی کنترل سلول به عنوان مثال تغییر در ژنوم سلول و افزودن یا کاستن اطلاعات ژنتیکی خاص به آن، ظرفیت آن را در اختیار خود داشته باشند. برای نمونه می‌توانند پس از کنترل مرکز فرماندهی سلول، دستورات جدیدی را به سلول داده و آن را در راستای برنامه‌ی خود مدیریت نمایند. همین موضوع را می‌توان برای مرکز فرماندهی و کنترل

<sup>23</sup> Adenine

<sup>24</sup> Thymine

<sup>25</sup> Cytosine

<sup>26</sup> Guanine

<sup>27</sup> Paul Davies

<sup>28</sup> The Demon in the Machine: How Hidden Webs of Information Are Solving the Mystery of Life?

موجودات زیستی یعنی مغز نیز در نظر گرفت. پس در صورتی که بتوان مغز را کنترل نمود، می‌توان اکثر ظرفیت حیاتی موجودات پرسلولی را نیز به دست گرفته و کنترل کرد. از این رو پروژه‌های کنترل مغز که به صورت سخت و نرم در حال انجام است، جایگاه بسیار قابل توجهی در این حوزه یافته‌اند.

۴. **تعمیق توانمندی تصرف، تغییرات بنیادین و حتی ایجاد آنچه سابقاً وجود نداشته در حوزه‌ی کنترل پدیده‌های زیستی در فرایندهای نظام هستی:** به دلیل توجه به بایوسایبرنتیک، دانشمندان متوجه این نکته‌ی مهم شده‌اند که تمام پدیده‌های زیستی - خصوصاً انسان - همانند یک کامپیوتر پیشرفته‌ی زیستی است که پتانسیل اجرایی بسیار بالایی دارد اما سیستم‌عاملی که این پتانسیل را به نحو مدنظر فعال نماید؛ در اختیار انسان نیست.

حال با استفاده از دیدگاه و تکنولوژی‌های مبتنی بر بایوسایبرنتیک، توانسته‌اند سیستم‌های عاملی که از این کامپیوتر زیستی پیشرفته، پردازش‌ها و خروجی‌های مدنظرشان را دریافت نماید؛ طراحی نموده و عملیاتی سازند. در این مسیر، ادبیات و حتی پروژه‌هایی نظیر هُمودئوس<sup>۲۹</sup>، محاسبات DNA، انسان نسخه‌ی ۲۰۲۰ سال‌ها است که تعریف شده و در مسیر اجرای آنها گام‌هایی نیز برداشته شده است.

۵. **تغییر و حتی حذف انواع گونه‌ها و نژادهای زیستی در محیط‌زیست، گیاهان، حیوانات و حتی انسان:** جنس تغییرات زیست‌محیطی مبتنی بر سایبرنتیک؛ شبیه به تغییرات زیستی سابق نیست. به عنوان مثال شناسایی، استخراج و تغییر پوشش جانوری، آبی و گیاهی غالب در مناطقی از بخش‌های مختلف یک کشور، می‌تواند بر اساس تغییراتی از جنس بایوسایبرنتیک باشد که در آینده، آثار متعدد اقتصادی، امنیتی و زیست‌محیطی فراوان برای عموم مناطق جهان رقم خواهد زد. به این نوع از تغییرات که ذیل بایوسایبرنتیک، خاصاً معطوف به محیط‌زیست شکل می‌پذیرد؛ تغییرات اِکوسایبرنتیکی گفته می‌شود که یک شاخه‌ی مطالعاتی بسیار مهم است. بعضی اقدامات نظیر حذف نژاد یک گونه‌ی خاص گیاهی یا جانوری؛ یا بر خلاف آن ایجاد گونه‌های زیستی جدید به طوری که پس از رهاسازی در اکوسیستم، کاری را انجام دهند که مد نظر طراح است نیز در زمره‌ی تغییرات بایوسایبرنتیک می‌باشد.

۶. **ایجاد بیماری‌های نوین و کاملاً متفاوت با بیماری‌های تجربه شده در تاریخ بشر از طرق مختلف نظیر تولید پاتوژن‌های جدید<sup>۳۱</sup> با تمرکز بر کنترل مبانی و مبادی کنترلی انسان از سلول تا سیستم عصبی:** تاکنون تصور بر این بوده که عوامل بیماری‌زا، عموماً از طریق داروها کنترل می‌شوند. برخی از عوامل جدید بایوسایبرنتیک، هر چند نسبت به پدیده‌های زیستی نظیر انسان، مهاجم هستند اما ذات زیستی ندارند. برای نمونه، عواملی که با فرکانس فعال / غیر فعال می‌شوند (موسوم به: Activated Frequency FAA) باعث بروز علائم بالینی منفی در انسان

<sup>29</sup>Homo Deus

<sup>30</sup>Human 2.0

<sup>31</sup>عوامل بیماری‌زای جدید

و سایر پدیده‌های زیستی می‌گردند و درمان دارویی ندارند. عموماً این دست عوامل به‌گونه‌ای طراحی می‌شوند که به‌راحتی درمان‌پذیر نیستند. در این شرایط متخصصان پزشکی اقدام به درمان‌های رایج می‌کنند در حالی که نه تنها اثر مثبتی نخواهد داشت، بلکه عوارض دارویی را نیز به فرد تحمیل می‌نمایند.

۷. **طرح‌ریزی انسان از حیث فرماندهی و کنترل مبتنی بر ژنوم:** کنترل انسان، چه پیش از تولد و چه در زمانی که یک انسان بالغ است؛ همواره یکی از دغدغه‌هایی بوده که در پروژه‌های تحقیقاتی مراکز پیشرفته‌ی علمی بایوسایبرنتیک، مورد بررسی و مطالعه قرار گرفته است. برای اینکه بتوان انسانی بالغ را تحت کنترل داشت؛ یکی از روش‌های آزموده شده، ایجاد یک رابط بین مغز و سیستم‌های کامپیوتری است که می‌تواند دستورات را به‌صورت سیستمی به مغز فرد ارائه داده و فرد با اتخاذ تصمیم اقدام به عمل نماید.

در این راستا پروژه‌هایی که بتوانند چنین رابطی را ایجاد نمایند می‌توانند بسیار حائز اهمیت باشند. آژانس تحقیقات پیشرفته دفاعی ایالات متحده آمریکا (دارپا)، با قدم گذاشتن در این فضا اقدام به طراحی و اجرای پروژه‌هایی نظیر «بازیابی حافظه‌ی فعال» و همچنین طراحی «سیستم مهندسی عصبی» نموده است. این آژانس به‌دنبال طراحی یک رابط است که شبکه‌ی گسترده‌ای از بافت‌های عصبی را شکل می‌دهد. رابط مذکور از طریق ایمپلنت در بالای قشر مغزی جایگذاری می‌شود. ساخت چنین رابطی، برقراری ارتباط به‌صورت بدون وقفه با مغز را ممکن می‌کند. گفته شده که این رابط عصبی، امکان درک فرایند پردازش‌های مغزی و رمزگشایی زبان گفتاری را به محققان خواهد داد. چنین سیستمی می‌تواند به مغز انسان کمک کند تا مستقیماً به مجموعه‌ای عظیم از اطلاعات، از تصاویر گرفته تا ویدیوها دسترسی داشته باشد و در عین حال این امکان را برای کامپیوترها فراهم می‌کند تا برای مثال آن چه را که ما با چشم‌مان می‌بینیم، ببینند.

سابقاً چنین مطالعاتی در اواخر دهه‌ی ۸۰ شمسی در کشور در حال انجام بوده اما به‌دلایل نامشخصی متوقف شده است. اما مقالات علمی حاصل از مطالعات آن ایام، کمک زیادی به فهم عملیاتی بایوسایبرنتیک می‌نمایند. برای مثال مقاله‌ی پژوهشی «کنترل ذهن با فناوری صدای خاموش خیال یا واقعیت؟» که حاصل سال‌ها مطالعه‌ی علمی روی چنین مواردی بوده، در پاییز سال ۱۳۹۱ به پرسش‌های زیادی بر اساس اسناد پاسخ می‌دهد که حتی امروز نیز برای جامعه‌ی علمی کشور مورد سؤال قرار دارند.

البته مثال فوق، یک نمونه‌ی اولیه از پروژه‌های کنترل انسان مبتنی بر بایوسایبرنتیک است. امروزه استفاده از تکنولوژی‌ها و روش‌های جدیدتر مطرح است، برای نمونه استفاده از نانوپارتیکل‌های مختلف نظیر ذرات نانو اکسید گرافن، تیتانیوم دی‌اکسید و ... در بدن انسان و سپس تحت تأثیر قرار دادن آنها از طریق میدان امواج؛ به اهدافی عمیق‌تر و وسیع‌تر از آنچه در مدل اولیه بیان شد، دست می‌یابند.

## ۴ نتیجه گیری

عصر حاضر، عصر تولید قدرت و اعمال کنترل بر اساس دانش‌های سایبرنتیک پایه و تکنولوژی‌های حاصل از آنها است؛ لذا تمام امور اساسی هر کشور از خط‌مشی‌گذاری تحقیق و توسعه‌ی دانش‌های مختلف در مجموعه‌های علمی، پژوهشی و دانشگاهی تا طرح‌ریزی الگوهای حاکمیتی برای پاسخ به موضوعات راهبردی نظیر دشمن‌شناسی، پدافندهای بلادرنگ و مؤثر در مقابل تهدیدات نوین، طرح‌ریزی‌های آفندی، طراحی و پیاده‌سازی راهبردهای بازدارندگی<sup>۳۲</sup> و به‌طور کل حفظ و ارتقاء قدرت ملی در سطح منطقه و بین‌الملل، کاملاً به دانش‌های ماحصل از دانش سایبرنتیک وابسته است و بدون به‌روزرسانی علمی نمی‌توان در موارد فوق و سایر موضوعات مهم، به نتایج مطلوب و به‌روز دست یافت. علت جدی این تغییر مهم، تغییر مبنای منطق دانش در جهان است؛ بدین صورت که مبنای دسته‌بندی دانش‌ها در دهه‌های اخیر به سمت مفهوم اطلاعات و اعمال کنترل بر اساس جریان اطلاعات سوق یافته، به‌گونه‌ای که هر چقدر یک دانش در حوزه‌ی اطلاعات اثرگذارتر باشد، دانش بنیادین‌تر و مهم‌تری تلقی می‌شود. لذا دانش سایبرنتیک که دانش پایه در کنترل جریان اطلاعات و اعمال کنترل از این طریق است؛ به‌عنوان دانش ثقل و مرکزی قرار گرفته و با راهیابی منطق سایبرنتیک به سایر دانش‌ها، تحولی عظیم در منظومه‌ی دانش‌ها رقم خورده است. از این رو باید توجه جدی شود که بایوسایبرنتیک، بایولوژی یا سایبرنتیک نیست اما نیازمند پیشرفته‌ترین حوزه‌های بایولوژی و سایبرنتیک و افزوده شدن مطالعات میان‌رشته‌ای است که در راستای منطق سایبرنتیک، موجودات زیستی را مطالعه نموده و به‌صورت عملیاتی کنترل نماید.

بر این اساس، در زمان حال و آینده نزدیک، شاهد آن خواهیم بود که حوزه‌های مختلف از اقتصاد گرفته تا سیاست، از تکنولوژی‌های نوین ارتباطی و محاسباتی تا الگوهای نوین جامعه‌شناختی، از عصب‌شناسی تا جدیدترین روش‌های درمانی در پزشکی؛ همگی تحت تأثیر نگاه بایوسایبرنتیک، روش‌های علمی آن و تکنولوژی‌های حاصل از آن قرار خواهد گرفت؛ زیرا در تمامی حوزه‌های فوق و سایر حوزه‌هایی که با پدیده‌های زیستی - خصوصاً انسان - سر و کار دارند؛ نگاه بایوسایبرنتیک بسیار نافذ و تأثیرگذار است. در این راستا ضرورت دارد به روزرسانی علمی کشور در حوزه‌های مختلف انجام شود که موارد زیر بخشی از آن می‌باشد:

۱. شناخت دقیق مفهومی، نظری و عملی دانش سایبرنتیک؛
۲. الگوی طراحی و تولید دانش‌های سایبرنتیک پایه حاصل شده و در مجموعه‌های علمی و دانشگاهی کشور مورد توجه قرار گیرد؛
۳. ضرورت دارد برهم‌کنش و اثرگذاری سایبرنتیک بر سایر دانش‌ها تبیین و مشخص شود؛
۴. رویکرد طراحی چشم‌انداز و آینده‌پژوهی نظام علمی کشور به سمت موارد فوق سوق یابد؛
۵. تکنولوژی‌ها و فضای آزمایشگاهی منطبق با دانش‌های جدید، شناسایی و عملیاتی گردد؛

<sup>32</sup>Deterrence Strategy

حوزه‌ی نوین دانش بایوسایبرنتیک نیز عملاً حاصل مراحل پنجگانه‌ی فوق است که یقیناً شناخت آن از سویی و طرح‌ریزی‌های علمی، تحقیقاتی و عملیاتی برای آن از سوی دیگر نیز نیازمند عملیاتی شدن مراحل فوق‌الذکر می‌باشد.

البته باید در نظر داشت که دانش و تکنولوژی، همواره دو لبه دارد و در عین اینکه می‌تواند سودمند و نافع باشد؛ ظرفیت تبدیل شدن به تهدید را نیز دارا است. لذا جمهوری اسلامی ایران می‌تواند با تسلط بر حوزه‌های نظری و عملی بایوسایبرنتیک، علاوه بر تأمین بسیاری از حوزه‌های ضروری و مورد نیاز کشور، نسبت به تهدیدات نوین ذی‌ربط نیز الگوها و برنامه‌های پدافندی را تدبیر و تدوین نماید. در پایان باز هم بر این نکته‌ی بسیار مهم در خصوص دانش بایوسایبرنتیک تأکید می‌گردد که معادل دانش زیست‌شناسی نیست و بسیار فراتر از آن است زیرا:

۱. سطح کنش‌گری را فراتر از سقفی تعریف می‌کند که در زیست‌شناسی مطرح شده است. به عبارت دیگر در بایوسایبرنتیک، جامعه‌ی انسانی به مثابه یک «سوپر ارگانیسم» دیده می‌شود که می‌توان تمامیت آن را کنترل نمود و در دو سطح میکرو ارگانیسم و ماکرو ارگانیسم که در زیست‌شناسی تعریف شده، متوقف نشده است.

۲. به دلیل اتکا به منطق فرماندهی و کنترل سایبرنتیک، دانش بایوسایبرنتیک از سایر عوامل مؤثر بر سیستم‌های فرماندهی و کنترل زیستی استفاده نموده و محدود به حوزه‌ی بایولوژی نشده است. برای مثال استفاده از امواج و تحت تأثیر قرار دادن عملکرد انسان از این طریق - که در مبحث بایو رزونانس مطرح می‌شود- از جمله جنبه‌های کنترلی در بایوسایبرنتیک است.

همچنین توصیه می‌شود به متخصصان علاقمند که برای ادامه‌ی مسیر شناخت دانش بایوسایبرنتیک و تسلط هر چه بیشتر بر آن، اولاً اسناد پایه‌ی علمی که مبانی این دانش در آنها مطرح شده، ثانیاً مقالات علمی که تازه‌های نظری و عملی بایوسایبرنتیک را دربر دارند و ثالثاً اسناد راهبردی کشورهایی که در حوزه‌ی بایوسایبرنتیک فعال هستند (نظیر آمریکا، انگلیس و آلمان) را به صورت توأمان مطالعه نمایند تا هر چه دقیق‌تر با پیوستار گذشته، حال و آینده‌ی این دانش نوین آشنا گردند.

## مراجع

- [۱] مجله‌ی علمی مطالعات عملیات روانی، شماره ۱۰، پاییز ۱۳۸۴، صفحات ۲۸ تا ۵۱.
- [۲] حمید هادیان، «روحیه‌ی جنگی در پروژه‌ی گذار ارتش آمریکا به قرن بیست و یکم»، مجله‌ی علمی مطالعات عملیات روانی، شماره ۱۰، پاییز ۱۳۸۴، صفحه‌ی ۴۶.
- [۳] محمدعلی شکوهیان‌راد، «اخلاق در سیستم‌های فرماندهی و کنترل، مبنای چهارچوب نوین طراحی تهدیدات و بحران‌ها»، یازدهمین کنفرانس ملی فرماندهی و کنترل، تهران، دانشگاه صنعتی امیرکبیر پاییز ۱۳۹۸.
- [۴] پایگاه azquotes، بخش نویسندگان، صفحه‌ی آندره ماری آمپر، پیوند:

<https://www.azquotes.com/quote/899233>



- [۵] کاظم معتمدنژاد، «وسایل ارتباط جمعی»، تهران، ۱۳۸۶ ه.ش، انتشارات دانشگاه علامه طباطبایی، چاپ ششم، ص ۴۱-۴۲.
- [۶] نوربرت وینر، «استفاده‌ی انسانی از انسان‌ها»، ترجمه‌ی مهرداد ارجمند، تهران، سازمان انتشارات و آموزش انقلاب اسلامی، ۱۳۶۶ ه.ش، صفحه‌ی ۱.
- [۷] محمدعلی شکوهیان‌راد، «نظریه‌ی جنگ در عصر سیستم‌های فرماندهی و کنترل»، تهران، مؤسسه‌ی آموزشی و پژوهشی شهید صیاد شیرازی، ۱۳۹۷، صفحه‌ی ۵۹.
- [۸] دایرةالمعارف علمی بایوسایبرنتیک، صفحه‌ی نخست به پیوند:  
<http://www.biological-cybernetics.eu/index.html>
- [۹] پایگاه علمی اسلام کوئست، «فیزیک و متافیزیک چیست؟ و رابطه آن دو چگونه است؟»، ۲۱/۲/۱۳۸۸، پیوند:  
<https://www.islamquest.net/fa/archive/fa5252>
- [۱۰] مرکز راهبردی فناوری‌های همگرا، «زیست‌شناسی مصنوعی، در گفتگو با آقای دکتر مرعشی»، ۱۰ مرداد ۱۳۹۶، پیوند:  
<https://nbic.ir/news/60060>
- [۱۱] پل دیویس، «شبح در ماشین»، مترجم: تورج حوری، انتشارات مازیار، ۱۳۹۹، صفحه‌ی ۴۷.
- [۱۲] سید حسین محمدی نجم، مجله‌ی علمی-پژوهشی مطالعات عملیات روانی، شماره ۳۴، پاییز ۱۳۹۱، صفحات ۱۹۱ تا ۲۰۶.
- [13] MartaKozuń and Coworks, "Influence of atherosclerosis on anisotropy and incompressibility of the human thoracic aortic wall," Biocybernetics and Biomedical Engineering, Volume 41, Issue 1, January–March 2021, Pages 15-27.
- [14] Vladimir L. Kodkin, "Digital Identification of the Human Condition as a Prerequisite for the Effectiveness of the Organizational Automation (Biocybernetic) Systems Operation," Journals Sensors, Volume 22, Issue 10, DOI 10.3390/s22103649.
- [15] Dmitry.A. Novikov, "Cybernetics, From Past to Future," Moscow, Springer, 2015, Page 1.
- [16] Dean Hamer, "The God Gene: How Faith Is Hardwired Into Our Genes," Anchor Books, 2005, ISBN 0-385-72031-9.
- [17] Max Planck Society, "Reproductive genome from the laboratory," 17 Feb 2020, Link: <https://phys.org/news/2020-02-reproductive-genome-laboratory.html>.
- [18] Lauren Thau and coworks, "Anatomy, Central Nervous System," National Library of Medicine (NIH), Oct 2021, Link: <https://www.ncbi.nlm.nih.gov/books/NBK542179/>.
- [19] Dr. Joanna Arthur, "Neural Engineering System Design (NESD)," DARPA, Year 2022, Link: <https://www.darpa.mil/program/neural-engineering-system-design>.



## امکان سنجی تقنین در فضای مجازی با تأکید بر اصول قانون اساسی

زهرا رئوفی فرد<sup>۱</sup>، فیروز اصلانی<sup>۲</sup>

<sup>۱</sup> دانشجوی دکتری، دانشکده حقوق و علوم سیاسی، دانشگاه تهران  
zahra.raoofi.fard@ut.ac.ir

<sup>۲</sup> دانشیار، دانشکده حقوق و علوم سیاسی، دانشگاه تهران  
aslanif@ut.ac.ir

### چکیده

اینترنت، به عنوان یکی از پدیده‌های نوین معاصر، موجب تحول جوامع بشری شده است. حاکمیت می‌بایست با اتکا به قواعدی به تنظیم روابط افراد شهروندان در فضای مجازی بپردازد. بی‌گمان، دامنه‌ی اختیارات و آزادی‌های مردم در فضای مجازی کاملاً متفاوت از فضای حقیقی است. حفظ حریم خصوصی، منع هرزه‌نگاری، حمایت از حق نشر مؤلفان و... مستلزم ایجاد محدودیت دامنه‌ی فعالیت کاربران است. قانون اساسی، خطوط کلی حقوق و آزادی‌های شهروندان را تبیین می‌کند. پرسشی که مطرح می‌شود این است که آیا قوانین فعلی می‌تواند پاسخگوی مشکلات فضای مجازی باشد و یا نیازمند تقنین در این حوزه هستیم؟ به نظر می‌رسد قواعد خودتنظیمی نمی‌تواند به تنظیم روابط مردم در این فضا بپردازد. به یاری تفسیر و تحلیل قوانین موجود، نمی‌توان اینترنت را قاعده‌مند ساخت. در این خصوص وضع قانون جامع امری ضروری است این نوشتار با رویکردی توصیفی - تحلیلی (با مراجعه به منابع کتابخانه‌ای) درصدد پاسخ دادن به آن است.

**کلمات کلیدی:** خودتنظیمی، قانون جامع، حق نشر، اینترنت، فیلترینگ.

### ۱ مقدمه

در دنیای معاصر، فضای مجازی کانونی برای فعالیت‌های روزانه بشری است. ارسال پیام‌ها، به اشتراک گذاشتن فایل‌ها و تصاویر، مشاهده کلیپ و فیلم‌ها، تبادل معلومات و... تنها بخش‌هایی از رخدادهایی است که از طریق اینترنت انجام می‌شود. حقوق نمی‌تواند نسبت به این وقایع بیگانه باشد. صیانت از ارزش‌ها و پاسداری از حقوق و منافع شهروندان اقتضا می‌نماید که قانون‌گذار با وضع قواعدی نسبت به قاعده‌مند نمودن آن اقدام نماید. در سال‌های اخیر، قوانین متعددی در حوزه تجارت الکترونیک، جرائم رایانه‌ای و... به تصویب رسیده است. در پرتو قوانین مزبور، قانون‌گذار ضمن تبیین بایدها و نبایدهایی شهروندان را مکلف

و ملزم به تبعیت و پیروی از آنها می‌نماید؛ با وجود این، باید توجه داشت اینترنت در مقایسه با سایر وسایل ارتباطی پیچیدگی بیشتری دارد. دخالت عوامل مهم سخت‌افزاری و نرم‌افزاری بر پیچیدگی آن افزوده است. اینترنت را نمی‌توان با سایر رسانه‌ها و وسایل ارتباط جمعی (همچون رادیو و تلویزیون) مقایسه نمود. ممانعت از برهم خوردن نظم و آسایش عمومی، حمایت از ارزش‌های اخلاقی، فرهنگی و اجتماعی و ... از اسباب لزوم مدیریت فضای مجازی هستند. در این خصوص، ضرورت تبیین خط‌مشی و چارچوب کلی برای مدیریت فضای مجازی امری اساسی است.

کشورهای مختلف در این زمینه به شیوه متفاوتی عمل نموده‌اند: برخی سیاست فیلترینگ تارنماها را اعمال می‌کنند و پاره‌ای نیز صرفاً هرزه‌نگاری کودکان را ممنوع نموده‌اند و گروهی دیگر نیز اولویت را به حریم خصوصی داده‌اند. در کشور ما قواعد چندانی پیرامون استفاده از اینترنت در مدارس، ادارات دولتی، دسترسی آزاد به اطلاعات، حریم خصوصی، کپی‌رایت و ... وجود ندارد. جرم‌انگاری پاره‌ای از اعمال اگرچه سودمند است، لیکن چارچوبی کلی را ارائه نمی‌دهد.

در حوزه فضای مجازی چند کتاب وجود دارد من جمله آنها می‌توان به کتب جایگاه فقهی حقوقی فیلترینگ در رسانه‌های مجازی از دیدگاه مذاهب خمسه، حقوق بشر و اینترنت اشاره نمود.<sup>۱</sup> این کتب مسئله اینترنت و فضای مجازی را به نحو کلی مورد بررسی قرار داده‌اند و بین قواعد پیرامون نظام حاکم بر آن خودداری نموده‌اند؛ همچنین در حوزه مقالات نیز مقاله‌های متعددی پیرامون فضای مجازی به رشته تحریر در آمده است.<sup>۲</sup> هیچ یک مسئله مورد پژوهش را به طور جامع بررسی نکرده است. نوآوری پژوهش نسبت به نوشتارهای مزبور ارائه راهکار اساسی در خصوص چالش‌های فضای مجازی است.

تحلیل تفصیلی سیاست‌های تقنینی در فضای مجازی با تأکید بر اصول قانون اساسی، پرسش‌هایی را مطرح می‌سازد: آیا در حوزه فضای مجازی نیازی به وضع قانونی جامع هستیم یا تفسیر قوانین موجود و قواعد خودتنظیمی می‌تواند روابط شهروندان را تنظیم کند؟

این پژوهش، با رویکردی توصیفی - تحلیلی و با استفاده از منابع کتابخانه‌ای همچون (کتب، مقالات و ...) همچنین استفاده از مهم‌ترین منابع موجود در این حوزه، ضمن واکاوی دیدگاه‌های مطرح شده پیرامون موضوع پژوهش امکان‌سنجی اعمال آنها را با تکیه بر اصول قانون اساسی بررسی می‌نماید. در خصوص موضوع پژوهش، تحقیقات محدودی انجام شده است؛ از میان پژوهش‌های انجام شده، می‌توان به مقاله قانون‌گذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران نوشته ضیایی و شکیب نژاد اشاره نمود، همچنین گستره و قلمرو حریم خصوصی در فضای مجازی نوشته فتحی و شاه‌مرادی و در نهایت به مقاله تبیین سیاست‌گذاری فضای مجازی در جمهوریت اسلامی ایران نوشته فرهنگی، میرترابی و گلشنی اشاره نمود. در این نوشتارها، صرفاً فضای مجازی در حوزه مسائلی همچون فیلترینگ، ارائه سیاست‌های کلی در فضای مجازی و اصول

<sup>۱</sup> روزبهانی، محمدرضا (۱۳۹۳) جایگاه فقهی حقوقی فیلترینگ در رسانه‌های مجازی از دیدگاه مذاهب خمسه، کتاب آوا، چ اول، تهران؛ هیک، استیون و ادوارد اف هلپین و اریک هوسکینز (۱۳۹۳ ه.ش)، حقوق بشر و اینترنت، ترجمه قاسم زمانی و مهناز بهرام‌لو، تهران: انتشارات خرسندی، چ. اول.

<sup>۲</sup> فتحی، یونس و خیراله شاه‌مرادی، گستره و قلمرو حریم خصوصی در فضای مجازی، مجله حقوقی دادگستری، ش. ۹۹. نصراللهی، محمدصادق (۱۳۹۰ ه.ش) ضرورت‌یابی قانون جامع رسانه‌های همگانی در جمهوری اسلامی ایران، مطالعات فرهنگ - ارتباطات، ش ۴۶.

مدیریت این فضا به طور کلی مورد تبیین قرار گرفته است و از ارائه راهکار در حقوق ایران خودداری شده است. ضمناً در نوشتارهای مزبور، چالش‌های فضای مجازی به صورت پراکنده و اجمالی بررسی شده است. این مقاله، ضمن تحلیل دیدگاه‌های نوین در باب مدیریت فضای مجازی، چالش‌های موجود در آن را تبیین نموده است. ضمناً تقنین احتمالی در این حوزه با تأکید بر اصول قانون اساسی تحلیل شده است. مقاله حاضر مشتمل بر دو قسمت است: در قسمت نخست، مدیریت فضای مجازی و در قسمت دوم، حوزه‌های تقنین در فضای مجازی را بررسی و تحلیل می‌کنیم.

## ۲ مدیریت فضای مجازی

مراد از مدیریت فضای مجازی، اعمال راهکارهایی پیرامون فیلترینگ، وضع قواعد در مورد این فضا، محدود نمودن دسترسی شهروندان و ... است (روزبهنانی، ۱۳۹۳: ۸۶). بررسی تحلیلی مدیریت فضای مجازی، پرسشی را مطرح می‌سازد: چه نیازی به لزوم مدیریت فضای مجازی وجود دارد؟ در مدیریت فضای مجازی از چه نظامی (الگو یا ساختاری) می‌بایست تبعیت نمود؟

### ۱.۲ ضرورت مدیریت فضای مجازی

فضای مجازی دارای ویژگی‌های خاص و منحصر به فردی است؛ این فضا آکنده از تصاویر چندبعدی، اخبار، اطلاعات، سایتها، پایگاه‌های علمی و ... است، شهروندان بدون رابطه دیداری با یکدیگر ارتباط برقرار می‌سازند. یکی از مظاهر حاکمیت دولت‌ها، مدیریت فضای مجازی از طریق وضع قاعده و تبیین ضمانت اجرای تخطی از قانون است. تردیدی وجود ندارد که فضای مجازی علی‌رغم مزایای فراوان، مشکلات زیادی از قبیل امکان نقض حریم خصوصی، افشای اطلاعات، انحرافات اخلاقی، نشر اکاذیب، فریب شهروندان و ... را دارد. قانون‌گذار می‌بایست با اعمال تدابیری، ضمن فراهم آوردن زمینه‌های استفاده شهروندان از فضای مزبور، از بروز مشکلات احتمالی بکاهد. این امر از طریق مدیریت فضای مجازی انجام می‌شود.

بی‌گمان، دولت‌ها دارای حاکمیت مستقل و دائمی هستند؛ توانایی فرماندهی آنها در کنترل امور از قدرت عمومی سرچشمه می‌گیرد. قدرت دولت از نهاد بیرونی اخذ نمی‌شود (عباسی، ۱۳۹۳: ۵۰؛ مدنی، ۱۳۷۴: ۷۴). حاکمیت دولت، پلی میان نظم عمومی و نظم بین‌المللی است که موجب پیوند آنها به یکدیگر می‌شود (گرچی از ندریانی، ۱۳۸۸: ۱۶). خصیصه فراملی و جهانی بودن اینترنت نمی‌تواند مانعی در کنترل آن توسط دولت شود؛ صیانت از حقوق شهروندان اقتضا می‌کند که قانون‌گذار مبادرت به مدیریت آن نماید.

یکی از نویسندگان معتقد است رسانه‌های گروهی نقشی مهم در آگاهی عمومی مردم دارند. بسیاری از تحلیل‌گران سیاسی از رسانه‌های مزبور به منظور آگاه‌سازی مردم استفاده می‌کنند. ممانعت از فعالیت رسانه‌های مزبور، موجب انحراف و فساد جامعه می‌شود. در این میان گروهی به دنبال انحصارطلبی آنها و دیکته نمودن عقاید خویش هستند. پاره‌ای نیز تحمل انتقاد را ندارند و با آزادی‌های مزبور مخالف هستند؛ هر دو گروه جامعه را به انحطاط می‌کشانند (هاشمی، ۱۳۹۲، ج ۱: ۲۶۸).

از زمان پیدایش اینترنت تا به امروز عقاید متعددی مطرح شده است. یکی از مهم‌ترین عقاید این است

که آیا می‌توان اینترنت را تحت کنترل و مدیریت درآورد؟ در آمریکا قاعده‌مند نمودن اینترنت در زمان ریاست جمهوری «بیل کلینتون» شدت بیشتری گرفت. حزب حاکم در آن زمان به دنبال ارائه یک چارچوب برای تجارت الکترونیک جهانی بود. نتیجه اعمال تدابیر مزبور، تبدیل اینترنت به محیط کاملاً نظارتی بود. طبق دیدگاه کلینتون، اینترنت از اهمیت زیادی برخوردار است. به منظور حمایت از آزادی در اینترنت، می‌بایست توسط بخش خصوصی اداره شود. نیازی نیست قواعدی و مقرراتی پیرامون اینترنت وضع شود. بازارها در این خصوص می‌توانند نقشی محوری ایفا کنند. در این مورد می‌بایست بیشترین نقش را به دولت (در امر مداخله و تنظیم مسائل مربوط به اینترنت) تا حد امکان داد (Savin, 2013: 8-9).

چین (از لحاظ حجم و تعداد محدودیت) اولین کشور در مسدود نمودن تارنما‌های اینترنتی در جهان است. در این کشور، موتور جست و جوی گوگل از ارائه برخی خدمات اینترنتی و نتایج جست و جو (بنا به درخواست مقامات چینی) خودداری می‌کند. نتایج مزبور، در خارج از چین قابل تحصیل هستند؛ همچنین تصاویر کشتار (مربوط به برخی وقایع تاریخی) در سال‌های گذشته قابل مشاهده نیست. مقامات چینی از فناوری برای کنترل فضای مجازی استفاده می‌کنند. روی مانی‌تور تلفن همراه آنها، نرم‌افزاری وجود دارد که اشاعه شایعات سیاسی را ردیابی می‌کند. چین تعداد زیادی از افراد را برای مدیریت نمودن فضای مجازی استخدام نموده است. روند فیلتر نمودن سایت‌ها از سال ۱۹۹۶ آغاز شد و در سال ۲۰۰۲ شدت پیدا کرد (روزبهرانی، ۱۳۹۳: ۸۶).

اینترنت باید از آزادی بیان حمایت کند. در جوامع برای تقویت گفتمان عمومی و شکل‌گیری اراده دموکراتیک، اینترنت می‌بایست به راحتی در دسترس باشد. برای اینکه اینترنت خدماتش را به نحو مطلوب‌تری ارائه دهد، دولت باید دامنه و حوزه‌ای از قدرت را در اختیار داشته باشد تا بتواند مقررات را تنظیم کند (Kim, 2002: 139-140).

در کشور ما، از جمله تکالیف دولت، ارتقای دانش عمومی در همه زمینه‌ها با استفاده از مطبوعات و رسانه‌های گروهی و وسایل دیگر است (بند دوم اصل سوم قانون اساسی). در این بند، بر لزوم آگاه شدن مردم از اطلاعات عمومی تأکید شده است. دولت مکلف است از طریق وسایل ارتباط جمعی سطح آگاهی و اطلاعات شهروندان را بالا ببرد. صیانت از ارزش‌های موجود در جامعه و حفظ سلامت جسمی و روانی شهروندان از تکالیف زمامداران در جوامع دموکراتیک است؛ بی‌گمان برخورداری مطلق شهروندان از حقوق و آزادی‌های عمومی در این فضا ممکن است به سلب آزادی دیگر شهروندان منجر شود. قانون‌گذار می‌بایست با اتکا به قانون اساسی چارچوب کلی اعمال حقوق و آزادی شهروندان را تبیین کند. لزوم مدیریت فضای مجازی از بسیاری اصول قانون اساسی قابل استنباط است:

الف) طبق اصل نهم قانون اساسی، هیچ فرد یا گروهی حق ندارد به نام آزادی، به استقلال سیاسی، فرهنگی، تمامیت ارضی، نظامی، اقتصادی و.. خدشه وارد نماید. شکی نیست که اینترنت می‌تواند ابزاری برای سوءاستفاده احتمالی بیگانگان در اعمال سلطه فرهنگی، سیاسی، اقتصادی تبدیل شود. دولت می‌بایست با اقتدار سیاسی به پاسداری از ارزش‌های اجتماعی بپردازد.

ب) طبق اصل بیست و یکم قانون اساسی، دولت مکلف به ایجاد زمینه‌های مناسب برای رشد شخصیت



زن و احیای حقوق مادی و معنوی او را فراهم کند. متأسفانه مشاهده می‌شود فضای مجازی ابزاری برای تضعیف کیان خانواده و زن از طریق ترویج بی‌بندوباری و مسائل غیراخلاقی و مستهجن تبدیل شده است. لازمه حفظ ارزش‌ها و قداست‌ها، مدیریت این فضا توسط دولت است.

ج) در فضای مجازی امکان نقض حقوق شهروندی، توهین و هتک حیثیت شهروندان وجود دارد. بسیاری از اصول قانون اساسی بر صیانت بر ارزش‌ها تأکید دارد؛ از میان این اصول می‌توان به اصل مصونیت تعرض به جان، مال، حقوق مردم (اصل ۲۲ قانون اساسی)، ممانعت از هرگونه تجسس (اصل ۲۵ قانون اساسی)، منع هتک حرمت و حیثیت افراد (اصل ۳۹ قانون اساسی)، منع اضرار به غیر و تجاوز به منافع عمومی (اصل ۴۰ قانون اساسی) اشاره نمود. شکی نیست که حاکمیت می‌تواند با وضع قانون در فضای مجازی و تعیین ضمانت اجرا از حقوق مردم حمایت کند.

در خصوص دسترسی افراد به اطلاعات و انتشار آن در فضای مجازی باید توجه داشت، حذف و فیلتر نمودن پیام‌رسان‌هایی همچون تلگرام را می‌توان نقض آزادی اطلاعات و حق دسترسی مردم به اطلاعات دانست. برخی نظام‌ها مواردی همچون نظم عمومی، امنیت ملی، امنیت عمومی را تفسیری موسع می‌کنند و دسترسی شهروندان به اطلاعات را محدود می‌کنند؛ در حالی که عناوین مزبور عناوینی مبهم و واجد تفسیر هستند (محسنی، هاشمی، جاوید و عباسی، ۱۳۹۸: ۳۵۰-۳۴۹).

## ۲.۲ سازوکارهای مدیریت فضای مجازی

مستنبط از اصول قانون اساسی (اصول فوق‌الذکر)، مدیریت فضای مجازی نه تنها حق دولت است بلکه تکلیف نیز است. دولت مکلف است ضمن تبیین چارچوب‌هایی، شهروندان را به تبعیت از قوانین ملزم نماید. پرسشی که در این مورد مطرح می‌شود است که دولت از چه شیوه‌هایی در این مورد استفاده نماید. نظریه خودتنظیمی، تفسیر قوانین جاری، وضع قانون در موردی خاص و ارائه قانونی جامع، از جمله دیدگاه‌های مطرح شده در این مورد هستند که ذیلاً به تبیین آنها می‌پردازیم.

### ۱.۲.۲ قواعد خودتنظیمی

روش‌های خودتنظیمی، از جمله دیدگاه‌هایی است که پیرامون مدیریت فضای مجازی ارائه شده است. خودتنظیمی به معنای تفویض اختیارات به بخش خصوصی است؛ در واقع، خودتنظیمی به معنای بی‌قانونی است. دولت به جای وضع قانون در حوزه اینترنت، از شرکت‌های ارائه‌دهنده اینترنت می‌خواهد که پاره‌ای قیود و شروط را در قراردادهای خود با کاربران اعمال نمایند. در این روش، دولت ضمن ممانعت از ورود به حوزه قانون‌گذاری، اختیارات خویش را به بخش خصوصی اعطا می‌کند. روش‌های خودتنظیمی دارای مزایایی است: الگوی خودتنظیمی، الگویی انعطاف‌پذیر و قابل انطباق با پیشرفت و فناوری است. مضافاً هیچ‌گونه هزینه‌ای را (در مقایسه با وضع قانون) بر دولت یا نهادهای اجرایی قرار نمی‌دهد. کاربران نیز انگیزش بالایی در پذیرش آن دارند (ادریسی و صفادوست، ۱۳۹۳: ۴۰). چنین رویکردی از منظر اجتماعی پذیرفتنی است. این امر به معنای اعمال اختیاری قواعد مطلوب - اختیاری در حوزه فضای مجازی است. ارائه‌دهندگان خدمات

اینترنتی با فراهم نمودن الگوهای قراردادی از استفاده کنندگان می‌خواهند به آن تعهدات عمل نمایند. قواعد مندرج در قرارداد میان ارائه دهندگان خدمات اینترنتی و کاربران اینترنتی نمی‌بایست یک‌جانبه و به نفع شرکت ارائه‌دهنده خدمات اینترنتی باشد. این قواعد می‌بایست تا حد امکان آزادی کاربران را تضمین نماید (Marsden, 2011: 48).

در عمل با افزایش روزافزون اینترنت و فضای مجازی، اعمال مقررات خودتنظیمی با دشواری‌هایی مواجه شد: با افزایش رو به رشد استفاده کنندگان خدمات اینترنتی و افزایش پهنای باند کاربران، خطرات امنیتی و چالش‌هایی از قبیل مسئولیت کاربران مطرح شد. در سال ۱۹۹۷ صرفاً ۱۴ میلیون خانوار از خدمات اینترنتی برخوردار بودند. در حالی که در سال ۲۰۰۷ حداقل تعداد ۲۰۰ میلیون خانوار از چنین خدمات برخوردار شدند. چنین تحولی را می‌توان به چرخه توزیع مواد مخدر در میان اشخاص تشبیه نمود. پس از ارائه نسخه جالب محصول در میان کاربران، نسخه جالب‌تر آن ظاهر می‌شد (Ibid, 49).

به کارگیری مطلق خودتنظیمی متضمن عیوبی است. این روش نمی‌تواند پاسخگوی نیازی‌های جامعه باشد و بر آن ایراداتی وارد است:

الف) احتمال نقض حقوق شهروندان به دلیل فقدان ضمانت اجرای مناسب بسیار بالا است. خودتنظیمی نمی‌تواند ابزاری برای ممانعت از ارسال تبلیغ‌های ناخواسته اینترنتی، ارسال هرزنامه‌های اینترنتی (اسپم‌ها) یا منع قماربازی اینترنتی باشد.

ب) شهروندان به درستی از دامنه حقوق و آزادی‌های خود آگاهی ندارند. این احتمال وجود دارد که آنها ناخواسته حریم خصوصی دیگران را نقض کنند، حق نشر مؤلفان را نادیده بگیرند و یا به سایت‌های ممنوعه دسترسی پیدا نمایند. بی‌گمان، استفاده از قرارداد خصوصی کاربران و شرکت‌های ارائه‌دهنده خدمات اینترنتی نمی‌تواند این ایرادات را بکاهد یا آنها را برطرف سازد.

اصل ۷۱ قانون اساسی اختیار وضع قانون در عموم مسائل را به مجلس شورای اسلامی داده است. نظر به اهمیت فضای مجازی و کاربرد آن در جامعه و نارسایی قواعد خودتنظیمی، استفاده از قوانین برای مدیریت این فضا امری ضروری است.

## ۲.۲.۲ تسری مفاد قوانین به پدیده‌های جدید

از جمله دیدگاه‌هایی که پیرامون مدیریت فضای مجازی ارائه گردیده است؛ تسری قوانین مرتبط، به فضای مجازی است. طبق این دیدگاه، از وضع قانون جدید در حوزه خودداری می‌شود و قوانین موجود در این مورد جریان می‌یابد. برای روشن‌تر شدن این مسئله به ذکر مثال‌هایی می‌پردازیم:

**مثال اول:** در آمریکا قانون «حریم خصوصی ارتباطات الکترونیکی» ۱۹۸۶م وجود دارد. هرچند قانون مزبور پیش از پیدایش و گسترش اینترنت به وجود آمده بود لیکن صاحب‌نظران آن را در حوزه ارتباطات الکترونیکی از طریق اینترنت نیز به کار می‌برند. طبق قانون مزبور، ارتباطات الکترونیکی عبارت است از «هرگونه انتقال علائم، سیگنال‌ها، نوشتن، اصوات، داده‌ها یا اطلاعات به‌طور کامل یا جزئی از طریق سیم،

رادیو، الکترومغناطیسی، عکس الکترونیکی یا سیستم نوری». در حقوق این کشور می‌توان با اتکا به حکم دادگاه و به‌منظور انجام تحقیقات جنایی مبادرت به نقض حریم خصوصی قرارداد مشارکتی نمود (Tripathi, 2020: 12).

**مثال دوم:** در استرالیا قانونی (قانون مصوب سال ۱۹۹۲) در خصوص پخش برنامه‌ها (برنامه‌های تلویزیونی) وجود دارد که مفاد آن در خصوص اینترنت نیز به کار برده می‌شود. این قانون در سال ۱۹۹۹ مورد اصلاح قرار گرفت و در خصوص انتقال محتوای اینترنت تسری پیدا نمود. اصلاحات مزبور، در پاسخ به نگرانی جامعه استرالیا در خصوص کودکان بود. در یادداشت‌های توضیحی این قانون آمده بود: نگرانی دولت و جامعه در خصوص مطالب و برنامه‌هایی است که به‌صورت آنلاین پخش می‌شود؛ به‌ویژه در مورد سهولت دسترسی به مواردی از قبیل هرزه‌نگاری یا سایر مواردی که برای کودکان نامناسب است. هدف قانونگذار از وضع قانون، ارائه چارچوب مناسب در خصوص برنامه‌های آنلاین از طریق اینترنت است. این اصلاحات با هدف تحقق سه مورد بود: (الف) ارائه وسیله‌ای برای رسیدگی به شکایات مربوط به برخی از مطالب اینترنتی، (ب) محدود کردن دسترسی به برخی از محتوای اینترنت که احتمالاً موجب ارتکاب جرم برای فردی متعارف و منطقی می‌شود و (ج) برای محافظت و حمایت از کودکان در برابر محتوای نامناسب اینترنت (Brian, 2008: 45). تسری قوانین عام و مادر به حوزه فضای مجازی، اگرچه دارای مزایایی است لیکن خالی از اشکال نیست: برخی مسائل موجود در قوانین مزبور در فضای مجازی قابل انطباق نیستند. پاره‌ای از مسائل حوزه اینترنت در قوانین موجود مشاهده نمی‌شود. اگرچه این دیدگاه نسبت به دیدگاه پیشین: قواعد خودتنظیمی تا حد زیادی تعدیل شده است لیکن مشکلات ناشی از فقدان قانون در برخی موارد مشاهده می‌شود.

### ۳.۲.۲ وضع قوانین

نارسایی قوانین فعلی، اندیشه وضع قانونی جدید را به ذهن متبادر می‌سازد. ماهیت جهانی اینترنت حکایت از این امر دارد که این پدیده صرفاً مرزهای جغرافیایی را در نمی‌نوردد بلکه وارد دامنه‌هایی همچون فرهنگ، عقاید و ... می‌شود. این در حالی است که داده‌ها و اطلاعات در اینترنت همه‌وقت و همه‌جا وجود دارند و هیچ‌گونه هم‌گرایی در خصوص کنترل آنها وجود ندارد. از حیث عقیدتی نیز بسیاری از کشورها عقاید یکسانی با دیگر کشورها ندارند.

برخی معتقدند دولت‌ها در امر تقنین در فضای مجازی می‌بایست از الگوهای سنتی فاصله بگیرند. وضع قوانین می‌بایست با توجه به خصوصیات منحصر به فرد آن باشد. در این خصوص می‌بایست قواعد غیر حقوقی، هنجارهای اجتماعی، خصیصه فراملی بودن اینترنت و ... را در نظر بگیرند و مفاهیم سنتی (که ظهور در زمان و مکان دارد)، در این مورد جریان نمی‌یابد (رضایی و بابازاده مقدم، ۱۳۹۳: ۵۸).

اتحادیه اروپا در سال ۲۰۰۲ دستورالعملی را در خصوص حریم خصوصی و ارتباطات الکترونیکی وضع نمود. دستورالعمل مزبور چنین مقرر می‌کرد: ارسال اسپم و فاکس، بازاریابی تلفنی امکان‌پذیر نیست مگر این که پیش از آن رضایت گیرنده اعلام گردد و یا این که بتوان رضایت وی را از قبل استنباط کرد. بسیاری از کشورهای عضو اتحادیه اروپا در خصوص اسپم قوانین را وضع نموده‌اند. از این کشورها می‌توان به جمله

اتریش، دانمارک، فنلاند، آلمان، یونان، ایتالیا، بلژیک و اسپانیا اشاره کرد. در انگلیس قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰م وجود دارد که در خصوص اسپم‌ها می‌تواند مؤثر واقع شود. بر طبق قانون مزبور دسترسی غیرمجاز به رایانه‌ها من جمله ارسال هرزنامه‌ها ممنوع است. در مجموع می‌توان گفت مقابله با اسپم نیازمند تلاش جهانی برای مقابله با آن است. در برخی کشورها اگرچه قانونی در خصوص اسپم وجود ندارد؛ اما کاربران می‌بایست به دنبال روش‌هایی برای کاهش اسپم باشند. نرم‌افزارهای مقابله با اسپم از کارایی لازم برخوردار نیستند. دولت‌ها می‌بایست در خصوص ارسال کنندگان اسپم اقدامات لازم را اتخاذ کنند و هزینه‌هایی که شهروندان برای مقابله با اسپم متحمل می‌شوند؛ بر آنها تحمیل شود. از جمله این راهکارها تعیین میزان هزینه‌ای برای ارسال هر پیام از طریق ایمیل است (Schwabach, 2005, p275).

در وضع قانون جدید در حوزه فضای مجازی می‌بایست به اصول قانون اساسی توجه کرد. یکی از نویسندگان معتقد است انسان در اعمال حق خویش چاره‌ای ندارد جز اینکه حقوق و آزادی‌های دیگران را رعایت کند. برای رعایت نظم اجتماعی و رعایت حقوق دیگران و احترام به آن می‌توان محدودیت‌هایی را بر آزادی‌های اشخاص وارد نمود. آزادی مطلق انسان چیزی جز به معنای نبود عقل و تن وی نیست (لطفی، ۱۳۸۹: ۱۵۲).

برخی معتقدند با توجه به تفاوت فاحش فضای سایبر و فضای سنتی می‌بایست در فضای سایبر در هر موردی به دقت تقنین صورت گیرد. فضای مزبور، فضایی است که به‌طور مستمر و دائم در حال تغییر و تحول است. لازم است که قوانین هرچند مدت یک بار مورد اصلاح و بازنگری قرار گیرند (صابر نژاد و حسین پور، ۱۳۹۶: ۱۲۶). یکی از اصول مهم در قانون اساسی ایران، اصل حاکمیت قانون است. طبق اصل مزبور در کلیه امور عمومی، اتخاذ تصمیم می‌بایست طبق قانون باشد. براساس این اصل، مقامات عمومی، لشکری و کشوری می‌بایست طبق قانون عمل نمایند. این اصل موجب زوال خودکامگی و استبداد حکام می‌شود. علاوه بر این، انجام اعمال اداری طبق قانون تضمین‌گر حقوق همه‌جانبه و امنیت قضائی می‌شود (هاشمی، ۱۳۹۲، ج ۱: ۳۱۷). برخی معتقدند قانون‌گذار ایرانی به دنبال پیروی از عرف بین‌المللی در فضای مجازی است اما در عین حال قواعد حقوق داخلی را هم لحاظ می‌کند (جعفری، ۱۳۹۸: ۱۲۷-۱۲۶). برخی معتقدند در امکان‌سنجی قاعده‌مند نمودن سیستم حقوقی در فضای سایبر می‌بایست بین قانون و گزاره‌های اخلاقی قائل به تفکیک شد: در گزاره‌های مزبور، صرفاً از انجام پاره‌ای امور نهی شده است (همانند سیگار نکشیدن یا پارک نکردن)؛ در حالی که قانون دارای محتوا و ضمانت اجرای حقوقی است (همانند پرداخت جریمه در صورت پارک اتومبیل). اصل حاکمیت قانون اقتضا می‌کند که بایدها و نبایدهای حقوقی در متون قانونی همراه با محتوا (مثلاً ضمانت اجرا) درج شود. ضمانت اجرای نقض قانون اساسی صرفاً ممانعت از انجام عمل است نه بیشتر (قاجارلو قیونلو، ۱۳۹۱: ۲۲۶-۲۲۶۷).

نباید چنین پنداشت که وضع قانون جدید در حوزه اینترنت خالی از اشکال نیست. بی‌گمان، تقنین در این فضا مشکلاتی را به همراه دارد: در بخش‌های متعدد و متفاوت از دنیای معاصر، حقوق حاکم بر اینترنت متفاوت از بخش‌های دیگر است. قواعد حقوقی قواعدی الزام‌آور هستند که در بخش‌های معینی از دنیا اعمال می‌شوند. باید پذیرفت از حیث سرزمینی، قواعد یکسانی در مورد اینترنت اعمال نمی‌شود. اینترنت را می‌توان همچون ماهواره دانست. مسائل مربوط به اینترنت قواعد چند کشور و منطقه را با یکدیگر مرتبط می‌سازد؛

طوری که این امکان وجود دارد که امری در کشوری دارای قواعد حقوق مشخصی باشد و در کشور دیگر قواعد حقوقی دیگری در مورد آن اعمال شود (Consalvo, 2013: 149).

برخی بر حاکمیت فضای مقررات داخلی یک کشور بر فضای مجازی ایراداتی وارد نموده‌اند. از منظر آنها فعالیت‌های موجود در فضای مجازی صرفاً در یک کشور انجام نمی‌شود. برابری حاکمیت کشورها اقتضا می‌کند چنین حقی را برای سایر کشورها داشته باشیم. اصل حاکمیت قوانین داخلی موجب تخریب فضای حاکم بر اینترنت می‌شود. چنین اصلی با فضای بین‌المللی بودن اینترنت در تعارض است. حاکمیت قوانین داخلی کشورها در قلمرو جغرافیایی آنها به معنای حاکمیت آن در فضای مجازی نیست (رجبی، ۱۳۹۶: ۲۹۹).

شکی نیست که دولت‌ها در خصوص امور داخلی قوانین و مقرراتی دارند و آنها را در مورد شهروندان و مردم به کار می‌برند. در پاره‌ای موارد، معاهداتی بین‌المللی را منعقد می‌کنند و بدان ملتزم می‌شوند. در قوانین داخلی کشورها این امکان فراهم شده که به یاری قواعد حل تعارض، قوانین خارجی در حوزه دادگاه‌های داخلی نیز اجرا شود. به نظر می‌رسد در حوزه فضای مجازی نیز قانون‌گذار می‌تواند از چنین رویکردی استفاده کند و وجود چالش‌های تقنینی نمی‌تواند مانعی در راستای مدیریت فضای مجازی از طریق وضع قانون جدید ایجاد نماید.

### ۳ حوزه‌های تقنین در فضای مجازی

کشورهای مختلف در حوزه تقنین فضای مجازی به شیوه یکسان عمل ننموده‌اند: برخی کشورها در خصوص مسائلی تقنین نموده‌اند که در کشورهای دیگر مورد توجه قرار نگرفته است. برعکس، پاره‌ای دیگر از کشورها اولویت را به مسائل دیگری داده‌اند. هرزه‌نگاری، حریم خصوصی، حق نشر ادارات دولتی، مدارس و ... از جمله حوزه‌های وضع قانون است. تحلیل این مسائل می‌تواند از حیث تقنین احتمالی و اقتباس قانون‌گذار ایرانی مفید باشد. ذیلاً به ذکر موارد مزبور می‌پردازیم.

#### ۱.۳ هرزه‌نگاری

در سالیان اخیر هرزه‌نگاری یکی از چالش‌های مهم در آمریکا بوده است. این کشور در مقایسه با سایر کشورها (همچون ولز و کانادا) شاهد تغییرات اساسی بوده است. در سال ۱۹۹۶م قانون محدودیت هرزه‌نگاری کودکان به تصویب رسید. طبق قانون مزبور، ایجاد تصاویر از طریق کامپیوتر و رایانه به منظور تحریک صریح کودکان به انجام رفتارهای جنسی جرم است. قوانین ایالتی و فدرال، هرزه‌نگاری کودکان را ممنوع نمودند. ایالات متعدد این کشور، پس از تصمیم دیوان عالی، مبادرت به وضع قوانین متعدد در این حوزه نمودند. دیوان عالی این کشور بر این مسئله تأکید داشت که مداخله کودکان در حوزه هرزه‌نگاری می‌بایست مسئله‌ای جدی تلقی شود. دادگاه عالی ایالات متحده بر این مسئله تأکید نمود که استفاده از کودکان در مسئله هرزه‌نگاری منجر به ایجاد صدمات جسمی و روحی بر آنها می‌شود. تحصیل سود مالی از طریق هرزه‌نگاری کودکان، توزیع فیلم در خصوص فعالیت‌های جنسی نوجوانان یا سوءاستفاده جنسی کودکان جرم ممنوع است. در

پرونده «آزبورن به طرفیت اوهایو»<sup>۳</sup> دادگاه چنین مقرر نمود که ممنوع نمودن هرزه‌نگاری کودکان، ابزاری برای محافظت از کودکان در برابر استثمار است (Akdeniz, 2008: 95). قانون مذکور چنین مقرر می‌کند: مراد از هرزه‌نگاری صرفاً تولید تصاویری نیست بلکه ایجاد هرگونه توصیف یا تصویر ذهنی در کودکان از قبیل عکس، فیلم، تصاویر یا غیرتصاویر و هر چیزی که منجر به حضور آنها در فعالیت‌های جنسی شود. قانون مزبور صرفاً به تولید هرزه‌نگاری محدود نمی‌شد بلکه توزیع، تولید، توصیف و ارتقا و ... را در بر می‌گرفت. همچنین عکس‌های شبه‌ناشایست و استفاده بزرگسالان در هرزه‌نگاری کودکان، به تصویر کشیدن کودکان در هرزه‌نگاری جرم تلقی می‌شود (Ibid: 97).

در انگلستان در سال ۱۹۹۴ قانون حمایت از کودکان مصوب سال ۱۹۷۸ مورد اصلاح قرار گرفت. تصاویر ایجاد شده توسط رایانه را نیز اضافه نمود و پورنوگرافی کودکان از طریق اینترنت بدنی واسطه ممنوع گردید. در سال ۱۹۹۵ پورنوگرافی کودکان تبدیل به یک دغدغه عمومی گردید و اقدامات قضائی در راستای حمایت از کودکان در این خصوص اعمال گردید. برخی در پرونده‌های خاصی تحت تعقیب قضائی قرار گرفتند. در سال ۱۹۹۴ در باب پورنوگرافی کودکان جرم‌انگاری گردید و جرم مزبور از مصادیق جرایم جنسی که مستقیماً به کودکان آسیب می‌رساند تلقی گردید (Akdeniz, 2008: 18).

در خصوص فیلترینگ باید توجه داشت که فیلتر نمودن سایت‌ها با مشکلاتی مواجه است. این فیلترینگ توسط نرم‌افزار و ماشین انجام می‌شود و اندیشه‌های انسانی در آن نقشی ندارند، امکان اشتباه وجود دارد، این احتمال وجود دارد که مطلب موجود سایتی علمی را مستهجن تلقی کرده و مبادرت به مسدود نمودن آن کند. همچنین فیلترینگ به کلیه کاربران به مثابه شخصی واحد می‌نگرد و تبعیضی را در نظر نمی‌گیرد. این امکان وجود دارد که مطالبی برای شخصی گمراه‌کننده باشد و برای فرد دیگر مطالب مناسبی باشد (روزبهرانی، ۱۳۹۳: ۲۲).

طبق اصل دهم قانون اساسی جمهوری اسلامی ایران، همه قوانین و برنامه‌ریزی‌ها می‌بایست در راستای تسهیل تشکیل خانواده، استواری روابط خانوادگی بر مبنای حقوق و اخلاق اسلامی و پاسداری از حرمت و قداست خانواده باشد. بی‌گمان، صرف جرم‌انگاری در حوزه هرزه‌نگاری کفایت نمی‌کند. کودکان و خانواده‌ها می‌بایست در یک محیط ایمن به کار و فعالیت‌های خویش مشغول شوند. اینترنت نمی‌بایست بستری برای کجروی‌های جنسی - اجتماعی کودکان باشد.

یکی از اساتید معتقد است که مذاقه در بسیاری از اصول قانون اساسی همانند اصل چهارم، مقدمه قانون اساسی، حکایت از اهمیت ارزش‌های مذهبی در قانون اساسی دارد. شورای نگهبان نیز از آنچه برخلاف موازین اسلامی است ممانعت به عمل می‌آورد. شکی نیست این ارزش‌ها بنیان حکومت اسلامی را تشکیل می‌دهد و حاکمیت در تمامی موارد مقید به آن است (کاتوزیان، ۱۳۷۷: ۳۵۴-۳۵۳).

<sup>3</sup>Osborne v. Ohio.



## ۲.۳ حریم خصوصی

حریم خصوصی و آزادی بیان از مؤلفه‌های جامعه دموکراتیک است. یک جامعه دموکراتیک، بدون تصور آزادی بیان امکان پذیر نیست. در پرتو حق مزبور، شهروندان می‌بایست بتوانند صریح و بی‌پرده مطالبی را در مورد نهادهای عمومی بیان کنند. توانایی شرکت در مناظره یک حق مسلم است و از زمان ظهور اینترنت این حق ابعاد نوینی پیدا کرده است. ماهیت اینترنت به گونه‌ای است که هر شخصی می‌تواند نظرات مخالف دیدگاه‌های دیگران را بیان کند. همچنان که برخی شورشیان از طریق اینترنت دیدگاه‌های خود را در خصوص دولت مخالف خویش اعلام می‌نمایند. هر چند اینترنت پناهگاهی برای مخالفان سیاسی محسوب می‌شود لیکن امکان اجرای حق آزادی بیان به نحو مطلق (بدون هیچگونه محدودیتی) در برخی موارد موجب نقض حریم خصوصی دیگر شهروندان است. بر این اساس، هنگامی که شخصی در یک مکان عمومی مطالبی را بیان می‌کند که موجب رنجش خاطر دیگران را فراهم می‌کند یا در انظار عمومی نمایشی نامناسب را انجام دهد، عمل مزبور جرم محسوب می‌شود. افراد در حریم خصوصی خویش آزاد هستند که عقاید خویش را بیان کنند لیکن چنانچه حریم مزبور حالت علنی و عمومی پیدا نمود؛ چنانچه منجر به ایجاد نفرت شود، آزادی بیان محدود می‌شود (هیک، هلپین و هوسکینز، ۱۳۹۳: ۲۸۳).

در ژاپن حریم خصوصی به‌عنوان یکی از حقوق اساسی مورد شناسایی قرار گرفته است. چنین حقی، مستنبط از اصل ۱۳ قانون اساسی است. براساس اصل مزبور، مردم حق دارند خوشبختی را مطالبه کنند. قانون حمایت از اطلاعات شخصی در سال ۲۰۰۳ به تصویب رسید. حق حمایت از حریم خصوصی مورد تأیید و حمایت اصل ۱۳ قانون اساسی این کشور است و قانون حمایت از اطلاعات شخصی سال ۲۰۰۳ حریم خصوصی را نیز شامل می‌شود. بر این اساس، شرکت‌هایی که داده‌های شخصی را پردازش می‌کنند؛ مکلف به حفظ حریم خصوصی هستند (Komkai, 2020: 25). در کانادا در ژوئیه سال ۲۰۱۴ قانون ضدهرزنامه‌ی ایمیل اعمال شد. رسالت قانون مزبور حمایت از تجارت ناخواسته و تشویق به رشد الکترونیکی تجاری و اعتماد به بازار آنلاین بود. قانون مزبور ارسال پیام‌های الکترونیکی ناخواسته را ممنوع نمود مگر با رضایت گیرنده. رضایت مزبور می‌تواند صریح یا ضمنی باشد. رضایت ضمنی در مواردی وجود دارد که سابقه فعالیت تجاری میان طرفین وجود دارد. قانون‌گذار مرکزی تحت عنوان مرکز گزارش اسپم را در خصوص رسیدگی به پیام‌های الکترونیکی تجاری ناخواسته در نظر گرفت. کمیسیون رادیو و تلویزیون کانادا و کمیساریای حریم خصوصی مجاز به تحقیق در این خصوص در شرایط مناسب هستند (Teresa 2020: 62).

اصل بیست و سوم قانون اساسی ایران تفتیش عقاید را ممنوع دانسته است. براساس اصل مزبور، هیچ شخصی را نمی‌توان به دلیل داشتن عقیده‌ای خاص مؤاخذه کرد. بطلان تفتیش عقاید، ناظر به حالتی است که اندیشه در درون یک فرد باشد. انتشار افکار گمراه‌کننده جایز نیست. شکی نیست مباحث علمی مابین افراد دارای سطح بالا در فضای مناسب (مثلاً دانشگاه‌ها) با هیچ ایرادی مواجه نیست. بیان مطالب علمی برای اشخاصی با دانش پایین و بی‌اطلاع به مباحث علمی منطقی و عقلایی نخواهد بود (نجفی، ۱۳۷۹: ۴۵۵). برخی معتقدند نقض حریم خصوصی افراد مشهور زمانی امکان‌پذیر است که منافع عمومی اقتضا نماید. در مورد رجال سیاسی مشهور (نظر به الگو بودن آنها در جامعه) می‌بایست حداکثر تلاش برای حفظ حریم

خصوصی آنها انجام شود (ذاکریان و جاور و بطحایی، ۱۳۹۹: ۱۳۶). شکی نیست که جریان آزاد اطلاعات از ویژگی‌های جامعه دموکراتیک است. با وجود این، لازم است در خصوص اطلاعات شغلی افراد که به سبب شغلی به دست نیامده، انتشار ابلاغ‌نامه‌های دادگستری در فضای مجازی، اعلام نمرات دانشجویان، به‌بارگیری دوربین مخفی و ... قوانین صریحی ارائه شود (محسنی، ۱۳۸۴: ۸۸).

دولت به نمایندگی از شهروندان از جایگاه قانون‌گذاری برخوردار است و به نمایندگی از تمامی منافع جامعه عمل می‌کند و حق ایجاد هماهنگی و موازنه میان آزادی اندیشه‌ها را برخوردار است؛ به‌گونه‌ای که یک اندیشه (اندیشه‌ی یک شهروند) موجب نقض سایر اندیشه‌ها (اندیشه‌ی سایر شهروندان) نشود (زولر، ۱۳۸۹: ۱۷۵-۱۷۲). در حوزه فضای مجازی قانون‌گذار مکلف است میان آزادی شهروندان در کسب اطلاعات و نقض حریم خصوصی تعادل ایجاد نماید. قانون نیز می‌بایست در راستای حفظ منافع عمومی شهروندان باشد؛ به‌گونه‌ای که اعمال حق از سوی شهروندان موجب تضرر سایر شهروندان (نقض حریم خصوصی) نشود (اصل چهارم قانون اساسی).

### ۳.۳ حق نشر

از منظر بسیاری از تولیدکنندگان فیلم، ناشران، نویسندگان و ... فضای مجازی به‌مثابه کابوسی برای مالکیت فکری تولیدات آنها است. پیدایش فناوری این امکان را به اشخاص داده است که از تولیدات آنها بازدید کنند. تولیدات آنها نه تنها برای یک شخص، بلکه برای هر شخصی در هر زمان ممکن از طریق اینترنت قابل دسترسی است. اشخاص می‌توانند به‌جای مراجعه به فایل اصلی از طریق یک هارددیسک تولیدات را در اینترنت ذخیره نمایند. در آمریکا طبق قانون حق نشر دیجیتال ۱۹۹۸ نقض حق نشر و شبیه‌سازی جرم محسوب می‌شود. بسیاری از تولیدکنندگان، در فضای مجازی سایت‌هایی را ایجاد می‌کنند و اجازه بهره‌برداری و دسترسی مطالب و محتواها را به اشخاص نمی‌دهند مگر اینکه آنها مبادرت به پرداخت بهای آنها نمایند. چنین امری مبتنی بر این اندیشه است که اساساً منصفانه نیست که اشخاص در هر زمان ممکن بتوانند به هر چیزی دسترسی پیدا کنند (Robert, 2001: 23).

در چین قانون کپی‌رایت شبکه‌ای وجود دارد. در سال ۲۰۰۰ تفسیری در خصوص قانون مزبور ارائه شد. تفسیر مزبور، مشتمل بر ۱۰ ماده بود. برای نقض حق نشر در اینترنت خسارتی را تعیین نمود. در سال ۲۰۰۱ قانون کپی‌رایت چین مورد اصلاح قرار گرفت. نقض حق کپی‌رایت در اینترنت به آن اضافه شد. به هر شکل این قانون صرفاً متضمن سه ماده در خصوص اینترنت است. در مورد اختلافات مربوط به حق چاپ در اینترنت راهکاری را ارائه نمی‌داد. در سال ۲۰۰۳ اصلاحاتی بر قانون مزبور انجام شد. حداکثر مبلغ برای خسارت وارده در نتیجه نقض کپی‌رایت دیجیتالی تعیین گردید. حداقل مبلغ برای خسارت مزبور حذف گردید. مسئولیت مدنی در خصوص دورزدن فناوری تعیین گردید. به موجب اصلاحات بعدی برای نقض حق چاپ مسئولیت کیفری در نظر گرفته شد با این شرط که انتشار آثار دارای حق چاپ از منظر اینترنت انتشار و توزیع غیرقانونی تلقی شود؛ همچنین با توجه به تفسیر کپی‌رایت اصلاح‌شده شبکه‌ها، بازنشر آنلاین و گزیده آثار (به‌استثنای نرم‌افزار، فیلم و رمان)، قبل از ۱ جولای ۲۰۰۶، به‌عنوان نقض حق چاپ محسوب

نمی‌شود. شکی نیست مقررات مربوط به دادگاه عالی چین در هر دعوا یا ادعایی قابل اعمال است. در کشور چین عنصر اساسی اعمالی که منجر به نقض حق چاپ می‌شود، «کپی» است. این مفهوم زمانی گسترش می‌یابد که «پیوند دادن و جست‌وجو» ترکیب شوند (Brian, 2008: 18).

در فرانسه بر طبق قانونی که در سال ۲۰۰۹م به تصویب رسید این اجازه به فراهم‌کنندگان خدمات اینترنتی اعطا شد که کاربرانی که به صورت غیرقانونی مبادرت به دانلود بدون رعایت حق کپی‌رایت میکنند را از اتصال به اینترنت محروم کنند.

همچنین بر اساس قانون دیگری که در سال ۲۰۰۹ به مجلس این کشور تقدیم شد این اجازه به دولت این کشور داده شده که نسبت به تارنماهای غیراخلاقی اقداماتی از قبیل فیلتر و مسدود نمودن را اعمال نمایند. همچنین بر طبق قانونی که در سال ۲۰۰۱ به تصویب رسید کشور فرانسه فعالیت‌های اینترنتی و پست‌های اینترنتی مشتریان و کاربران را تا یک سال ذخیره می‌کند. همچنین این امکان به پلیس این کشور داده شد که با هدف کشف و اثبات جرم پیام‌های شهروندان را بررسی نماید (Zittrain, 2003: 79).

حمایت از حقوق مالکیت فکری و حق نشر امری مسلم است. طبق اصل بیست و دوم قانون اساسی، حقوق اشخاص مصون از تعرض است. دولت مکلف به حمایت از حقوق مزبور است. قوانین مربوط به حق نشر نمی‌توانند پاسخگوی نقض حقوق مربوط به نقض حق نشر در فضای مجازی باشند. این در حالی است که طبق اصل ۱۷۱ قانون اساسی مجلس شورای اسلامی می‌تواند در حدود مقرر قانون اساسی مبادرت به وضع قانون نماید. این امر با وضع قوانین ویژه پیرامون نقض مالکیت فکری در فضای مجازی محقق می‌شود.

### ۴.۳ کارمندان دولتی

یکی از مسائل مهم در فضای مجازی، نظارت بر عملکرد و نوشته‌های کارمندان در فضای مجازی است. دادگاه توکیو در این مورد اعلام کرد: تحت نظارت قرارداد دادن ایمیل‌های کارکنان و کارمندان برای شرکت‌ها امری اجتناب‌ناپذیر است. دستورالعملی پیرامون استفاده کارکنان در خصوص استفاده شخصی ابزارهای الکترونیکی وجود ندارد (آنها ملزم به استفاده ابزارهای مزبور صرفاً در امور شغلی هستند). دستورالعمل وزارت کار، رفاه و بهداشت و همچنین وزارت اقتصاد، تجارت و صنعت امکان نظارت دقیق و مشخص بر کارمندان را تبیین می‌کند. دستورالعمل مزبور از لزوم موافقت صریح کارمندان برای نظارت بر آنها سخن می‌گوید (Komukai, 2020: 261).

در آمریکا در برخی از شرکت‌ها و ادارات دولتی، دسترسی کارمندان و خدمه به سایت‌های هرزه‌نگاری محدود شده است. همچنین کلیه کارمندان مکلف به استفاده از نسخه‌های اصل و مادر بر روی کامپیوترها هستند. در پاره‌ای از موارد، صاحبان برخی ادارات یا شرکت‌ها کامپیوترهایی را سفارش می‌دهند که صرفاً در حوزه شغلی می‌توان از آن استفاده نمود و امکان دسترسی به موارد دیگر وجود ندارد (Zittrain, 2003: 670).

در کشورهای مزبور، کارمندان از انجام امور غیرشغلی در زمان اداری ممنوع هستند. محدودیت مزبور صرفاً محدودیت‌هایی است که کارمندان به سبب و علت شغل خویش متحمل شده‌اند و فلسفه آن اعمال انضباط اداری است. کارمندان مکلف‌اند تمام توان خویش را در راستای تحقق اهداف ادارات دولتی اعمال

نمایند و از انجام اعمال غیرمرتبط با شغل خویش خودداری نمایند. چنین قاعده‌ای تفسیر مضیقی از مفهوم آزادی را ارائه می‌دهد. در بند دهم اصل سوم قانون اساسی ایران مکلف به ایجاد نظام اداری صحیح و حذف تشکیلات غیرضروری شده است. لازمه چنین امری وضع قواعدی پیرامون محدودیت دسترسی کارکنان اداری به تارنماهای غیرمرتبط در حین انجام وظیفه است.

### ۵.۳ مدارس

در آمریکا طبق قانون حمایت از اینترنت کودکان ۲۰۰۰ م، اشخاص زیر سن ۱۸ سال از دسترسی به بعضی از رسانه‌ها ممنوع هستند. مدارس و کتابخانه‌های الکترونیکی مدارس که از بودجه دولتی استفاده می‌نمایند مکلف به پیروی نمودن از این مقررات هستند. بسیاری از مدارس و کتابخانه‌ها این قانون را محدودکننده و پالایش‌دهنده سایت‌های اینترنتی می‌دانند. بر این اساس، چنانچه مطالبی که در اینترنت مورد جست‌وجو قرار می‌گیرند با محتوای آموزشی و تحصیلی تناسبی نداشته باشد؛ مقامات مدرسه مکلف‌اند دسترسی کودکان را محدود نمایند. فیلترنمودن و غربال‌گری برخی کلمات از پیش تعیین شده به تشخیص آنها بستگی دارد. همچنین این امکان وجود دارد که دسترسی به برخی مطالب را محدود نمایند؛ همانند (همجنس‌باز). باید توجه داشت اگرچه حق آزادی بیان حقی تضمین شده در قانون اساسی آمریکا است و هرگونه تلاشی برای محدود کردن آن می‌بایست با توجه به دلیلی موجه و متناسب با اهداف دولت باشد، در این موارد، محدود نمودن کودکان از دسترسی به اینترنت متناسب با این هدف است. بر این اساس، مطالب مربوط به هرزه‌نگاری فیلتر می‌شوند. البته طبق قانون مزبور متون مورد فیلتر قرار نمی‌گیرند؛ صرفاً تصاویر محدود و ممنوع می‌شوند. همچنین فیلتر نمودن تصاویر نامناسب برای خردسالان الزامی است. شکی نیست اگرچه طبق قانون مزبور دسترسی کودکان و اشخاص زیر سن ۱۸ سال به اینترنت محدود شده است؛ اما این اختیار به مقامات مدرسه یا سایر افراد ذی‌صلاح داده شده است که بر مبنای حسن نیت و تحقق سایر اهداف قانونی (انجام امور پژوهشی و تحقیقات علمی) در مواردی خاص مبادرت به رفع فیلتر نمایند (Conn, 2002: 13-14).

طبق بند دوم اصل سوم قانون اساسی دولت مکلف به ارتقای دانش عمومی شهروندان در تمامی زمینه‌ها با استفاده از رسانه‌های گروهی، مطبوعات و ... شده است.

بسیاری از قوانینی که پیرامون معاملات اطفال، مسئولیت مدنی و کیفری آنها در قوانین ما مشاهده می‌شود، چهره‌ای حمایتی دارند. قانون‌گذار به‌منظور حمایت از آنها مبادرت به وضع قوانینی مغایر با افراد بالغ و بزرگسال می‌نماید. نظر به نقش اینترنت در پرورش فکری کودکان شایسته است مقرراتی حمایتی در خصوص اینترنت تصویب شود.

بر طبق اصل دهم قانون اساسی ایران همه‌ی قوانین و برنامه‌ریزی‌ها می‌بایست در راستای تسهیل تشکیل خانواده، استواری روابط خانوادگی بر مبنای حقوق و اخلاق اسلامی و پاسداری از حرمت و قداست خانواده باشد. بی‌گمان، صرفاً جرم‌انگاری در حوزه زمینه پورنوگرافی کفایت نمی‌کنند. کودکان و خانواده‌ها می‌بایست در یک محیط ایمن به کار و فعالیت‌های خویش مشغول شوند. اینترنت نمی‌بایست بستری برای کج‌روی‌های جنسی - اجتماعی کودکان باشد. وضع قوانین در خصوص دسترسی کودکان و بزرگسالان از طریق نام کاربری و رمز عبور می‌تواند موثر باشد.

قانونی تحت عنوان «قانون حمایت از اطفال و نوجوانان» مصوب ۱۳۹۹/۲/۲۳ وجود دارد. طبق بند ۶ ماده ۱۰ این قانون، در دسترس قرار دادن یا ارائه محتوا با اثر مستهجن جرم و قابل مجازات است. همچنین طبق بند هفت همان ماده استفاده از اطفال و نوجوانان برای تهیه، تولید، تکثیر، نمایش، فروش و نگهداری آثار سمعی بصری مستهجن و مبتذل، جرم است. بند هشت همان ماده، واردات، صادرات، تکثیر، انتشار، عرضه، معامله و بارگذاری محتوا یا اثر مستهجن اطفال و نوجوانان را مستوجب مجازات درجه شش قانون مجازات اسلامی می‌داند.

## ۴ نتیجه‌گیری

مدیریت فضای مجازی مستلزم ارائه بهترین راهکارها در خصوص قاعده‌مند نمودن این فضا است. پایان دادن به آشفتگی موجود در این فضا از طریق وضع بهترین و شایسته‌ترین قواعد ممکن در این خصوص امکان‌پذیر است. حقیقت این است که فضای مجازی دارای خصایص خاص خود است اما این فضا همچون فضای سنتی می‌بایست قاعده‌مند گشته و روابط میان اشخاص در آنها تنظیم شود. در این خصوص وضع قانون جامع در این مورد ضروری است. قانون جامع نه تنها به دنبال صیانت از فضای مجازی در خصوص تهدیدات موجود در آن باشد، بلکه می‌بایست متضمن قواعدی پیرامون تنظیم روابط اشخاص در این فضا باشد. مسائل همچون نقض حقوق مالکیت فکری، ممانعت از ارسال هرزه‌نامه‌ی الکترونیکی، تبلیغات ناخواسته اینترنتی، مقابله با قماربازی اینترنتی و ... از جمله مسائلی هستند که می‌بایست در این قانون مورد لحاظ قرار گیرند. طبیعت فضای مجازی به گونه‌ای است که نمی‌توان تمامی قواعد فضای سنتی را در مورد آن به کار گرفت. مفهوم حریم خصوصی در فضای مجازی کاملاً مغایر با این مفهوم در حوزه فضای سنتی است. شهروندان در استفاده از حریم خصوصی در فضای مجازی بخش‌هایی از حقوق و آزادی‌های خویش را از دست می‌دهند. بنابراین، تفسیر فعلی قوانین موجود و تسری آنها به فضای مجازی نمی‌تواند در همه‌ی موارد راه‌گشا باشد. به عبارت دیگر، اندیشه تسری قوانین فعلی به حوزه فضای مجازی نیز خالی از اشکال نیست: حقیقت این است که قوانین فعلی در برخی موارد گنجایش و کشش تسری به فضای مجازی را ندارند. مضافاً فلسفه وجودی این قواعد حمایت از وضعیت خاصی بوده است؛ این قواعد قابلیت تسری به فضای مجازی را ندارند. بنابراین نمی‌توان به قواعد مزبور اکتفا نمود و از وضع قانون خودداری نمود. وضع قانون هرچند می‌بایست به عنوان راهکار در نظر گرفته شود، لیکن فضای مجازی حوزه‌ای است که نمی‌بایست بدون خلأ قانونی در نظر گرفته شود. در وضع قوانین در فضای مجازی می‌بایست طبیعت این فضا را نیز مورد لحاظ و رعایت اصول و ضوابط قانون اساسی را مورد لحاظ قرار داد.

## مراجع

- [۱] ادیسی، فرهاد و مجتبی صفاری دوست (۱۳۹۳). قانونمند کردن اینترنت با تطبیق در حقوق کامن‌لا، پژوهش‌های حقوق تطبیقی، دوره ۱۸، ش ۴، صص ۲۵-۴۶.
- [۲] جعفری، افشین (۱۳۹۸). حاکمیت بر فضای سایبر از منظر حقوق بین‌الملل و نظام حقوقی جمهوری اسلامی ایران، رهیافت انقلاب اسلامی، ش ۴۹، صص ۱۰۹-۱۳۲.



- [۳] ذاکریان، اکبر و حسین جاور و سید فرهاد بطحایی (۱۳۹۹). حریم خصوصی افراد مشهور و فرزندانشان، فصل نامه دانش حقوق عمومی، ش ۳۰، صص ۱۴۰-۱۱۷.
- [۴] صابرزاد، علی و پری حسین پور (۱۳۹۶). تحلیل حقوقی گونه‌شناسی نقض حریم خصوصی در فضای سایبر، جستارهای حقوق عمومی، ش ۳، صص ۲۳۰-۲۱۵.
- [۵] رجبی، عبدالله و نسرين ترازى (۱۳۹۶). بررسی انتقادی حاکمیت حقوقی ساختار فنی اینترنت بر فضای مجازی، تحقیقات حقوقی، ش ۸۰، صص ۳۰۷-۲۸۳.
- [۶] رضایی، مهدی و حامد بابازاده مقدم (۱۳۹۳). اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا، فصل‌نامه پژوهش حقوق عمومی، ش ۴۲، صص ۸۲-۴۳.
- [۷] روزبهانی، محمدرضا (۱۳۹۳). جایگاه فقهی حقوقی فیلترینگ در رسانه‌های مجازی از دیدگاه مذاهب خمس، تهران: کتاب آوا.
- [۸] زولر، الیزابت (۱۳۸۹). درآمدی بر حقوق عمومی، ترجمه سید مجتبی واعظی، تهران: انتشارات جنگل.
- [۹] عباسی، بیژن (۱۳۹۳). مبانی حقوق عمومی، تهران: انتشارات دادگستر.
- [۱۰] قاجارلو قیونلو، سیامک (۱۳۹۱). مقدمه حقوق سایبر، تهران: انتشارات میزان.
- [۱۱] کاتوزیان، ناصر (۱۳۷۷). مبانی حقوق عمومی، تهران: انتشارات دادگستر.
- [۱۲] گرجی ازدریانی، علی اکبر (۱۳۸۸). مبانی حقوق عمومی، تهران: انتشارات جنگل.
- [۱۳] لطفی، اسدالله (۱۳۸۹). حقوق اساسی و ساختار نظام جمهوری اسلامی ایران، تهران: انتشارات جنگل جاودانه.
- [۱۴] هاشمی، سید محمد (۱۳۹۲). حقوق اساسی جمهوری اسلامی، ج ۱، چ ۱۲، تهران: انتشارات میزان.
- [۱۵] هیک، استیون و ادوارد اف هلیپین و اریک هوسکینز (۱۳۹۳). حقوق بشر و اینترنت، ترجمه قاسم زمانی و مهناز بهراملو، تهران: انتشارات خرسندی.
- [۱۶] نجفی اسفاد، مرتضی و فرید محسنی (۱۳۷۹). حقوق اساسی جمهوری اسلامی ایران، تهران: انتشارات بین‌المللی المهدی.
- [۱۷] محسنی، فرید (۱۳۸۴). تلاقی حریم شخصی و آزادی اطلاعات در حقوق ایران، دیدگاه‌های حقوق قضایی، ش ۳۷ و ۳۶، صص ۹۰-۷۱.
- [۱۸] محسنی، وجیهه و سید محمد هاشمی و محمدجواد جاوید و بیژن عباسی (۱۳۹۸). تحلیل حقوقی نسبت سنجی حق دسترسی عموم به اطلاعات با تحقق حقوق شهروندی با تأکید بر نظام حقوقی ایران، پژوهش حقوق عمومی، ش ۶۲، صص ۳۵۴-۳۲۱.
- [۱۹] مدنی، سید جلال‌الدین (۱۳۷۴). حقوق اساسی تطبیقی، تهران: انتشارات گنج دانش.
- [20] Akdeniz Yaman (2008). Internet child pornography and the law national and international responses, British Library Cataloguing in Publication Data, England.
- [21] Brian Fitzgerald, Fuping Gao, Damien O'Brien, Samsung Xiaoxiang Shi (2008). Copy right Law, Digital Content And The Internet In The Asia-Pacific, Sydney University Press.
- [22] Consalvo, Mia & Charles Ess (2013). The Blackwell hand book of internet studies, Oxford, UK: Blackwell Publications.
- [23] Conn, Kathleen (2002). The Internet and the Law What Educators Need to Know, Association for Supervision and Curriculum Development Alexandria, Virginia USA.
- [24] Marsden, T. Christopher (2011). Internet Co Regulation European Law, Regulatory Governance And Legitimacy In Cyberspac, Cambridge University Press, First published.



- [25] Kim, Jae Young (2002). *Sorting Out Deregulation Protecting Free Speech and Internet Access in the United States, Germany, and Japan* (Law and Society), LFB Scholarly Publishing LLC, New York. [http://firstmonday.org/issues/issue7\\_6/altinta/index.html](http://firstmonday.org/issues/issue7_6/altinta/index.html).
- [26] Komukai, Taro (2020). *IUS Comparatum Global Studies in Comparative Law. Data Protection in the Internet: Japanese National Report*, Springer, Switzerland.
- [27] Robert E. Litan (2001). *Law and Policy in the Age of the Internet*, Duke Law Journal, Duke University School of Law, Vol. 50, No. 4.
- [28] Savin, Andrej (2013). *EU Internet Law*, Edward Elgar Pub, USA.
- [29] Tripathi, Keyur (2020). *Protection of Privacy in Cyberspace: A Comparative Analysis Between India and USA*. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3611622](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3611622).
- [30] Schwabach, Aaron (2005). *Internet and the Law Technology, Society, and Compromises-ABC-CLIO*, Santa Barbara, California.
- [31] Scassa, Teresa (2020). *Data Protection and the Internet: Canada, Ius Comparatum – Global Studies in Comparative Law.*, Springer, Switzerland.
- [32] Zittrain, Jonathan (2003). *Internet Points of Control*, Boston College Law Review.



# شناسایی جملات حاوی کلمات توهین آمیز با استفاده از الگوریتم‌های یادگیری ماشین در سرویس‌های ابری آمازون

امیرعلی خانه‌نقا<sup>۱</sup>، زهرا موحدی<sup>۲</sup>

<sup>۱</sup> کارشناسی مهندسی کامپیوتر، دانشگاه تهران  
amiralikhanehanqa@ut.ac.ir

<sup>۲</sup> استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکده‌گان فارابی دانشگاه تهران  
zmovahedi@ut.ac.ir

## چکیده

با گسترش فضای مجازی، نظارت بر این فضا در جهت حفظ ارزش‌های جامعه امری ضروری است. مسئله‌ی استفاده از جملات توهین آمیز، زورگویی‌های اینترنتی و استفاده از کلمات مخالف با هنجارهای فرهنگی می‌بایست مورد بررسی و نظارت قرار گرفته و از بروز و نشر آن جلوگیری شود. در این مقاله، راهکاری مبتنی بر پردازش زبان طبیعی ارائه می‌شود تا بتوانیم در زبان فارسی جملات حاوی کلمات توهین آمیز را به کمک یادگیری ماشین پردازش کنیم. روش انجام کار به کمک سرویس‌های مختلف ابری آمازون اجرا شده است. نتایج نشان می‌دهد که در مقایسه با روش‌های سنتی، سرویس‌های آمازون موجب تسریع عملیات یادگیری ماشین می‌شوند و توانایی ارائه درصد بالایی از دقت و همچنین پیش‌پردازش و پردازش سریع داده‌ها و استقرار ماشین را دارا می‌باشند.

**کلمات کلیدی:** شناسایی کلمات ناهنجار، یادگیری ماشین، پردازش زبان طبیعی، سرویس‌های ابری آمازون.

## ۱ مقدمه

امروزه گستردگی فضای مجازی در جهان به قدری است که مکان و زمان را تحت شعاع خود قرار داده و به نوعی هم موجب راحتی و آسایش و هم باعث بروز مشکلاتی از جنس دیگر شده است. مقوله ارتباطات که زمانی رسیدن به نقطه‌ی نهایی توسعه آن دغدغه‌ای برای بشر محسوب می‌شد، اکنون با پیشرفت روزافزون علم و تکنولوژی به نقطه‌ای رسیده است که بسیاری از دولت‌ها سعی در مهار افسارگسیختگی این فضا را دارند. فضای مجازی زمانی در کشور عمومی‌تر شد که متولیان فرهنگی و اجتماعی و مدیران بخش‌های مرتبط با فناوری اطلاعات هیچگونه پیش‌زمینه‌ی لازم به جامعه در خصوص پیامدهای منفی و مخرب فضای مجازی ایجاد نکرده بودند و تا پیش از گستردگی اینترنت و شبکه‌های اجتماعی، کاربران این فضا اکثراً اساتید، نخبگان

و سازمان‌هایی بودند که اینترنت لازمه پژوهش و ارتباطات آنان با سایر نقاط دنیا بود. زمانی که بحث اینترنت به عوام تسری یافت و فراوانی گوشی‌های همراه پیشرفته، فضای مجازی را از حالت اختصاصی خارج کرد بدون اینکه هیچ آموزش و آگاهی در این خصوص به کاربران ارائه شود. نکته‌ای که قابل تاکید می‌باشد این است که تمامی کشورها مدیریت و حاکمیت خاصی بر فضای سایبری اعمال کرده و چارچوبی را برای فعالیت‌ها در این فضا معین نموده‌اند چون آنان نیز به این نتیجه واقف شده‌اند که افسار گسیختگی فضای مجازی در طولانی‌مدت می‌تواند به آسیب‌های جدی اجتماعی دامن زده و بر فرهنگ مردم تاثیر بگذارد و این در حالی است که در صورت کنترل شدن فضای مجازی این بخش قادر خواهد بود جنبه‌های مثبتی را برای کاربران مشخص کرده و رشد و توسعه را برای جامعه رقم بزند.

در فضای مجازی افراد متعددی وجود دارند که صحبت‌ها و کلماتی را بیان می‌کنند که در زندگی واقعی‌شان کمتر از این حرف‌ها از آن‌ها شنیده می‌شود و احساس بی‌بند و باری در فضای مجازی بیشتر نمود پیدا می‌کند؛ محققان به این پدیده مهارگسیختگی (disinhibition) می‌گویند، بدان معنا که افراد کمتر شرم از بیان احساسات خود دارند و از طرفی راحت‌تر شروع به صحبت‌های بی‌ادبانه و پراکندن خشم، نفرت، انتقادهای زننده و حتی تهدید می‌کنند. توانایی در مخفی شدن پشت اکانت کاربری، اطمینان از مواجه نشدن با افراد در حال مکالمه و یا دور بودن از زمان ملاقات حضوری و بازی انگاشتن فضای مجازی باعث بروز چنین رخدادهایی خواهد شد که نیاز به ایجاد قوانین و بسترسازی جهت جلوگیری از تخریب فرهنگی یک کشور را به امری ضروری مبدل می‌سازد. با توجه به شناخت معضل، بررسی راهکارها جهت جلوگیری از رویداد آن‌ها امری مهم تلقی شده است که در این زمینه یکی از تکنولوژی‌های به‌روز که می‌تواند به حل مسئله یاری رساند، پردازش زبان طبیعی خواهد بود.

منظور از پردازش زبان طبیعی این است که رایانه‌ای داشته باشیم که قادر باشد زبان انسان را تحلیل کند، بفهمد و بتواند زبان طبیعی تولید کند. در نتیجه استفاده از پردازش زبان طبیعی، موجب آماده‌سازی ماشین هوشمند جهت یادگیری و تمییز جملات خوب از بد می‌شود.

در این مقاله، ما دو مدل یادگیری ماشین را در ابتدا برای این مسئله پیاده‌سازی کرده و سپس با کمک سرویس‌های ابری آمازون مدل دیگری را بدست آورده و نتایج آن‌ها را مقایسه می‌کنیم. در انتها مدل به دست آمده را پیاده‌سازی کرده و نتایج آن را با مدل اولیه آمازون مقایسه نموده‌ایم.

در ادامه ساختار مقاله به این صورت است: بخش دوم، کارهای پیشین مورد بررسی قرار گرفته است. در بخش سوم، توصیف روش پیشنهادی آورده شده است. بخش چهارم، پیاده‌سازی روش پیشنهادی و ارزیابی نتایج آن و مقایسه با کارهای پیشین می‌باشد. در بخش پنجم، نتیجه‌گیری و کارهای آینده مورد بحث قرار گرفته است.

## ۲ مروری بر کارهای گذشته

با توجه به گستردگی موضوع نظارت بر محتوای فضای مجازی، شاهد مقالات با موضوعات مشابه در خصوص زبان‌های مختلفی هستیم که به ترتیب، زبان آلمانی [۱]، زبان انگلیسی [۲]، زبان ترکی [۳] و زبان اردو [۴] به

جدول ۱: مقایسه پارامترهای استخراج شده در حوزه شناسایی کلمات توهین آمیز با کمک مدل های بررسی شده

مقاله مرجع	خلاصه کارهای انجام شده	روش استفاده شده	پارامتر بررسی شده
[۵]	مقاله رویکردی برای شناسایی محتوای توهین آمیز به دو زبان انگلیسی و فارسی ارائه شده است.	در این پژوهش، ترکیب BERT با CNN، ANN و RNN بررسی شده است.	F1 macro: 0.863
[۶]	مقاله رویکردی برای شناسایی محتواهای نفرت آمیز در زبان انگلیسی و سپس به صورت چندزبانه ارائه شده است.	در این مقاله ابتدا جملات در زبان انگلیسی به کمک مدل Bert پردازش شده اند؛ سپس چند زبان دیگر به خصوص زبان فارسی با مدل های از پیش پردازش شده با مدل Bert بررسی شده اند.	F1 macro: 0.878

انجام کارهای مشابه پرداخته اند که نشان از اهمیت موضوع دارد. در مقاله های یاد شده ابتدا به چالشی بودن مسئله زبان مهاجمانه در زبان های مختلف پرداخته شده و سپس با کمک مدل های مختلف به کمک پردازش زبان طبیعی به حل مسئله پرداخته اند که نشان از اهمیت بالای این موضوع در زبان های مختلف دارد. در زبان فارسی چالش پیش رو چندان مورد توجه قرار نگرفته و داده های عمومی برای آن آماده نشده است؛ با این حال [۵]، یک راهکار دوزبانه ارائه داده است و مسئله را همزمان برای دو زبان فارسی و انگلیسی به کمک مدل Bert و سایر مدل ها بررسی کرده است که داده های فارسی آن از ۴۹۸۸ ورودی مختلف تشکیل شده است. طبق پارامترهای بررسی شده در مقاله، بهترین متد بیان شده، مدل شبکه عصبی کانولوشن با امتیاز  $F1$ ،  $0.863$  و  $Loss$ ،  $0.4617$  بیان شده است. همچنین [۶] به این مبحث به صورت چند زبانه پرداخته است که البته یک داده ساختار تشکیل شده از ۶۰۰۰ توثیت فارسی را مورد بررسی قرار داده است، متدولوژی این تحقیق نیز بر روی مدل Bert و شبکه های عصبی کانولوشن پایه گذاری شده است و چندین مدل مختلف با یکدیگر به رقابت گذاشته شده اند. جدول ۱ خلاصه کارهای پیشین در زبان فارسی را نشان می دهد.

### ۳ روش های پیشنهادی

در روش های پیشنهادی، ابتدا دو مدل  $k$ -نزدیک ترین همسایه و مدل شبکه عصبی با توجه به پژوهش های انجام گرفته بررسی شده اند؛ سپس به کمک سرویس AutoML، مدل پیشنهادی سرویس آمازون را بررسی کرده و مدل به دست آمده را شبیه سازی کرده تا بتوانیم نتایج پیشین را بررسی و مقایسه کنیم.

### ۱.۳ مدل k-نزدیک‌ترین همسایگی

طبق [۷]، الگوریتم k-نزدیک‌ترین همسایگی (KNN) برای مسائل طبقه‌بندی و رگرسیون قابل استفاده است. اگرچه در اغلب مواقع از آن برای مسائل طبقه‌بندی استفاده می‌شود. برای ارزیابی هر روشی به طور کلی به سه جنبه مهم آن توجه می‌شود: (۱) سهولت تفسیر خروجی‌ها، (۲) زمان محاسبه و (۳) قدرت پیش‌بینی الگوریتم KNN در سه مرحله لیبل داده جدید را تخمین می‌زند:

۱. در مرحله اول KNN، فاصله نمونه تست را با تمامی نمونه‌های آموزش محاسبه می‌کند.
۲. سپس در مرحله دوم بر اساس فاصله بدست آمده، k تا نزدیک‌ترین همسایه از داده‌ی آموزش به داده‌ی تست را پیدا می‌کند.
۳. در مرحله‌ی آخر رای‌گیری انجام می‌دهد تا متوجه شود که از بین این k تا نزدیک‌ترین همسایه کدام کلاس بیشترین همسایه از داده‌ی آموزش به نمونه تست دارد تا تصمیم بگیرد که نمونه جدید به آن کلاس تعلق دارد.

جهت آماده‌سازی داده‌ها، در ابتدا می‌بایست با استفاده از رمزگذار لیبل‌ها، داده‌های جمع‌آوری شده جهت آموزش و تست به دیتافریم قابل استفاده در کدنویسی تبدیل شوند. سپس قسمت‌های مختلف داده‌ی تست که دارای لیبل خوب یا بد بودن جملات است از هم جدا شده و در دیتافریم‌های مختلف ذخیره می‌گردند و خروجی‌ها برای استفاده در مدل، تبدیل به داده‌ی ساختار لیست می‌شوند. بخش بعدی انتقال داده به حالت استاندارد و تبدیل آن‌ها به ویژگی‌های قابل استفاده توسط ماشین است؛ بدین معنی که داده‌ها باید یک ارزش اولیه به خود گرفته و عادی‌سازی انجام شود. سپس یک لیست از داده‌ها و مقدار مربوطه ساخته می‌شود تا بتوان پردازش را بر روی آن‌ها انجام داد. در بخش بعدی، نوبت به انجام عملیات یادگیری ماشین به کمک مدل توضیح داده‌شده رسیده است. ابتدا مشخص می‌کنیم چند درصد از داده تست به عنوان آموزش و چند درصد برای ارزیابی قرار بگیرد؛ سپس به کمک مدل از پیش آماده k-نزدیک‌ترین همسایه را فراخوانی کرده و داده‌ی آماده‌شده به ورودی آن داده شده است. این مدل نیاز دارد بداند که فاصله بین ویژگی‌ها را در چه ابعادی بررسی کند. پس از اتمام پردازش یادگیری ماشین، همانگونه که داده‌های آموزشی انتقال یافتند، داده‌های تست نیز آماده و برای پیش‌بینی به مدل داده می‌شوند و خروجی مورد نظر جهت ارزیابی ذخیره خواهد شد.

### ۲.۳ مدل شبکه عصبی

شبکه‌های عصبی مجموعه‌ای از نورون‌ها هستند که از الگوریتم‌های منحصر به فردی پیروی می‌کنند [۸]. این مجموعه که از مغز انسان الگوبرداری و الهام گرفته شده است، با هدف شناسایی الگوها طراحی می‌شود و مورد استفاده قرار می‌گیرد. به طور کلی می‌توان گفت که شبکه عصبی شامل الگوریتم‌هایی است برای یادگیری ماشین، که منجر به طبقه‌بندی کردن داده‌های ورودی و ارائه خروجی مطلوب می‌گردد. به همین دلیل است که می‌توان شبکه‌های عصبی را به عنوان جزئی از فرایند یادگیری ماشین در نظر گرفت.



برای شناخت ساختار شبکه باید دانست، این شبکه از دو قسمت اصلی تشکیل شده است. قسمت اول لایه‌ای با عنوان Embedding می‌باشد که به کمک آن برداری از اعداد متناسب با هر کلمه ذخیره می‌شوند. به معنای دیگر در این لایه برای هر کلمه یک بردار از اعداد نسبت داده می‌شود که اعداد داخل این بردار در حین آموزش شبکه تغییر می‌کنند. تعدادی از این لایه‌های Embedding از قبل آموزش دیده موجود است که می‌توان از آن‌ها استفاده کرد و دیگر نیازی به آموزش شبکه نباشد؛ ولی به دلیل این که داده‌های موجود، فارسی می‌باشند نمی‌توانیم از Embedding‌های آماده استفاده کنیم و نیاز است که شبکه را آموزش بدهیم. قسمت دوم شبکه را لایه‌های LSTM تشکیل می‌دهند. از این لایه‌ها اغلب برای داده‌های سری زمانی استفاده می‌کنند که در زمینه‌ی داده‌کاوی و پروژه‌های مشابه نیز کاربرد دارند. پس از آموزش شبکه موجود برای تست شبکه، نمونه داده‌هایی را وارد کرده و خروجی بررسی خواهد شد. نتیجه تست شبکه آموزش دیده را بر روی داده‌های تست می‌توان مشاهده کرد.

## ۴ پیاده‌سازی و نتایج

در این بخش، دو حالت پیاده‌سازی را مورد بررسی قرار می‌دهیم. حالت اول مدل k-نزدیک‌ترین همسایه و شبکه عصبی جهت تشخیص کلمات توهین‌آمیز می‌باشد که به صورت لوکال پیاده‌سازی و اجرا شده است و حالت دوم پیاده‌سازی و اجرا توسط سرویس‌های آمازون است.

### ۱.۴ پیاده‌سازی الگوریتم‌های پیشنهادی

داده‌های جمع آوری شده تعداد ۶۰۰ جمله هستند که قسمتی از آن‌ها توهین‌آمیز و قسمتی دیگر جملات مودبانه می‌باشند. البته دیتاست موجود به سه قسمت سالم، ناسالم و بسیار ناسالم تقسیم شده است ولی برای راحتی کار دو دسته‌ی آخر در گروه ناسالم قرار گرفته شده‌اند. تمامی داده‌ها (جملات) در فایل اکسل قرار می‌گیرند. در فایل اکسل علاوه بر جملات در ستون جداگانه‌ای با عنوان "Label" مقدار صفر برای داده‌های ناسالم و یا یک برای جملات سالم اختصاص داده شده است؛ در واقع با این کار داده‌های هدف خود را ایجاد می‌کنیم که برای آموزش شبکه مورد نیاز می‌باشند. در ادامه داده‌ها خوانده و در یک جدول ذخیره شده‌اند تا برای ورود به مدل‌های ارائه شده آماده باشند. پردازش‌های پیشنهاد شده در بخش ۳، به کمک پردازنده Core i7-10750H با قدرت پردازشی 2.60 GHz انجام شد؛ همچنین از یک حافظه Ram، 16 GB استفاده شده است. پیاده‌سازی انجام شده، به کمک زبان برنامه‌نویسی پایتون، و به کمک کتابخانه‌های Pandas [۹] که در جهت خواندن فایل‌ها و Scikit Learn [۱۰] و Keras [۱۱] برای پیاده‌سازی مدل‌های مختلف استفاده شده‌اند. با توجه به حجم داده‌ی سرعت پردازش‌ها به مرور کاهش می‌یابد، به هر میزان داده افزایش یابد با در نظر گرفتن محدودیت‌های سخت افزاری آموزش داده‌ها زمان بیشتری را خواهد طلبید. در ادامه استفاده از سرویس ابری آمازون مورد بحث قرار گرفته است.

## ۲.۴ استفاده از سرویس‌های یادگیری ماشین آمازون با داده‌های موجود

Amazon SageMaker Studio یکی از معروف‌ترین سرویس‌های آمازون کلود برای آموزش و استقرار مدل‌های مختلف یادگیری ماشین است. Autopilot یکی از ابزارهای سرویس SageMaker است که وظایف کلیدی فرایند یادگیری ماشین را خودکار می‌کند؛ یعنی داده‌ها را بررسی کرده، الگوریتم‌های مربوط به نوع مسئله را انتخاب و داده‌ها را برای آموزش و تنظیم مدل آماده می‌کند [۱۲].

Best model	Accuracy	PrecisionMacro	BalancedAccuracy	F1macro	RecallMacro	Algorithm
OffensivePersianLanguageTest2bJL-083-c4e9819e	0.962	0.968	0.933	0.947	0.933	XGBoost

Model name	Objective: Accuracy	F1macro	Status
OffensivePersianLanguageTest2bJL-083-c4e9819e	0.962	0.947	Completed
OffensivePersianLanguageTest2bJL-084-b5e2ac8a	0.962	0.945	Completed
OffensivePersianLanguageTest2bJL-063-270278b5	0.961	0.944	Completed
OffensivePersianLanguageTest2bJL-081-3ecda2f2	0.961	0.944	Completed
OffensivePersianLanguageTest2bJL-096-5172b861	0.961	0.946	Completed
OffensivePersianLanguageTest2bJL-065-330fd40f	0.959	0.943	Completed
OffensivePersianLanguageTest2bJL-094-3058535b	0.959	0.944	Completed
OffensivePersianLanguageTest2bJL-059-4afd9843	0.959	0.941	Completed
OffensivePersianLanguageTest2bJL-091-6e523b67	0.959	0.941	Completed

شکل ۱: بخشی از مدل‌های مختلف بررسی شده به صورت اتوماتیک و انتخاب مدل XGBoost به عنوان بهترین مدل و درصد دقت و F1

در مرحله اول داده‌ها باید در Amazon S3 قرار بگیرند تا به آن‌ها از سمت Amazon SageMaker Studio دسترسی داده شود. در مرحله بعد، از بخش فایل گزینه Experiment را انتخاب می‌کنیم تا به محیط ساخت یک پایپلاین Autopilot هدایت شویم. در ادامه مشخص می‌کنیم که کدام ستون هدف ما خواهد بود تا استودیو بتواند داده را تجزیه تحلیل کرده و بر اساس آن یک مدل پیشنهاد دهد. در انتها نیاز است تعیین گردد پروژه از چه نوعی است و چه نوع پردازشی براساس داده‌ها بهتر است که البته دارای نوع خودکار نیز می‌باشد. به ازای هرکدام از این مراحل داده‌های مخصوص به آن را آمازون استخراج کرده و در یک بخش مخصوص به خروجی آن قرار می‌دهد و برای بررسی بهتر قابل دسترسی خواهد بود. در ادامه سیستم Autopilot، شروع به مهندسی ویژگی می‌کند. مهندسی ویژگی یا استخراج ویژگی، فرایند استفاده از دانش دامنه برای استخراج ویژگی‌ها از داده‌های خام است. انگیزه‌ی استفاده از این ویژگی‌های اضافی برای بهبود کیفیت نتایج حاصل از فرایند یادگیری ماشین در مقایسه با ارائه تنها داده خام به فرایند یادگیری ماشین می‌باشد. در این راه آمازون داده‌های با ساختار بهتر برای استفاده در مدل‌ها ایجاد می‌کند.

در بخش اصلی پردازش سرویس، مدل‌های مختلف موجود با داده‌های پردازش شده تحلیل می‌گردند و دقت آن‌ها ارزیابی شده و در نهایت بهترین مدل توسط سرویس معرفی می‌گردد. همچنین در این مرحله هر بار مدل‌ها تنظیم می‌شود، تنظیم معمولاً یک فرآیند آزمون و خطا است که توسط آن برخی از فرآیندها تغییر داده می‌شوند (مثلاً تعداد درخت‌ها در یک الگوریتم مبتنی بر درخت یا مقدار آلفا در یک الگوریتم خطی)، دوباره الگوریتم روی داده‌ها اجرا می‌شود، سپس عملکرد آن در مجموعه اعتبارسنجی مقایسه می‌شود تا

مشخص شود کدام مجموعه از فرآپاراترها دقیق‌ترین مدل را به دست می‌آورند. با این حساب، دقت مدل تا جای امکان توسط خود سامانه Autopilot انجام می‌گیرد.

همان‌طور که در شکل ۱ مشخص است، بهترین مدل موجود از نظر آزمون مدل XGBoost است. الگوریتم Extreme Gradient Boosting از دسته الگوریتم‌های گرادیان تقویتی بوده که عملکرد بسیار خوبی در دسته‌بندی، رگرسیون و رتبه‌بندی داشته و به دلیل پیش‌بینی دقیق، سرعت زیاد و پشتیبانی از اجرای چندمنظوره و توزیع‌شده‌ی آن، در مسائل دسته‌بندی بسیار محبوب است. XGBoost به طور خاص، این الگوریتم را برای تقویت درخت تصمیم با یک عبارت تنظیم سفارشی اضافی در تابع هدف پیاده‌سازی می‌کند.

### ۳.۴ پیاده‌سازی سرویس مدل XGBoost

با توجه به اطلاعات بدست‌آمده، الگوریتم XGBoost [۱۳] را همانند مدل‌های پیشنهادی در بخش ۳، پیاده‌سازی کرده‌ایم تا علاوه بر مقایسه با کارهای پیشین در این مقاله و همچنین مقایسه با کارهای پیشین در فصل دو بتوانیم این اطلاعات را با یک پیاده‌سازی توسط عامل انسانی نیز مقایسه کنیم. پیاده‌سازی این مدل به کمک کتابخانه XGBoost انجام شد و مراحل آن همچون مدل KNN می‌باشد.

با وجود دانش بر استفاده از مدل XGBoost، بدون تنظیم دقیق مدل بر اساس داده و پیش‌پردازش دقیق به درصدی پایین‌تر از خروجی مدل آزمون و با مقادیری نزدیک به مدل‌های قبلی خواهیم رسید که نشان از تاثیرگذاری پردازش‌های آزمون بر روی متن و همچنین شخصی‌سازی مدل برای داده را دارد. با این وجود برای پردازش داده‌های خاص و پر اهمیت نیاز به یک متخصص علم داده برای فهم و ایجاد تغییرات مورد نیاز است. همچنین با توجه به استفاده آزمون از کتابخانه‌های اختصاصی خود متخصص در صورت نیاز به انجام پروژه‌های خاص‌تر و یا شخصی‌سازی شده‌تر نیاز به آشنایی با نحوه کار با این کتابخانه‌ها خواهد داشت و یادگیری آن‌ها می‌تواند زمان یادگیری برای انجام کار را بیش از پیش کند. همچنین در صورت نیاز به استقرار محصول، معمول‌ترین راه استفاده از مدل‌ها استفاده از خود آزمون است و در صورت نیاز به استقرار به صورت محلی چالش‌هایی وجود دارد. در نهایت به نظر می‌آید وجود محصولات نوین در سرویس‌های ابری می‌تواند کمک شایانی به رشد علوم مختلف کند.

### ۴.۴ ارزیابی نتایج

در این پژوهش تلاش شد تا به بررسی کنترل محتوای متنی فضای سایبری با گرایش پردازش زبان پرداخته شود تا مزایای روش‌های جدید نسبت به روش‌های معمول نشان داده شود. هدف از پیدایش سرویس‌هایی همچون Amazon Autopilot کمک به صنایعی است که علاقه‌مند به رشد خود به کمک هوش مصنوعی را دارند. از این طریق این علم به‌روز نیز فرصت‌های بیشتری برای پیشرفت پیدا خواهد کرد. همچنین کاربران نهایی نیز می‌توانند از پیشنهادات و همچنین سهولتی که توسط صاحبان صنایع برایشان ایجاد کرده‌اند، استفاده کرد.

بایستی اشاره کرد همچنان نیز دانشمندان علم داده و محققان عرصه هوش مصنوعی گام‌های متعددی

Metric Name	Value	Standard Deviation
accuracy	0.9625	0.0036570983477315945
weighted_recall	0.9625	0.003657098347731561
weighted_precision	0.9641346500721502	0.0034308255123618463
weighted_f0_5	0.9627209249918511	0.0036665997672579364
weighted_f1	0.9616973988367469	0.003823846455268386
weighted_f2	0.9618344359589286	0.003778078644836735
accuracy_best_constant_classifier	0.496875	0.005375001455356815
weighted_recall_best_constant_classifier	0.496875	0.005375001455356815
weighted_precision_best_constant_classifier	0.246884765625	0.005316383722923077
weighted_f0_5_best_constant_classifier	0.2745070361362057	0.005588829785636524
weighted_f1_best_constant_classifier	0.3298669102296451	0.005937197673386191
weighted_f2_best_constant_classifier	0.4131962604602511	0.005961186581812905

شکل ۲: اطلاعات آماری قابل برداشت از سرویس Amazon Autopilot

جهت اعتلای این علوم نوین در پیش خواهند داشت و بیشتر این ابزار جهت تسهیل راه آن‌ها در برداشتن این گام‌ها خواهد بود. جدای از زمان مورد نیاز برای جمع‌آوری داده‌های قابل استفاده برای یک پروژه‌ی یادگیری ماشین، انجام مراحل پیش‌پردازش، پردازش و استقرار یک ماشین آموزش‌دیده در آمازون در برابر طی کردن مسیر به طور معمول بسیار کمتر بود؛ به نحوی که ششصد داده‌ی آماده‌شده توسط سرویس‌های این مجموعه کمتر از دو ساعت به طول انجامید؛ در حالی که انجام موارد مستلزم دو مدل قبلی و پردازش به کمک آن‌ها زمان بسیار بیشتری از نظر پیدا کردن الگوی مناسب و همچنین پیش‌پردازش نیاز داشت و تمامی کار در حدود یک ماه به طول انجامید که البته در صورت وجود یک متخصص ممکن بود بسیار کاهش پیدا کند. علاوه بر این، نیاز صنایع برای به‌کارگیری متخصصان حرفه‌ای با توجه به ابزارهای موجود در آمازون کاهش پیدا می‌کند.

شایان ذکر است از لحاظ کارآمدی مدل‌های آموزش‌دیده KNN و شبکه عمیق نسبت به مدل‌های آماده‌شده و تنظیم‌شده توسط آمازون دقت کمتری را ارائه داده‌اند.

## ۵.۴ ارزیابی نتایج

همان‌طور که در جدول ۲ مشخص شده است، دقت مدل پردازش‌شده توسط آمازون از مدل‌های آماده‌شده‌ی قبلی بالاتر بوده و نشان‌دهنده‌ی دقت بالای این سرویس است. با این وجود آمازون قابلیت این را دارد که کاربر مدل را تحلیل کرده و در صورت نیاز تغییراتی در آن ایجاد کند.

## ۵ نتیجه‌گیری

در این مقاله به بررسی شناسایی کلمات توهین‌آمیز در خطوط متنی فارسی زبان با هدف نظارت بر سلامت اخلاقی فضای مجازی پرداختیم. در راستای این هدف، دو مدل یادگیری ماشین نزدیک-k همسایه و مدل شبکه عصبی پیشنهاد شد. سپس با کمک سرویس Amazon SageMaker و ابزار Autopilot این سرویس بر روی دیتاست موجود، مدل XGBoost به عنوان مدل برتر با دقت بهتر به دست آمد. در نهایت جهت اعتبارسنجی نتیجه‌ی سرویس Autopilot آمازون، این مدل نیز پیاده‌سازی و با دو مدل قبلی مقایسه گردید.

جدول ۲: مقایسه پارامترهای استخراج شده در حوزه شناسایی کلمات توهین آمیز با کمک مدل های بررسی شده

F1 macro	دقت	مدل
0.594	0.875	KNN
0.292	0.835	شبکه عصبی
0.933	0.962	Amazon Autopilot XGBoost
0.561	0.860	XGBoost

نتایج به دست آمده حاکی از برتری این مدل و در نتیجه اعتماد به سرویس Autopilot آمازون است.

## مراجع

- [1] Samantha Kent. (2018). German hate speech detection on Twitter, In Proceedings of the 14th Conference on Natural Language Processing (KONVENS'18), 120–124.
- [2] Georgios Pitsilis, Heri Ramampiaro, and Helge Langseth, (2018). Effective hate-speech detection in Twitter data using recurrent neural networks, Appl, Intell, 48, 4730–4742.
- [3] Selma Ayse Ozel, Esra Sarac, Seyran Akdemir, and Hulya Aksu, (2017). Detection of cyberbullying on social media messages in Turkish, In Proceedings of the International Conference on Computer Science and Engineering (UBMK'17), 366–370.
- [4] Raza Mustafa, M. Saqib Nawaz, Javed Ferzund, M. Ikram Ullah Lali, Basit Shahzad, and Philippe Fournier-Viger, (2017). Early detection of controversial Urdu speeches from social media. Data Sci, Pattern Recog, 1, 26–42.
- [5] Marzieh Mozafari. (2021). Hate speech and offensive language detection using transfer learning approaches. Document and Text Processing, Institut Polytechnique de Paris.
- [6] Alavi, P., Nikvand, P., & Shamsfard, M. (2021). Offensive Language Detection with BERT-based models, By Customizing Attention Probabilities. ArXiv, abs/2110.05133.
- [7] Guo, G., Wang, H., Bell, D., Bi, Y., Greer, K. (2003). KNN Model-Based Approach in Classification. In: Meersman, R., Tari, Z., Schmidt, D.C. (eds), On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE. OTM 2003. Lecture Notes in Computer Science, vol 2888. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-540-39964-3\\_62](https://doi.org/10.1007/978-3-540-39964-3_62).
- [8] Alshemali, B., & Kalita, J. (2019). Improving the reliability of deep neural networks in NLP: A review. Knowledge-Based Systems. <https://doi.org/10.1016/j.knosys.2019.105210>.
- [9] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... & Duchesnay, E. (2011). Scikit-learn: Machine learning in Python. the Journal of machine Learning research, 12, .2825-2830

- [10] McKinney, W. (2011). Pandas: a foundational Python library for data analysis and statistics. *Python for high performance and scientific computing*, 14(9), .1-9
- [11] Ketkar, N. (2017). Introduction to keras. In *Deep learning with Python* (pp. 97-111). Apress, Berkeley, CA.
- [12] Antje Barth, Shelbee Eigenbrode, Sireesha Muppala, Chris Fregly, Analyze Datasets and Train ML Models using AutoML, Coursera. <https://www.coursera.org/lecture/automl-datasets-ml-models/specialization-overview-eqDJv>.
- [13] Chen, T., He, T., Benesty, M., Khotilovich, V., Tang, Y., Cho, H., & Chen, K. (2015). XGBoost: extreme gradient boosting. *R package version 0.4-2*, 1(4), .1-4



## سیستم اعتبار اجتماعی: مروری بر دیدگاه‌ها

علیرضا زینی<sup>۱</sup>، حسین عظیمی<sup>۱</sup>، علی لکزائی<sup>۱</sup>، کاظم فولادی قلعه<sup>۲</sup>

<sup>۱</sup> دانشجوی کارشناسی مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران  
{alireza.zeini2001,husein.azimi,sinalakzaee}@ut.ac.ir  
<sup>۲</sup> استادیار، گروه مهندسی کامپیوتر، دانشکده مهندسی دانشکدگان فارابی دانشگاه تهران؛  
سرپرست آزمایشگاه پژوهشی فضای سایبر دانشگاه تهران  
kfouladi@ut.ac.ir

### چکیده

با پیشرفت تکنولوژی در زمینه‌ی جمع‌آوری و تحلیل داده‌ها، داده‌های تولید شده از فعالیت‌های مختلف انسان‌ها ارزش بسیار بیشتری برای حاکمان سیاسی و دولت‌ها پیدا کرده است و به آنها این قدرت را داده است تا بینش بهتر و همچنین کنترل شدیدتری بر شهروندان خود داشته باشند. به‌منظور دستیابی به این مقصود، کشورهای مختلف به دنبال سیستمی هستند که افراد را بر حسب عملکرد آنها اعتباربخشی کند که به آن «سیستم اعتبار اجتماعی» گفته می‌شود. این نوع از سیستم‌های اعتباربخشی در جهان، عمدتاً تک‌بعدی هستند و بخش‌های خاصی از زندگی افراد را دربر می‌گیرد. در میان این سیستم‌ها، سیستم اعتبار اجتماعی چین، دارای ابعاد متعددی است و جنبه‌های گوناگونی از زندگی شهروندان چینی در آن مورد توجه قرار گرفته است. در این مقاله، این سیستم را از ابعاد مختلف اقتصادی، فرهنگی، اجتماعی، سیاسی، قانونی و فنی در دیدگاه‌های صاحب‌نظران مختلف واکاوی کرده‌ایم. نتایج این مطالعه نشان می‌دهد که اگرچه جنبه‌های مثبتی در خصوص این سیستم‌ها در نگاه برخی اندیشمندان وجود دارد، اما نگرانی‌ها از گسترش این سیستم‌ها بسیار جدی‌تر بوده و توجه طیف وسیع‌تری از پژوهشگران به جنبه‌های منفی سیستم اعتبار اجتماعی معطوف شده است.

**کلمات کلیدی:** سیستم اعتبار اجتماعی، رتبه‌بندی شهروندان، حاکمیت سایبرنتیکی.

### ۱ مقدمه

اعتبار افراد یکی از مهم‌ترین شالوده‌های تعامل در جامعه می‌باشد؛ به همین خاطر برخی از کشورها به سمت سیستمی اعتباری حرکت کرده‌اند تا بتوانند بر اساس راهبرد تنبیه و پاداش به سازمان‌ها، شرکت‌ها و افراد اعتبار ببخشند.

می‌توان از این دست سیستم‌ها به سیستم‌های امتیاز اعتباری<sup>۱</sup> اشاره کرد. برای نمونه شرکتی در آمریکا

<sup>۱</sup> credit score systems

به نام FICO<sup>۲</sup> بر اساس اطلاعات مالی افراد از جمله سابقه پرداخت، طول تاریخ اعتبار و مبالغ بدهکاری، امتیاز اعتباری افراد رامحاسبه می‌کند [۱]. امتیاز هر شهروند بر نرخ بهره‌ی پیشنهادی، دریافت وام و کارت اعتباری آن شخص تأثیرگذار است [۲]. شرکت‌های مالی دیگری مثل Affirm در آمریکا نیز بر اساس گزارش اعتبار مرسوم به بررسی پروفایل افراد در پلتفرم‌های رسانه‌های اجتماعی مانند فیسبوک ارزیابی می‌کنند که چه افرادی شایسته دریافت وام هستند [۳، ۴]. در استرالیا نیز، شرکت لادکس<sup>۳</sup> احتمال بازپرداخت وام را از طریق تجزیه و تحلیل فعالیت‌های تلفن هوشمند افراد نظیر خریدهای آنلاین و شیوه‌ی پاسخ‌دادن به ایمیل‌ها پیش‌بینی می‌کند [۲]. همچنین در آلمان شرکت شیوفا<sup>۴</sup> با استفاده از امتیازدهی جغرافیایی، عمل رتبه‌بندی اعتباری را انجام می‌دهد [۵].

با وجود تعدد این نوع ساختار در کشورهای مختلف، سازه‌ای به نام سیستم اعتبار اجتماعی در چین فراتر از سیستم‌های اعتباری سایر کشورها است؛ زیرا نه تنها فعالیت‌های مالی و تجاری، بلکه رفتارهای اجتماعی را نیز در نظر می‌گیرد؛ به‌صورتی که این سیستم از نظر صاحب‌منصبان یک «نظام اعتبار اجتماعی گسترده»<sup>۵</sup> در نظر گرفته می‌شود [۶]. به همین علت در این مقاله سیستم اعتبار اجتماعی چین بررسی می‌شود. کلمه «اعتبار»<sup>۶</sup> در زبان چینی تعاریف گسترده‌ای دارد. معمولاً برای مجموعه‌ای از فضایل اخلاقی مانند امانت‌داری، وفای به عهد، پایبندی به هنجارها، صداقت و نجابت به کار می‌رود [۷]؛ به عبارتی در تاریخ چین، «اعتبار» برای نشان‌دادن اصول اخلاقی، به‌ویژه اخلاق فردی به کار گرفته می‌شد [۸]؛ اما در چین معاصر، مفهوم اعتبار شامل معانی گسترده‌تری از جمله جنبه‌های اجتماعی، جنبه‌های مالی، و جنبه‌های حقوقی را نیز در بر می‌گیرد [۹].

این سیستم با کمک فناوری دیجیتال به‌عنوان یک سیستم نوآورانه برای بهبود قابلیت اعتماد در جامعه و افزایش اجرای قوانین و مقررات طراحی و اجرا می‌شود. برای انجام این کار، این برنامه از یک سیستم رتبه‌بندی به‌ازای رعایت قوانین، هنجارهای اخلاقی و عمل به وعده‌ها استفاده می‌کند [۱۰]. این سیستم اعتباری، متشکل از دو لیست سیاه و قرمز می‌باشد. افراد در صورت عدم رعایت قوانین و هنجارهای اخلاقی با کاهش اعتبار در لیست سیاه قرار می‌گیرند که تبعاتی از جمله ممنوعیت سفر هوایی یا ریلی، اقامت در برخی هتل‌ها و ممنوعیت در ثبت‌نام فرزندان آنها در مدارس خصوصی و سایر موارد خواهد داشت [۱۱، ۳۵].

همچنین در صورت رعایت موارد مذکور با افزایش اعتبار، افراد در لیست قرمز قرار می‌گیرند که منجر به دسترسی آسان به خدمات عمومی، اعمال تخفیف در صورت‌حساب‌ها، تسهیل در دریافت وام و مواردی از این دست خواهد شد [۱۲].

در اوایل دهه‌ی ۱۹۹۰، ایده‌ی ایجاد یک سیستم اعتباری در پاسخ به مشکل بدهی شرکت‌های چینی مطرح شد. در واقع، تقاضا برای یک سیستم اعتباری در چین را می‌توان به «بدهی مثلی» در اوایل سال

<sup>۲</sup>Fair Isaac Corporation

<sup>۳</sup>Lodex

<sup>۴</sup>Schufa

<sup>۵</sup>broad social credit system

<sup>۶</sup>xinyong

۱۹۹۰ یافت که با توسعه اصلاحات اقتصادی، بسیاری از شرکت‌های چینی در پرداخت بدهی‌های خود قصور کرده و به یکدیگر بدهکار شدند. در همین راستا از دلایل دیگری که موجب احداث این نوع سیستم شد، عدم پرداخت وام‌های دریافتی بود [۱۳]. در نتیجه، حمایت اولیه از یک سیستم اعتباری در چین، به رسیدگی مشکلات در بخش‌های تجاری و مالی بر می‌گردد [۱۴].

در سال ۲۰۰۲، رئیس‌جمهور «جیانگ زمین»<sup>۷</sup> تقاضای سیستم اعتبار اجتماعی را برای تنظیم رفتار بازار مطرح کرد [۱۵]. در مارس ۲۰۰۷، شورای دولتی، اطلاعیه‌ای تحت عنوان «نظرات اداره کل شورای دولتی در مورد ایجاد یک سیستم اعتبار اجتماعی» صادر کرد [۱۶]. همان‌طور که پیش‌تر نیز ذکر شد، این سند بر نیاز فوری به ایجاد یک سیستم اعتبار اجتماعی برای حفظ «اقتصاد بازار سوسیالیستی» تأکید می‌کند. در ۱۴ ژوئن ۲۰۱۴، شورای ایالتی سند دیگری صادر کرد که مبنی بر موضوع: «اعلامیه شورای ایالتی در مورد صدور طرح کلی برنامه‌ریزی برای ایجاد یک سیستم اعتبار اجتماعی - ۲۰۱۴ تا ۲۰۲۰» بود [۱۷]. در مقایسه با سند قبل، این سند تصویر دقیق‌تری در مورد ایجاد یک سیستم اعتبار اجتماعی یکپارچه ارائه می‌دهد. دولت چین دامنه‌ی تعریف اعتبار اجتماعی را گسترش و مفهوم اعتبار اجتماعی برای حل طیف وسیعی از مسائل اجتماعی به چهار بعد سیاسی، اقتصادی، اجتماعی و قضایی تقسیم کرد [۱۸]. از دیدگاه محققان مفاهیم اعتبار می‌توانند در چهار بعد، اهدافی را دنبال کنند؛ یعنی دولت:

- در بعد اقتصادی با اجرای امتیاز اعتبار مالی و اجرای قانون در میان فعالان بازار، به دنبال مدیریت بهتر این حوزه است.
- از جنبه سیاسی به جهت مبارزه با فساد - هم‌چنین به‌عنوان ابزاری در سیاست جناحی - افزایش قابلیت‌های نظارتی حزب یا دولت مورد توجه واقع شد.
- از دیدگاه اجتماعی به‌سبب ایجاد اعتماد اجتماعی مطابق با استانداردها و ارزش‌های تعیین‌شده توسط حزب کمونیست چین، بهبود کنترل، مدیریت و حکمرانی بهتر مورد توجه قرار گرفته است.
- در نهایت از منظر بعد هنجاری ارتقای نقش‌ها و وظایف اجتماعی بر اساس منافع حزب کمونیست چین و مهندسی اجتماعی<sup>۸</sup> مورد اهتمام قرار گرفت [۱۹].

اما هدف اصلی از تأسیس سیستم اعتبار اجتماعی را می‌توان در شعار رهبران چینی فهمید که «افراد قابل اعتماد بتوانند در همه‌جا زیر آسمان قدم بزنند و در عین حال، برداشتن یک قدم برای افراد بی‌اعتبار سخت شود [۹۱].»

چندبعدی بودن این سیستم، موجب شد تا پژوهشگران از جنبه‌های مختلف آن را بررسی کنند. به‌سبب حجم زیادی از اطلاعات و بررسی‌ها از دیدگاه‌های متنوع، لزوم تدوین مقالاتی که به جمع‌آوری و انسجام‌بخشی به مطالب اقدام کنند، بسیار ضروری‌تر از گذشته احساس می‌شود. بر اساس چنین ضرورتی ما در این مقاله

<sup>7</sup>Jiang Zemin| 江泽民

<sup>8</sup>social engineering

مروری قصد داریم بازبینی دیدگاه‌های متنوع از جنبه‌های قانونی، اقتصادی، اجتماعی، فرهنگی، سیاسی و فنی را داشته باشیم.

## ۲ قانون

هدف رهبران کشور چین که «شکستن اعتماد در اینجا، محدودیت‌ها در همه‌جا»، اصل راهنمای مجازات‌ها و همکاری بخش‌های مختلف، در سیستم اعتبار اجتماعی است [۲۰]. در این سیستم به منظور اعتباربخشی، در مجموع ۳۰ معیار خاص، از جمله سوابق رفتار در جامعه، مبادلات پولی، سوابق مالیاتی، جرایم ترافیکی، شبکه‌های اجتماعی و فعالیت‌های اینترنتی و غیره به‌طور منظم ارزیابی می‌شوند. کسب امتیاز بالا می‌تواند منجر به قرارگیری در لیست قرمز و به‌تبع آن دسترسی سریع به خدمات حیاتی از جمله بیمه‌ی پزشکی و آموزش، رسیدگی سریع‌تر در امور گمرک، درخواست ویزا و مجوز نگهداری حیوانات و سایر موارد شود. از سوی دیگر افرادی که نمرات کمتری دارند، در لیست سیاه قرار گرفته و دسترسی به خدمات آنها محدود خواهد شد. دولت چین این افراد را غیرقابل اعتماد و آزارساننده به دیگران می‌داند [۲۱]. حتی اطلاعات این افراد را در معرض عموم قرار می‌دهد تا اثر شرم ایجاد کند.

از آنجایی که افزایش و یا کاهش اعتبار افراد بر مبنای قوانین حاکم و توسط ماشین (هوش مصنوعی) انجام می‌شود، عدم تدوین قوانین مشخص و شفاف در مورد این موضوع که چه چیزی رفتار قانون‌گیزانه یا قانون‌مدارانه تلقی می‌شود، به این معنی است که افراد و نهادها نمی‌دانند برای چه چیزی جریمه می‌شوند [۲۲، ۴۲]. از منظر صاحب‌نظران یکی از چالش‌های این سیستم اعتباری همین عدم شفافیت است؛ به‌گونه‌ای که در برخی موارد، افراد بدون اطلاع قبلی نام خود را در لیست سیاه یافته‌اند [۲۳، ۲۸]. به‌عنوان مثال ۸۳/۹ درصد از پاسخ‌دهندگان به نظرسنجی مرکز تحقیقات اجتماعی روزانه جوانان چین می‌ترسند بدون اطلاع در لیست سیاه قرار گیرند [۲۴].

لذا مشکلی که به وجود می‌آورد این است که افراد و شرکت‌ها از وضعیت خود در لیست سیاه آگاه نیستند تا زمانی که شرایطی مانند رزرو بلیط هواپیما برای آنها رخ دهد.

## ۱.۲ کنترل اجتماعی

مفهوم کنترل، ریشه در دانش سایبرنتیک دارد. سایبرنتیک که از واژه یونانی کوبرنتیس نشأت گرفته است، به‌معنای سکان‌داری و کنایه از حکمرانی است. به‌همین جهت سیستم اعتبار اجتماعی که بر پایه‌ی دانش سایبرنتیک شکل گرفته است، این باور را در پی دارد که چین به واسطه سیستم اعتبار اجتماعی به دنبال کنترل اجتماعی جمعیت خود می‌باشد. به‌عقیده مؤسسه مطالعات سیاسی آسیا<sup>۹</sup> «سیستم جدید چین یک سیستم اعتبار اجتماعی نیست؛ بلکه یک سیستم کنترل اجتماعی» است [۲۵].

در این سیستم اطلاعات افراد به‌صورت مداوم در جهت تخصیص اعتبار مورد ارزیابی قرار می‌گیرد. مطالباتی که از شهروندان می‌شود نه تنها باعث می‌شود که آن‌ها بر اساس دستور کار مسئولان رفتار کنند

<sup>۹</sup> کره جنوبی

بلکه زندگی و سبک زندگی آن‌ها را نیز شکل می‌دهد. در نتیجه ارزیابی دائمی و مداخله نیمه‌خودکار منجر به تعریف شهروند مبتنی بر امتیاز یا «شهروند سایبرنتیکی»<sup>۱۰</sup> خواهد شد [۲۶].

صرف نظر از اینکه به نظر می‌رسد یک شهروند در کوتاه‌مدت سیستم را شکست می‌دهد یا خیر، هر چه فرد بیشتر تلاش کند تا زندگی متکی بر خودش داشته باشد، بیشتر به خود داده‌ها و این سیستم وابسته است. در نهایت، دولت به دلیل عدم تقارن اطلاعاتی و معیارهای دلخواه برای مجازات‌ها و پاداش‌ها، دست بالا را در ساخت این سیستم و داده‌ها دارد. نتیجه نهایی تسلط خود به خودی داده‌ها و وابستگی بیشتر به دولت است. در واقع دیجیتالی‌سازی و اطلاع‌رسانی آیت‌های کلیدی با هدف صریح «استفاده از کلان‌داده برای مدرن‌سازی حکمرانی ملی» در دستور کار سیاسی چین می‌باشد؛ موضوعی که قرار است در برنامه‌ی پنج‌ساله‌ی (2020-2025) چین برجسته شود [۲۷]. کنترل اجتماعی در این سیستم اعتباری به دو صورت رخ می‌دهد: کنترل دولت بر شهروندان و کنترل شهروندان بر یکدیگر.

## ۱.۱.۲ کنترل دولت بر شهروندان

نگرانی محققان از این باب است که کنترل کلی از وضعیت زندگی افراد من جمله رصد مداوم شبکه‌های اجتماعی، استفاده طولانی‌مدت از اینترنت برای انجام بازی‌های ویدیویی، پرداخت دیرنگام قبوض و سایر فعالیت‌ها انجام می‌شود [۲۵]. به همین دلیل برخی شهروندان چینی نگران این نوع کنترل هستند که تحت چنین سیستمی به وجود آمده است؛ به گونه‌ای که این موضوع برای همه‌ی شهروندان بدون هیچ استثناء صدق می‌کند [۲۸]. از طرفی با توجه به شهرت چین به مقررات سخت‌گیرانه و سرکوب سخنرانی‌های سیاسی و دیگر فعالیت‌ها، یکی از نگرانی‌های اصلی این است که این سیستم می‌تواند مورد سوء استفاده برای کنترل اجتماعی دولت بر شهروندان قرار گیرد. حتی به دلیل مالکیت دولت بر این سیستم، می‌تواند به راحتی هر کسی را که خط حزبی مربوطه را رعایت نمی‌کند، شناسایی و مجازات کند [۲۸].

از سوی دیگر اعتبار اجتماعی به یکی از پایه‌های قانون ایدئولوژیک جدید «اندیشه‌ی شی جین پینگ»<sup>۱۱</sup> در مورد حاکمیت قانون» تبدیل شده است [۲۹]. شواهد نشان می‌دهد که مسئولین چین برای عدم قانون‌گریزی این نوع کنترل را الزامی می‌دانند. به عنوان نمونه شرط دریافت وام‌های گران‌قیمت برای افراد کم‌اعتبار، نصب فناوری‌های نظارتی روی وسایل نقلیه افراد می‌باشد تا خودرو و شخص به عنوان دارایی قابل مدیریت تبدیل شوند. در جریان این اطلاعات، این نوع از فناوری نظارتی، رفتارهای رانندگی و مکان‌های وام‌گیرنده را در جریان داده‌های بلادرنگ ثبت می‌کنند. در عین حال قدرت غیرفعال کردن خودرو از راه دور را به وام‌دهندگان می‌دهد [۳۰].

## ۲.۱.۲ کنترل شهروندان بر یکدیگر

از سویی نیز در این سیستم اعتباری، کنترل به خود شهروندان برمی‌گردد؛ بدین معنا که هر شهروندی برای عدم کاهش اعتبار خود، اطرافیان خود را تحت نظر قرار می‌دهد تا خطایی از آنها سر نزنند. هامفریز توضیح

<sup>10</sup> cybernetic citizenship

<sup>11</sup> Xi Jinping

می‌دهد: «به دلیل اینکه داده‌ها از طریق شبکه‌های اجتماعی ردیابی می‌شوند، دولت می‌داند که دوستان شما چه کسانی هستند. اگر هر یک از دوستان شما نظرات سیاسی مخالف پست کنند علاوه بر اینکه امتیاز آن شخص کاهش می‌یابد؛ به دلیل اینکه شما دوست آن فرد هستید موجب افت امتیاز شما نیز می‌شود. با پیوند دادن این دو، واضح است که دولت می‌خواهد همه مراقب دوستانشان باشند که پایشان را از حد فراتر نگذارند» [۳۱].

این حقیقت که کسی به خاطر رفتار دیگران مجازات شود ذاتاً ناعادلانه است [۱۲] سیاست تداعی گناه معمولاً در چین برای کنترل مردم، معترضان و ناآرامی‌ها اعمال می‌شود [۳۲]. اثر زنجیره‌ای که توسط شبکه اجتماعی هرکس ایجاد می‌شود، ممکن است به فرصت‌هایی برای سوزدها منجر شود که ناخودآگاه یکدیگر را کنترل کنند.

برخی نیز معتقدند که سیستم رتبه‌بندی اجتماعی این امکان را به افراد می‌دهد که شایسته‌ترین نامزدهای خدمات عمومی را مشخص کنند و موقعیت‌های مهم را به شایسته‌ترین افراد ارائه دهند [۳۳]. از طرفی امروزه رسانه‌ها در جهت‌دهی افکار عمومی، نگرش و گرایش‌های افراد، قدرت اثرگذاری هنگفتی دارند. این جهت‌دهی فکری، نوعی از یک کنترل نرم می‌باشد که نهایتاً کنترل در عمل را در پی خواهد داشت. در سیستم اعتبار اجتماعی چین نیز رسانه در جلب اعتماد افکار عمومی نقش پررنگی داشته است. بررسی محققان از شبکه‌های خبری چینی و ارتباطات عمومی و همچنین پست‌های رسانه‌های اجتماعی در وبلاگ‌ها، انجمن‌ها و خدمات تابلوی اعلانات چین در مورد این سیستم اعتباری برای یک دوره‌ی شش ماهه در سال ۲۰۱۷ این نتیجه را در پی داشت که اکثر مقالات خبری دارای تمرکز مثبت هستند و این سیستم را به عنوان «درمان همه‌ی مشکلات اجتماعی و اقتصادی» برجسته می‌کنند [۳۴]. این خود مدعی نقش تأثیرگذار رسانه در دیدگاه افکار عمومی است که موجب پذیرش این نوع سیستم از سوی شهروندان چینی شده است.

همان‌طور که مطرح شد در این سیستم، برخی از افراد نه به دلیل اقدامی که انجام داده‌اند، بلکه به دلیل ارتباط با شخصی که رفتار «اعتمادشکنی» انجام داده است، مشمول کاهش اعتبار می‌شوند. در این صورت اگر افراد شروع به گزارش رفتار دیگران کنند تا امتیاز خود را بالا نگه دارند، می‌تواند منجر به ازهم‌پاشیدگی جامعه شود [۳۵]. این موضوع، پدیده‌ی محاکمه توسط رسانه‌ها را آسان‌تر می‌کند که به عنوان فرآیندی پویا برای رسانه‌های خبری افراد در دادگاه افکار عمومی محاکمه و محکوم می‌شوند [۳۶]. در این وضعیت، رسانه‌ها نه تنها به عنوان نماینده‌ی افکار عمومی عمل می‌کنند، بلکه نقش دادستان، قاضی و هیأت منصفه را برای پرچسب‌زدن و شرم‌ساری فرد مورد هدف که از سوی دیگر تقریباً بی‌دفاع است را بر عهده می‌گیرند [۳۷].

از طرفی حقوق مسلم هر فرد عبارتند از:

۱. تحقق عدالت و عدم تبعیض

۲. حق آزادی بیان و عمل



### ۳. حق آزادی در نقل و انتقال

#### ۴. حفاظت در برابر دخالت در حیطه حریم خصوصی

محدودیت این حقوق تنها زمانی مجاز است که برای احترام به حقوق دیگران، حفاظت از امنیت ملی یا نظم عمومی لازم باشد [۳۸]. با در نظر گرفتن این حقوق جهانی، نگرانی‌های زیادی در مورد سیستم اعتبار اجتماعی چین مطرح شده است [۲۸، ۳۹] که در این بخش به این موضوعات در سیستم اعتبار اجتماعی می‌پردازیم.

### ۲.۲ تحقق عدالت و عدم تبعیض

تحقق عدالت در این است که هر صاحب حقی به حق خود برسد و در امور اجتماعی در جای شایسته‌ی خود قرار گیرد. در همه‌ی مسائل تضمین در برابر تبعیض، مستلزم این است که با همه‌ی مردم به‌طور یکسان رفتار شود و حق حفاظت برابر از قانون را داشته باشند [۳۸].

در حالی که در گذشته‌ی کشور چین، مجرمان توسط یک نهاد ناظر مانند دادگاه مورد محاکمه قرار می‌گرفتند، اکنون با مجموعه‌ای از مجازات‌ها مواجه هستند که مشترکاً تحت نظر چندین نهاد و اغلب از طریق سیستم‌های هوش مصنوعی اعمال می‌شوند. یکی از بزرگ‌ترین مشکلات این سیستم در حوزه عدالت، اعمال تحریم‌ها بدون هیچ‌گونه فرآیند قضایی است [۴۰]. این نوع از سیستم‌های هوشمند به جهت ذات خطاپذیر خود می‌تواند منجر به خطا در تشخیص اشخاص و اعمال مجازات ناحق شوند، همچنین زمانی که یک نام به لیست سیاه اضافه می‌شود، حذف آن نیز چالش‌برانگیز است حتی اگر برخی مقررات مربوط به حذف، دوره‌ی زمانی مشخص داشته باشند [۲۸، ۲۳، ۱۰]. از منظر محققان، از آنجایی که هیچ فرآیند درستی وجود ندارد که توسط آن افراد از تخلف احتمالی مطلع شوند و فرصتی برای پاسخگویی داشته باشند، عدالت سیستم کاملاً زیر سوال می‌رود [۲۳، ۴۱، ۴۲].

طبق یک سیاست ملی که در اواخر سال ۲۰۱۹ صادر شد، شهروندان می‌توانند اقداماتی را برای ترمیم اعتبار خود انجام دهند؛ مانند اصلاح «رفتار نادرست»، ارائه «خدمات رایگان» و شرکت در «فعالیت‌های خیریه». این رفتارها می‌توانند تا حدی آسیب‌های ناشی از قانون‌شکنی یا انواع دیگر رفتارهای نادرست را جبران کنند. با این وجود این روش می‌تواند نابرابری‌های اجتماعی نیز ایجاد کند؛ زیرا افرادی که دارای سرمایه‌ی بیشتری هستند، بهتر می‌توانند در فعالیت‌های خیریه شرکت کنند و در نتیجه کم‌تر در لیست سیاه قرار می‌گیرند و به امتیازات اعتبار اجتماعی بالاتری دست می‌یابند [۴۳] که این موضوع خود منجر به ایجاد طبقات اجتماعی در جامعه و در نهایت جامعه‌ای کاپیتالیستی<sup>۱۲</sup> خواهد شد.

همچنین از معایب دیگر، سنتی بودن برخی سیستم‌هاست که در جهت عدم تحقق عدالت حرکت کرده و حتی می‌تواند منجر به ایجاد فساد بیشتر شود؛ به‌عنوان نمونه، رسانه‌ها درباره سیستمی که در شهر جیاکوانگ ماجیا<sup>۱۳</sup> طراحی شده است، گزارش می‌دهند که یک نفر مسئول رتبه‌بندی همه شهروندان است. یعنی این

<sup>12</sup>Capitalism

<sup>13</sup>Jia kuang Majia

فرد مسئول ثبت دستی رفتارهای «خوب» یا «بد» افراد و اختصاص امتیاز به آنها است. بنابراین در این شرایط شهروندان به صورت دستی ارزیابی می‌شوند. شرح رسانه ادعا می‌کند که برای مثال، یک شهروند که هشت ساعت را به تعمیر یک سبد در زمین بسکتبال پرداخت، ۲ امتیاز دریافت کرده است؛ در حالی که دو شهروند با سپری کردن زمان خود در ارتش، هر کدام ۱۰ امتیاز دریافت کردند و همچنین شهروندی با اهدای ۳۰۰۰ یوان به یک مؤسسه خیریه ۳۰ امتیاز دریافت کرد. منطق پشت اعطای این امتیازها، به‌ویژه از نظر نسبت دادن مقادیر عددی به رفتارهای فردی، نسبتاً نامشخص و خودسرانه به نظر می‌رسد [۱۹] که در این نمونه، اهدای یکباره‌ی هزینه به مؤسسه خیریه سه برابر مهم‌تر از خدمت سربازی شناخته شد.

پژوهشگران معتقدند که از جمله مشکلات دیگر عدم تحقق عدالت این موضوع است که افراد کم‌اعتبار در این سیستم که مشمول مجازاتی مانند عدم تهیه بلیط قطارهای سریع‌السیر می‌شوند، نه تنها شامل کسانی می‌شود که از پرداخت بدهی‌های معوقه خودداری کرده‌اند، بلکه شامل افرادی می‌شود که قراردادهای خدماتی را نقض کرده‌اند و همچنین افرادی که به دلیل استعمال دخانیات در واگن‌های راه‌آهن مجازات شده‌اند [۴۴]. اینکه آیا افرادی که این سه تخلف را مرتکب شده‌اند، دارای همان درجه مجازات هستند یا عواقب جدی مشابهی دارند جای سؤال دارد! بنابراین نمی‌توان از روی برچسب عدم اعتماد علت قصور را تعیین کرد؛ چه زمانی که ناشی از مشکلات اقتصادی یا اجتماعی، سیاسی یا فرهنگی، سهوی یا عمدی و سایر شرایط باشد [۴۳].

مجازات‌های ترکیبی در این سیستم، مجازات‌هایی هستند که نه تنها اختیار و عمل خود فرد را محدود می‌کنند، بلکه بر خانواده و اطرافیان هم تأثیر می‌گذارند؛ به‌عنوان مثال فرزندان اشخاص کم‌اعتبار، از تحصیل در مدارس خصوصی منع شدند [۴۵] با توجه به اینکه هیچ فرزندی خانواده‌اش را خود انتخاب نکرده است، اگر فرزندی والدین ناشایستی داشته باشد، موجب سلب آزادی او از امکانات و در نتیجه رشد و پیشرفت او در چنین جامعه‌ای خواهد شد که خود از تحقق عدالت به دور است. اگرچه مقامات چین سعی می‌کنند این مجازات را به منظور جلوگیری از فرار بدهی توجیه کنند؛ اما نمی‌توانند تأثیر این رفتار را در تضييع حق اساسی کودکان یعنی آموزش نادیده بگیرند [۴۶].

## ۳.۲ حق آزادی بیان و عمل

آزادی بیان تضمین می‌کند که هر کسی حق دارد بدون مداخله، نظرات خود را بیان کند و ممکن است از طریق هر رسانه‌ای به انتخاب خود به دنبال دریافت و انتقال اطلاعات از هر نوعی باشد [۳۸] و آزادی عمل نیز بیان می‌کند هر انسانی اختیار عمل در رفتار و سرنوشت خود دارد.

یکی از مشکلاتی که از منظر محققان در این سیستم بررسی شد عدم آزادی بیان و عمل در مواردی مثل مغولستان داخلی<sup>۱۴</sup> است. والدینی که فرزندان خود را با برنامه‌ی درسی اجباری آموزش زبان ماندالین از مدارس خارج می‌کردند، با تهدید در لیست سیاه مواجه شدند<sup>۱۵</sup> [۴۷].

<sup>۱۴</sup> منطقه شمالی چین که از سوی شمال با مغولستان و روسیه هم‌مرز است.  
<sup>۱۵</sup> به قسمتی از مواردی که مربوط به سلب آزادی در این سیستم است در بخش‌های قبلی اشاره شد و به سایر موارد این حوزه نیز در ادامه بیشتر می‌پردازیم.

## ۴.۲ حق آزادی در نقل و انتقال

حق آزادی در نقل و انتقال بیان می کند که همه‌ی مردم باید این آزادی را داشته باشند که در کشور خود حرکت کنند و محل سکونت خود را انتخاب کنند. علاوه بر این، همه‌ی مردم باید اجازه خروج از هر کشوری از جمله کشور خودشان را داشته باشند [۳۸].

یکی از جریمه‌هایی که در این سیستم بیشتر گزارش شده است، ممنوعیت استفاده افراد با اعتبار اجتماعی پایین از نوع خاصی از وسایل حمل و نقل عمومی مانند پروازها یا قطارهای سریع‌السیر است. بر اساس داده‌های دادگاه عالی خلق، دادگاه‌های چین در مجموع ۱۲/۱۱ میلیون نفر را به دلیل سلب اعتماد و کاهش اعتبار مجرم شناخته‌اند. حدود ۱۴/۶ میلیون مسافر از خرید بلیط هواپیما و ۵/۲ میلیون مسافر از خرید بلیط قطار سریع‌السیر منع شده‌اند. نکته قابل توجه این که مجازات‌های مربوط به این حوزه، صرفاً در حمل و نقل محدود نمی‌شود [۴۹]. بنابراین محدودیت سفر یک فرد برای مواردی که معمولاً تخلف جزایی یا جزئی مدنی محسوب می‌شود، به آزادی رفت و آمد فرد تجاوز می‌کند [۱۲].

مشکل اصلی در این نوع برخورد زمانی تشدید می‌شود که مجازات‌های اعمال‌شده‌ی این سیستم، با تخلف انجام‌شده متناسب نباشد [۲۸، ۴۸، ۵۰، ۴۱]. یعنی فرد مورد نظر در اثر عبور از چراغ راهنمایی، محدودیتی در خرید بلیط هواپیما و یا در اثر استعمال دخانیات در واگن‌های راه‌آهن محدودیتی در خرید املاک برای آن اعمال می‌شود. در برخی موارد، پیامدها می‌توانند گسترده باشند و به طور موجهی با تخلف اصلی مرتبط نیستند [۴۱، ۲۸، ۵۰].

بنابراین، این مجازات منجر به ضرر مادی و اعتباری شدیدی برای افراد، شرکت‌ها و سازمان‌ها می‌شود که در خدمت هدف سیستم اعتبار اجتماعی یعنی «دشواری در برداشتن حتی یک قدم برای افراد بی‌اعتبار» است [۵۱].

## ۵.۲ حفاظت در حیطه حریم خصوصی

حفاظت در برابر مداخله حریم خصوصی مشخص می‌کند که هر کسی حق حفاظت از قانون در برابر چنین مداخله‌ای را دارد [۳۸، ۵۲]. امروزه توجه زیادی به حریم خصوصی شخصی و امنیت اطلاعات معطوف شده است. همان‌طور که بحث شد، فناوری‌های کلان‌داده جمع‌آوری اطلاعات شخصی دقیق را بدون اطلاع افراد امکان‌پذیر می‌سازد و این داده‌ها می‌توانند برای اهداف امنیتی یا سیاسی مورد استفاده قرار گیرند [۵۳]. بنابراین جنبه اصلی از این سیستم که نگرانی‌های مربوط به حریم خصوصی را افزایش می‌دهد، این است که رضایت در جمع‌آوری اطلاعات مورد نیاز نیست [۱۲]. همچنین در این سیستم اعتبار اجتماعی با تجمیع داده‌های مختلف، اطلاعات شخصی و حریم خصوصی ممکن است افشا شود [۱۰]. این در حالی است که روزنامه‌نگاران فاش کرده‌اند که دستیابی به اطلاعات شخصی و حریم خصوصی در چین به طرز شگفت‌آوری آسان است. بنابراین، در شرایطی که مشخص نیست شرکت‌ها و دولت چگونه داده‌ها را با یکدیگر به اشتراک می‌گذارند، نگرانی‌های خود را در مورد خطرات مربوط به امنیت داده‌ها ابراز کرده‌اند [۵۴].

یک مسئله کلیدی در تحول این است که دادگاه‌ها باید بین منافع عمومی در دسترس (امکانات) و حفظ

حریم خصوصی در انتشار اطلاعات تعادل برقرار کنند. بر اساس احکام دادگاه چین در مورد نشر اطلاعات در اینترنت توسط دادگاه‌های مردمی، اطلاعات شخصی شامل آدرس منزل، اطلاعات تماس، شماره شناسنامه، شماره حساب بانکی، وضعیت سلامت، شماره پلاک خودرو و شماره گواهی اموال منقول و غیرمنقول، باید از اسناد حذف شود (دادگاه عالی خلق جمهوری خلق چین ۲۰۱۶). با این حال، هنوز لیست‌های سیاه زیادی وجود دارد که توسط دادگاه‌های محلی منتشر شده‌اند که اطلاعات شخصی مذکور را افشا می‌کنند و نگرانی‌های قابل توجهی را در مورد حفظ حریم خصوصی ایجاد می‌کنند. یکی از اهداف رهبران چینی از افشای اطلاعات این است که فرد مجرم احساس شرم کند و از رفتار خود خجالت زده و در پی جبران آن باشد که در بعد اجتماعی بیشتر به آن می‌پردازیم. از سوی دیگر، نظر پژوهشگران در مورد احساس شرم این است که ناشناس‌سازی اطلاعات شخصی و محدودیت در گسترش لیست سیاه در سیستم اعتبار اجتماعی قدرت شرم را کاهش می‌دهد. اگر مردم قادر به شناسایی افراد در لیست سیاه نباشند، راهبرد شرم به طور مؤثر کار نمی‌کند. از طرفی در چین رایج است که افراد دارای نام‌های مشابهی هستند. بنابراین در بسیاری از موارد، اگر اطلاعات بیشتری ارائه نشود، مشخص نیست که نامی که در لیست سیاه قرار گرفته به چه کسی اشاره دارد. در واقع، چندین گزارش خبری تاکید کرده‌اند که افراد با همین مشکل تحت تأثیر هویت اشتباه قرار گرفتند. به این ترتیب، لیست‌های سیاه سیستم اعتبار اجتماعی با معضلی بین حفاظت از حریم خصوصی و اثربخشی شرم‌نامه‌سازی مواجه هستند [۸۸].

بنابراین شیوهی انتشار اطلاعات افرادی که در لیست‌های سیاه قرار گرفتند، عامل کلیدی نقض اصل انتقال اطلاعات محرمانه است [۵۵]. برخی از محققان معتقدند یک سیستم اعتبار اجتماعی که رفتار انسان‌ها را قضاوت می‌کند و رتبه‌بندی را منتشر می‌کند، ظالمانه و تجاوز بزرگ به حریم خصوصی به نظر می‌رسد [۱۲].

## ۳ اقتصادی

انگیزه‌ی اولیه از ایجاد یک سیستم اعتباری، به اوایل دهه‌ی ۱۹۹۰ در چین به رفع مشکلات اقتصادی بر می‌گردد، جایی که شرکت‌ها و افراد با عدم پرداخت بدهی‌ها و وام‌های دریافتی به یکدیگر و دولت بدهکار شدند؛ لذا در شانزدهمین کنگره‌ی حزب در سال ۲۰۰۲، رئیس‌جمهور جیانگ زمین تاکید کرد که چین باید یک سیستم اعتبار اجتماعی سازگار با اقتصاد بازار مدرن ایجاد کند [۵۶].

حزب کمونیست چین با توجه به کاهش اعتماد عمومی در معاملات، در پی ایجاد یک سیستم اعتباری اجتماعی مبتنی بر قوانین درآمد تا اعتماد را در جامعه تقویت کند و به نوبه خود اعتماد رسمی قوی‌تری به نهادها ببخشد. از دیدگاه برخی صاحب‌نظران در این نوع سیستم، هزینه‌های مبادله در بخش تجاری کاهش می‌یابد؛ زیرا در این صورت خطر تعامل با افراد کم‌اعتبار تقلیل می‌یابد. به این ترتیب، معاملات کارآمدتر می‌شوند که این باعث رشد بیشتر اقتصادی خواهد شد؛ اما نقدی که بر این موضوع وارد می‌شود، در این است که اگر شخصی بر اثر شرکت در امور غیرمالی اعتبار اجتماعی کسب کرده باشد، چه تضمینی وجود دارد که در معاملات نیز این شخص دارای اعتبار بالایی خواهد بود؟ به‌عنوان نمونه، فردی که در اثر اهدای خون یا شرکت در امور خیریه امتیاز خود را افزایش داده، چه تضمینی وجود دارد که در معامله فرد معتبری باشد؟

در بعد اعتبار شرکت‌ها و سازمان‌ها برخی معتقدند هدف سیستم اعتبار اجتماعی افزایش اعتماد در رابطه بین کسب‌وکار و همچنین روابط با سایر ذینفعان مرتبط (مانند سرمایه‌گذاران) از دو طریق است. اولاً، شفافیت اطلاعات، ریسک ذاتی در انتخاب شرکای تجاری را کاهش می‌دهد. ثانیاً مجازات‌ها و پاداش‌های مشترک با افزایش هزینه‌های عدم انطباق نه‌تنها خود کسب‌وکار، بلکه اعتبار شرکت‌های وابسته را نیز تحت تأثیر قرار می‌دهد. این امر به‌ویژه آنجایی نمود پیدا می‌کند که ارتباط تفاهم‌نامه بین مجازات‌ها و پاداش‌ها بین بخش‌ها و کنش‌گران منجر به عواقب شدیدتری برای شرکت‌ها می‌شود. به‌عنوان مثال، برای مناقصه‌های دولتی، یک معیار انتخاب، نه تنها انطباق با عملکرد شرکت اصلی، بلکه شرکای تجاری آن نیز می‌باشد (این که آن‌ها در فهرست سیاه باشند در ارزیابی شما هم تأثیر منفی می‌گذارد). [۵۷].

همچنین هنگامی که نهادهای شرکتی به‌دلیل قصور در قوانین در لیست سیاه قرار می‌گیرند، علاوه بر این که سازمان مشمول تحریم‌ها و رد صلاحیت‌ها می‌شود، مالکان و مدیران اجرایی نیز با محدودیت‌هایی در هزینه‌ی سفر، تعطیلات و ثبت نام در مدرسه فرزندان‌شان مواجه می‌شوند [۷، ۳۵]. به‌عبارتی اگر شرکتی به‌دلیل عدم اعتماد در لیست سیاه قرار گیرد، نهاد و افرادی مانند: خود شرکت، نمایندگان حقوقی شرکت، افرادی که مستقیماً مسئول این تخلف هستند، می‌توانند مجازات شوند [۵۹].

## ۴ اجتماعی

ظهور انبوهی از پلتفرم‌های دیجیتال در ارتباط با پیشرفت‌های محاسباتی که ظرفیت ذخیره‌سازی داده‌های بسیار زیادی را امکان‌پذیر می‌سازد، جامعه‌ای را به وجود می‌آورد که در آن بسیاری از جنبه‌های رفتار و زندگی انسان به‌صورت کمی اندازه‌گیری می‌شوند و قضاوت انسان با مدل‌های الگوریتمی جایگزین می‌شود [۶۰، ۵۸]. سیستم اعتبار اجتماعی نمونه‌ای از این پلتفرم است که در این بخش به این موضوع از دیدگاه اجتماعی می‌پردازیم.

### ۱.۴ شخصیت اجتماعی

اعتماد در محیط‌های بازار و کسب و کار اغلب حساب‌شده و شاید به‌حق باشد؛ زیرا معاملات در این زمینه به‌شدت حساس و سودمند هستند؛ در حالی که اعتماد در تعاملات اجتماعی گسترده‌تر و رابطه‌ای است؛ زیرا هنگامی که باورهای قوی در مورد حسن نیت، صداقت، تلاش‌های خیرخواهانه دیگران وجود دارد، روابط اجتماعی محکم‌تر می‌شوند [۸۹]. از منظر پژوهشگران «اخلاق را نمی‌توان به دولت یا بازار سپرد؛ بلکه باید از طریق یک جامعه مدنی قوی پرورش داد [۶۱].»

همچنین یکی از چالش‌ها تحت منطق کمی‌سازی - محاسبه عددگونه - شخصیت افراد مرموز و غیرقابل کنترل قابل ارزیابی نیست و به‌عنوان جلوه‌های قابل محاسبه عقلانیت<sup>۱۶</sup> (علمی) ظاهر می‌شوند؛ لذا یکی از مشکلات اساسی این سیستم ارزیابی اعمال کیفی افراد به‌صورت کمی است [۶۲]. این توجه نشان‌دهنده‌ی یک فرآیند کلی از اقتصادی‌شدن جامعه است که در آن منطق‌های اقتصادی وارد حوزه‌های غیراقتصادی

<sup>16</sup>rationality

می‌شوند [۶۳].

همان‌طور که پیش‌تر نیز ذکر شد، طبق یک سیاست ملی که در اواخر سال ۲۰۱۹ صادر شد، شهروندان می‌توانند اقداماتی را برای ترمیم اعتبار خود انجام دهند؛ مانند اصلاح «رفتار نادرست»، ارائه «خدمات رایگان» و شرکت در «فعالیت‌های خیریه». مضاف بر این موضوع که رفتار ترمیمی مطرح‌شده، ارتباط کمی با رفتار اعتمادساز دارد، می‌تواند اعتماد مردم به فرد مورد نظر را به طور کامل از بین ببرد [۴۳]؛ زیرا زمانی که فردی اعتبارش در میان مردم از بین برود به سختی می‌تواند مجدداً منزلت قبلی خود را کسب کند. سیستم‌های امتیازدهی به‌جای توانمندسازی افراد برای ایجاد و تمرین اعتماد، آن‌ها را برای کسب امتیاز بیشتر تشویق می‌کنند. در این سیستم، افراد تنها به هر روشی برای افزایش امتیازدهی تلاش می‌کنند تا متغیرهای ورودی را با خروجی مورد انتظار هماهنگ کنند؛ چه این روش‌ها از نظر اخلاقی خوب باشند و چه نامربوط باشند. در این صورت افراد دیگر نیازی به تعامل با دیگران برای اثبات قابل اعتماد بودن و کیفیت روابط اعتماد ندارند؛ بلکه آن‌ها مجبور می‌شوند برای نظارت بر وضعیت خود، بیشتر با الگوریتم‌ها تعامل کنند. این انتقال ارزیابی از عقل انسانی به عقلانیت الگوریتمی، تجلی معاصر عقل ابزاری صوری است؛ نوعی از عقلانیت که تنها مربوط به هماهنگی ابزارهای مؤثر با مقاصد عقلانی است [۶۵]. همچنین در ارتباط با نکته اخیر، مفهوم بازی‌سازی اعتبار اجتماعی نیز از دیدگاه غیرتجربی توسط سایر محققان مورد بحث قرار می‌گیرد [۶۶]. نکته پراهمیت دیگر این است که با توجه به وابسته‌شدن شهروندان به اعتباردهی دولت در ازای اعمالی من جمله اخلاقی، ارزش عمل در امتیاز آن نمایان می‌شود و نه در ارزش واقعی عمل؛ در این صورت اگر به‌ازای یک عمل اخلاقی، مردم اعتباری دریافت نکنند یا اعتبار پایینی دریافت کنند، ممکن است آن عمل را کنار بگذارند. در این شرایط علاوه بر شرطی شدن جامعه، ارزش واقعی عمل به خودی خود از بین می‌رود.

## ۲.۴ ساختار برچسب و شرم

در دیدگاه پژوهشگران، شرم به‌عنوان نوعی کنترل اجتماعی غیررسمی شناسایی و با شواهد تجربی نشان داده می‌شود که مجازات شدیدتری است و تأثیر قوی‌تری بر افراد نسبت به تحریم‌های رسمی توسط پلیس و قانون دارد [۶۴، ۶۷]. از نظر محققان شرم سه کارکرد عمده را داراست:

۱. به‌عنوان ابزاری برای کنترل اجتماعی که تلاش می‌کند رفتارهای پرخطرانه یا نامطلوب را سرکوب کند.
۲. به‌عنوان فشاری که انسجام اجتماعی را در جامعه از طریق طرد و ایجاد فاصله اجتماعی بین اعضای منحرف و گروه حفظ می‌کند.
۳. و به‌عنوان ابزاری مهم برای تسلط بر دیگران و دستکاری موقعیت اجتماعی آنها [۶۸].

تئوری برچسب‌گذاری به دنبال این است که «نشان دهد که چگونه هنجارها و انتظارات اجتماعی پیرامون یک برچسب به ساختن هویت برچسب‌خورده کمک می‌کنند [۶۹]» همچنین هدف رهبران چینی نیز از انتشار اطلاعات مجرمین این است که با توجه به این عمل احساس شرم کرده در پی جبران آن باشند.



با این تعریف، افکار عمومی بر رفتار افراد تأثیر می‌گذارد؛ در این شرایط ممکن است موجب طرد شدن افراد از سوی دیگران (به‌عنوان مثال، از یک گروه) شود. به‌عبارت دیگر، شرم نتیجه تهدیدی برای پیوند اجتماعی است و با احساس هویت فردی و شخصی مرتبط است [۷۰]. حتی این نوع رفتار برخلاف هدف مذکور می‌تواند اعتماد مردم به فرد مورد نظر را به‌طور واقعی از بین ببرد. این برچسب‌ها، به‌ویژه برچسب‌های منفی، می‌توانند گروه‌ها را از طریق ایجاد کلیشه‌های منفی قوی از بین ببرند و بنابراین می‌توانند ابزاری قدرتمند برای اعمال کنترل اجتماعی و ابزاری برای دستکاری هویت‌ها باشند [۷۱].

از جمله فعالیت‌هایی که سیستم اعتبار اجتماعی چین در این راستا انجام می‌دهد، می‌توان به‌عنوان نمونه به شهرهای مختلف، مانند ژنگزو<sup>۱۷</sup> یا دانگ‌فنگ<sup>۱۸</sup> اشاره کرد که به‌هنگام تماس با فردی در لیست سیاه، پیام صوتی پخش می‌شود تا به‌گیرنده‌ی تماس اطلاع دهد فرد مورد نظر در لیست سیاه قرار دارد و مجرم قانونی است [۷۲، ۷۳].

همچنین افراد متخلفی که در لیست سیاه قرار گرفته‌اند اطلاعات و تصویرشان بر روی صفحات نمایش (LED) بزرگ در ایستگاه‌های قطار یا در نمای بیرونی ساختمان‌ها در معرض عموم به‌جهت شرم‌نامه‌سازی قرار می‌گیرد که شکل ۱ نمایانگر این موضوع است.



شکل ۱: نمایش تصویر متخلفان بر روی صفحه نمایش‌های شهری

به این ترتیب، فرایندهای برچسب‌گذاری ممکن است اشکال جدید نابرابری را بیش از پیش تقویت کرده و روابط قدرت نابرابر موجود را حفظ کنند [۹۰]. پیامدهای برچسب‌گذاری به سه طریق اصلی با عدم توازن قدرت در فرآیندهای برچسب‌گذاری مرتبط هستند:

آ) به‌دلیل فاصله بین برچسب‌گذار و برچسب‌گیرنده، برچسب‌گذاری (به‌طور خاص برچسب‌گذاری

<sup>17</sup>Chinese : 鄭州 English: Zhengzhou

<sup>18</sup>Chinese: 登封; English: Dongfeng

بوروکراتیک) ممکن است منجر به عدم پاسخگویی نه تنها برای چگونگی طبقه‌بندی، بلکه برای نتایج این طبقه‌بندی شود [۷۴].

ب) فرآیندهای برچسب‌گذاری که انگیزه‌های متنوعی را در پی دارد، منجر به نتایج متفاوتی از جمله نتایج پیش‌بینی نشده و معمولاً منفی می‌شوند.

شواهد فراوانی وجود دارند که نشان می‌دهند برچسب‌ها می‌توانند باعث تبعیض و انگ‌زدن به افراد شوند و حتی بر روابط اجتماعی نزدیک، مانند بین اعضای خانواده و درون جوامع تأثیر بگذارند [۷۵].

ج) فرآیندهای برچسب‌گذاری بوروکراتیک ممکن است به سادگی تفاوت‌های میان آن‌هایی که برچسب یکسانی دارند را نادیده بگیرند [۷۶]. به عنوان مثال، در شرایط قصور مالی، شرکت‌هایی که موفق به پرداخت جریمه‌های کوچک نشده‌اند (در یک مورد تنها ۶۰۰ یوان) خود را در همان لیست سیاه شرکت‌هایی که در بازپرداخت وام‌های میلیاردی قصور کرده‌اند، یافته‌اند [۷۷].

## ۵ ابعاد فنی

افزایش دسترسی به ابزارهای تکنولوژیک، قابلیت‌های جمع‌آوری و ارزیابی داده‌های چین را به شدت افزایش داده و اینترنت را به نوعی سرویس اطلاعات دیجیتال خصوصی تبدیل کرده است. در این بخش به نحوه پیاده‌سازی این سیستم و مشکل عدم یکپارچه‌سازی آن می‌پردازیم.

### ۱.۵ پیاده‌سازی

چین به نظارت شدید دولتی شهروندان با استفاده از روش‌هایی مانند دوربین مداربسته، سنسور اینترنتی و تجزیه و تحلیل کلان داده شهرت دارد [۷۸]. معروف‌ترین ابزار نظارتی در اختیار دولت، شبکه ۶۲۶ میلیون دوربین است که به دولت در تشخیص چهره به منظور شناسایی و ردیابی افراد کمک می‌کند [۷۹]. شکل ۲ نمایی از این شبکه دوربینی را نشان می‌دهد.



شکل ۲: نمایی از شبکه دوربینی سیستم اعتبار اجتماعی در چین

در حال حاضر چندین شهر در چین از فناوری‌های تشخیص چهره برای ردیابی و شناسایی مجرمانی مانند کسانی که از وسط خیابان عبور می‌کنند استفاده و بلافاصله نام آنها را در رسانه‌های محلی منتشر می‌کنند [۸۰، ۹۲]. این فناوری‌های تشخیص چهره در حال حاضر در فرودگاه‌ها و بانک‌ها و بسیاری از اماکن دیگر برای تایید هویت و همچنین اجازه دسترسی به مکان‌هایی مانند هتل‌ها و اقامتگاه‌ها مورد استفاده قرار می‌گیرند [۷۸]. این فناوری حتی برای جرایم جزئی پلیس مانند سرقت دستمال توالت از دستشویی‌های عمومی با محدود کردن میزان دستمال توالتی که می‌توان برداشت کرد نیز مورد استفاده قرار می‌گیرد [۸۱، ۹۳]. علاوه بر این، فناوری تشخیص چهره به‌طور گسترده در چین برای موارد مختلف از دسترسی به سیستم مترو گرفته تا تعیین صلاحیت برای خدمات آنلاین تلفن همراه استفاده می‌شود [۸۲].

از طرفی به‌منظور اعتبار بخشی و اجرای سیستم اعتبار اجتماعی، اولین قدم این است که اطمینان حاصل شود که همه - افراد و سازمان‌ها - قابل شناسایی باشند [۸۳]. برای انجام این کار، کدیکتایی به نام «کد اعتبار اجتماعی یک شکل»<sup>۱۹</sup> ایجاد شد که شناسه‌های منحصر به فرد و سیستم‌های ثبت نام‌های حقیقی را برای پلتفرم‌های دیجیتال فراهم می‌کند تا دولت بتواند داده‌ها را به افراد و مشاغل مرتبط کند، در کنار استفاده از الگوریتم‌های تشخیص افراد، یک مشکل بالقوه این سیستم استفاده از الگوریتم‌های پیش‌بینی‌کننده به‌عنوان روشی برای سیاست‌گذاری است [۱۲]. در حالی که الگوریتم‌ها می‌توانند در حدس زدن شخصیت و رفتار افراد مفید باشند، می‌توانند برای نظارت انتخابی و نمایه‌سازی گروه‌ها، حتی زمانی که هیچ جرمی مرتکب نشده‌اند، استفاده شوند [۸۴، ۴۲]. این به نگرانی اساسی بر می‌گردد که سیستم اعتبار اجتماعی فقط به‌عنوان ابزار دیگری برای سرکوب استفاده می‌شود تا برنامه‌ای که به‌طور مؤثر جامعه را بهبود بخشد [۲۳، ۴۲].

برخی پژوهشگران معتقدند که سیستم اعتبار اجتماعی ظریف‌تر از ابزارهای نظارت سنتی است زیرا اهداف سیاسی را با الگوریتم‌ها ترکیب می‌کند [۸۴]. چندی از محققان برای این سیستم از تعبیر «حکومت الگوریتمی»<sup>۲۰</sup> یاد کردند [۶۵]. از دیگر چالش‌های این سیستم در پیاده‌سازی این است که بخش بزرگی از جمعیت چین همچنان از نظر دیجیتالی محروم هستند و امکان جمع‌آوری داده‌های مربوط به رفتار آنها با استفاده از فناوری‌های مدرن محدود است [۱۹].

## ۲.۵ عدم یکپارچگی

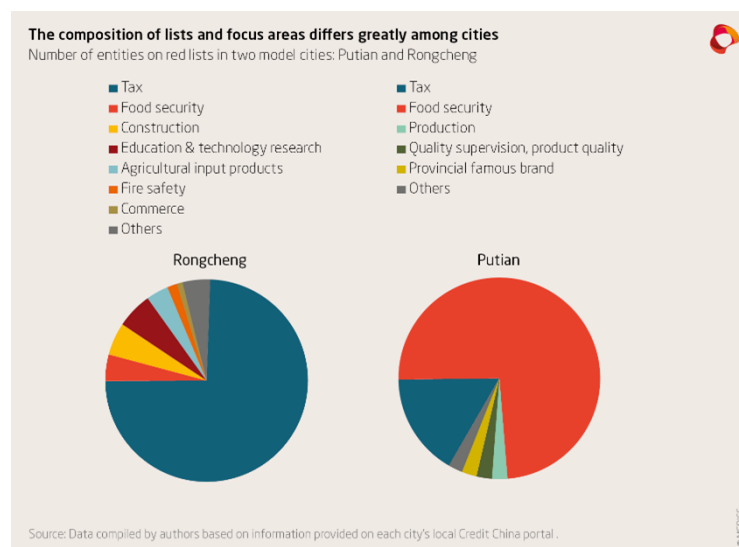
پوشش رسانه‌ای بین‌المللی که اغلب بر سال ۲۰۲۰ به‌عنوان تاریخ پایان طرح سیستم اعتبار اجتماعی از سال ۲۰۱۴ متمرکز شده بود این تصور را ایجاد می‌کرد که این سیستم به‌عنوان یک سیستم یکپارچه تا سال مذکور وارد عمل می‌شود. با وجود این واقعیت که برخی از مکانیزم‌های کلیدی آن سال‌ها است که وجود دارند، این سیستم اعتباری امروز یک سیستم یکپارچه و استاندارد نیست. آنچه امروز ایجاد شده است را می‌توان به بهترین شکل به‌عنوان یک چارچوب سیاست توصیف کرد که شامل تعداد زیادی از ابتکارات، یا به‌عنوان سیستمی از سیستم‌ها است [۱۷]. در حال حاضر، جمع‌آوری این داده‌ها و توسعه برنامه‌های آزمایشی بر عهده

<sup>19</sup>uniform social credit code

<sup>20</sup>algorithmic governmentality

دولت‌های محلی، عمدتاً در سطح شهرداری‌ها است. این فرآیند غیرمتمرکز است و نهادهای اداری مختلف بر اساس صلاحیت‌های خود بر حوزه‌های خاص تمرکز می‌کنند [۱۹].

یکی از مشکلات موجود در بعد فنی این است که هیچ نمره اعتباری واحدی وجود ندارد؛ بلکه پلتفرم‌های ملی و محلی از سیستم‌های ارزیابی یا رتبه‌بندی متفاوتی استفاده می‌کنند [۵۹]. به‌عنوان مثال، در شهر سوژو<sup>۲۱</sup>، سیستم اعتباری<sup>۲۲</sup> افراد را به‌صورت عددی در مقیاس ۰ تا ۲۰۰ طبقه‌بندی می‌کند، در حالی که در شهر سوشین<sup>۲۳</sup>، سیستم اعتباری<sup>۲۴</sup> رتبه‌بندی را از ۱۰۰۰ امتیاز شروع می‌کند و بسته به امتیاز، افراد به دسته‌هایی از A++ (بالاترین) تا D (پایین‌ترین) تقسیم می‌شوند [۸۵]. تفاوت‌هایی بین نسخه‌های محلی سیستم اعتبار اجتماعی وجود دارند که مشکل برابری در مقابل قانون را ایجاد می‌کنند [۸۶]. در واقع آنچه ممکن است منجر به لیست سیاه در یک شهر شود، ممکن است منجر به لیست سیاه در شهر دیگر نشود. شکل ۳ نشان می‌دهد که چگونه شهرها، فهرست‌های قرمز کاملاً متفاوتی را طراحی کرده و آنها را به‌طور متفاوتی اعمال می‌کنند. در سطح ملی نیز ۲۷ شهر آزمایشی در درجه اول به لیست‌های قرمز و سیاه دوتایی متکی هستند [۵۹]. از جمله مشکلات دیگر این است که امتیازها نیز بین شهرها به اشتراک گذاشته نمی‌شود زیرا هرکدام از آنها معیارها و مکانیسم‌های امتیازدهی متفاوتی استفاده می‌کنند؛ اگرچه برخی شهرها توافق‌نامه‌های تبدیلی امضا کرده‌اند [۸۷، ۹۴].



شکل ۳: لیست قرمزهای متفاوت دو شهر مختلف

<sup>21</sup> Suzhou  
<sup>22</sup> Osmanthus  
<sup>23</sup> Suqian  
<sup>24</sup> Xichu

## ۶ نتیجه گیری

سیستم اعتبار اجتماعی چین، سیستمی است که شهروندان را به جهت امتیازدهی به طور مداوم از جنبه‌های مختلف ارزیابی می‌کند و با استفاده از راهبرد تنبیه و پاداش و سپس اعمال محدودیت و دسترسی‌های متنوع، به طور خلاصه با استفاده از اهرم فشاری، به امکاناتی که قبل از این قابل دسترس همگان بود، محصور به دسترسی افرادی می‌کند که شاخص‌های همسو با دولت داشته باشند. این سیستم به جهت شالوده‌ی اصلی خود یعنی دانش سایبرنتیک امروزه مورد توجه کشورهای بیشتری قرار گرفته است؛ چرا که با این نوع سیستم شهروندان تحت حاکمیت دولت و آسان‌تر قابل کنترل هستند. بررسی منابع مختلفی که در این مقاله صورت گرفته است نشان می‌دهد که پیاده سازی چنین سیستمی با چالش‌های جدی اقتصادی، فرهنگی، اجتماعی، سیاسی، قانونی و فنی مواجه است و امکان ارائه این الگو برای همه کشورهای دنیا بدون در نظر گرفتن بافت فرهنگی و اجتماعی آنها چندان امکان پذیر نیست، بررسی جزئی‌تر این مطالب نیاز به پژوهش‌های عمیق‌تری دارد که در مقالات بعدی به آن پرداخته می‌شود.

## مراجع

- [1] Hurley, M., & Adebayo, J. (2017). Credit scoring in the era of big data. *Yale Journal of Law and Technology*, 18, 1-54. Retrieved from <http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1121&context=yjolt>.
- [2] Schneier, B. (2016, January 11). The risks –and benefits –of letting algorithms judge us. Retrieved from <https://edition.cnn.com/2016/01/06/opinions/schneier-china-social-scores/index.html>.
- [3] Redrup, Y. (2017, December 25). How email and smartphone data could help you get a loan. <http://www.afr.com/technology/how-email-and-smartphone-data-could-help-you-get-a-loan-20171202-h02zi0>.
- [4] Reisinger, D. (2015, December 1). Why Facebook profiles are replacing credit scores. Retrieved from <http://fortune.com/2015/12/01/tech-loans-credit-affirm-zest/>.
- [5] Jahberg, H. (2018, February 17). Germany edges toward Chinese-style rating of citizens. Retrieved from <https://global.handelsblatt.com/politics/germany-mass-surveillance-social-credit-china-big-data-710626>.
- [6] Han, J. (2014, July 27). “The Meaning and Extension of Social Credit System.” *China’s Reform Daily*. [http://www.crd.net.cn/2014-07/27/content\\_12105536.htm](http://www.crd.net.cn/2014-07/27/content_12105536.htm).
- [7] Xin Dai. (2020, January 15). Enforcing Law and Norms for Good Citizens: One View of China’s Social Credit System Project, 63:34–38. Retrieved from <https://doi.org/10.1047/s36301-020-00231-2>.
- [8] Lin, H. (2003). The Definition and Attributes of Credit and the Construction of China’s Credit System (Xinyong De Dingyi He Shuxing Yu Zhongguo Xinyong Zhidu Jianshe). *Fujian Finance* 10: 1–4.



- [9] Shi, X. (2007), “On Evolution of the Concept of Credit (Lun Xinyong Gainian De Lishi Yanjing).” Journal of Peking University 44 (6): 120–24.
- [10] Yongxi Chen & Anne Sy Cheung. (2017). The Transparent Self under Big Data Profiling: Privacy and Chinese Legislation on the Social Credit System, 12 J. COMP. L. 356, 322. (explaining the difference between government and commercial systems).
- [11] Alexandra Ma. (2018, Oct 28 ). China has started ranking citizens with a creepy ‘social credit’ system —here’s what you can do wrong, and the embarrassing, demeaning ways they can punish you, BUS. INSIDER , archived at <https://perma.cc/H9SZ-9700> (detailing how individuals placed on the blacklist for bad behavior are restricted in their daily lives).
- [12] Lizzy Rettinger. (2020). The Human Rights Implications of China’s Social Credit System, Journal of High Technology Law, Vol. XXI, No. 1.
- [13] Liu, Xiaoyuan [刘肖原]. (2016). On the Construction of the Social Credit System in China [我国社会信用体系建设研究]. Beijing: Intellectual Property Publishing House [知识产权出版社].
- [14] State Council Notice Clearing “Triangular Debts” across the Country. [http://www.gov.cn/zhengce/content/2010-12/17/content\\_2337.htm](http://www.gov.cn/zhengce/content/2010-12/17/content_2337.htm).
- [15] Liang, F., Das, V., & Kostyuk, N. (2018). Constructing a data-driven society: China’s social credit system as a state surveillance infrastructure. Policy & Internet, 10(4), 352–377.
- [16] State Council General Office. (2007). ”State Council General Office Some Opinions Concerning the Construction of a Social Credit System (Guowuyuan Bangongting Guanyu Shehui Xinyong Tixi Jianshe De Ruogan Yijian).” 1–3.[http://www.gov.cn/zwgk/2007-04/02/content\\_554314.htm](http://www.gov.cn/zwgk/2007-04/02/content_554314.htm).
- [17] [http://www.gov.cn/zfwj/2014-02/10/content\\_2411577.htm](http://www.gov.cn/zfwj/2014-02/10/content_2411577.htm).
- [18] State Council, The State Council Notice on Outline of Social Credit System Construction (2014-2020), 2014.
- [19] Alicja Bachulska. (2020, September). China’s social credit system and its development: between “Orwellian nightmare” and technocratic utopia?, Asia Research Centre Report.
- [20] Chen, Y.-J., Lin, C.-F. and Liu, H.-W. (2018). ‘“Rule of Trust” : The Power and Perils of China’s Social Credit Megaproject’ , Columbia Journal of Asian Law, 29(1), pp. 1–32.
- [21] Lee, Claire Seungeun. (2019, May 08). Datafication, dataveillance, and the social credit system as China’s new normal ,ONLINE INFORMATION REVIEW : THE INTERNATIONAL JOURNAL OF DIGITAL INFORMATION, RESEARCH AND USE, Vol. 38, Issue 6, pages 784 –795.
- [22] Vrinda Vinayak. (2020, April 19). The Human Rights Implications of China’s Social Credit System, OXFORD HUMAN RIGHTS HUB archived at <https://perma.cc/2A9Q-ZDEA>.



- [23] Xinyuan Wang. (2019, Dec. 19). Hundreds of Chinese citizens feel just fine about the controversial social credit system, PRI archived at <https://perma.cc/SKC2-42ZN>.
- [24] Hao, Jing. (2020). ”论行政法视域下正当程序对信用监管机制的规制 (On the Regulation of the Credit Supervision Mechanism from the Perspective of Administrative Law).” *Journal of Hebei Youth Administrative Cadres College* 29(5): 66–71.
- [25] The Asan Institute for Policy Studies ,Orwell’ s Nightmare: China’s Social Credit System. (2017) [Electronic resource]. <http://en.asaninst.org/contents/orwells-nightmare-chinas-socialcredit-system/> (accessed: 27.01.2020).
- [26] Orgad, Liav, and Wessel Reijers. (2020). “How to Make the Perfect Citizen? Lessons from China’s Model of Social Credit System.” *Social Science Research Network*. <https://doi.org/10.2135/ssrn.3467533>.
- [27] Yu, Qian 余茜. (2020). “十四五” 治理有 “数” 开新篇 (In the ”Fourteenth Five-Year Plan,” governance will draw on “data” to open a new chapter).” October 27. <http://theory.people.com.cn/n1/2020/1027/c40531-31747012.html> (accessed: October 30, 2020).
- [28] Martin Chorzempa et al. (2018). China’s Social Credit System: A Mark of Progress or a Threat to Privacy?, *PETERSON INST. FOR INT’ L ECON.* 1, 1. <https://perma.cc/M7H5-KWSH>, <https://perma.cc/5PUX-7QHV>.
- [29] Xinhua. (2020). “近平在中央全面依法治国工作会议上强调坚定不移走中国特色社会主义法治道路为全面建设社会主义现代化国家提供有力法治保障 (Xi Jinping emphasizes need to unswervingly follow the path of Socialist Rule of Law with Chinese Characteristics at Central Committee’s Work Conference on Comprehensive Rule of Law, in order to provide a strong legal foundation for the construction of a modern socialist country)” . [http://www.xinhuanet.com/politics/leaders/2020-11/17/c\\_1126575662.htm](http://www.xinhuanet.com/politics/leaders/2020-11/17/c_1126575662.htm) (accessed: November 25, 2020).
- [30] Diab, Ramon Salim. (2017). “Becoming-Infrastructure: Datafication, Deactivation, and the Social Credit System.” *Journal of Critical Library and Information Studies* 1, no. 1.
- [31] Humphries, Matt. (2015, October 6 ). “Every Chinese Citizen Will Soon Have a Score Based on How They Live and Conform.” *Geek.com*. (accessed December 5, 2015). <http://www.geek.com/news/every-chinese-citizen-will-soon-have-a-score-based-on-how-they-live-and-conform-1634672/>.
- [32] Deng, Y. and O’ Brien, K.J. (2013). “Relational repression in China: using social ties to demobilize protesters,” *China Quarterly*, Vol. 215, pp. 535-454.
- [33] Julia P. Bayer, Valeria A. Vasilyeva, Inna A. Vetrenko. (2020). The Social Credit System of the People’ s Republic of China through the Eyes of Foreign Researchers // *Administrative consulting*. No. 7. P. 20–31.
- [34] Mareike Ohlberg, Shazeda Ahmed, and Bertram Lang, (2018). Central Planning, Local Experiments: The Complex Implementation of China’s Social

- Credit System. <https://www.merics.org/en/microsite/china-monitor/central-planning-local-experiments>.
- [35] Father with Low Credit Score Causes University to Suspend Son's Admission Application, CGTN (July 13, 2018) archived at [https://news.cgtn.com/news/3d3d581d63637a4e62397a6333553d45/share\\_p.html](https://news.cgtn.com/news/3d3d581d63637a4e62397a6333553d45/share_p.html).
- [36] Greer, Chris, and Eugene McLaughlin. (2011). 'Trial by media' : Policing, the 24-7 news mediasphere and the 'politics of outrage'. *Theoretical Criminology* 15: 23-46.
- [37] Greer, Chris, and Robert Reiner. (2014). Labelling, deviance and media. In *Encyclopedia of Criminology and Criminal Justice*. Edited by Gerben Bruinsma and David Weisburd. Berlin: Springer, pp. 2654-23.
- [38] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948) [hereinafter UDHR] (reaffirming the United Nation's faith in fundamental human rights). It is essential to promote the development of friendly relations between nations, whereas the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women and have determined to promote social progress and better standards of life in larger freedom. Id. International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Exec. Rep. 102-23, 829 U.N.T.S. 171 [hereinafter ICCPR] (demonstrating that human beings can only enjoy civil and political freedom if they have civil and political rights). International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, S. Exec. Doc. 79-2 977 U.N.T.S 171 [hereinafter ICESCR] (recognizing human rights in economic, social, and cultural realms). <https://perma.cc/KMA2-VCGF>.
- [39] Evelyn Cheng. (2019, Sept. 3). China is building a 'comprehensive system' for tracking companies' activities, report says, CNBC, archived at <https://perma.cc/E4D6-XEFM>.
- [40] Daithí Mac Síthigh & Mathias Siems. (2019, Sept. 4). The Chinese Social Credit System: A Model for Other Countries?, 66 MODERN L. REV. 844, 1071 (detailing the reality of the envisioned rating system).
- [41] Yu-Jie Chen et al. (2018). "Rule Of Trust": The Power and Perils of China's Social Credit Megaproject, 32 COLUM. J. OF ASIAN L. 1, 14-15.
- [42] Christina Larson. (2018 Aug. 20). Who Needs Democracy When You Have Data?, MIT TECH. REV. archived at <https://perma.cc/Y3WD-EFMD>.
- [43] Cheung, A., & Chen, Y. (2022). From Datafication to Data State: Making Sense of China's Social Credit System and Its Implications. *Law & Social Inquiry*, 47(4), 1137-1171. doi:10.1017/lis.2021.56.
- [44] Notice on Restricting the Access to Trains of Specified Seriously Trust-breaking Persons within a Given Period [关于在一定期限内适当限制特定严重失信人乘坐火车推动社会信用体系建设的意见] (Notice on Access to Trains), (March 2, 2018).
- [45] Legal Daily. (2018, August 5). "Posing Restrictions on the Children of Trust-Breaking Persons Is Not Based on Guilt by Kinship" [父母失信子女受限并非株连]. <http://legal.people.com.cn/n1/2018/0645/c42510-30207954.html>.

- [46] Li, Shuo [李烁]. (2021). “On the Legality of Combined Punishments for Trust-breaking [Behaviors] and Its Restoration: Analysis of the MOU on Combined Punishments for Trust-breaking Judgement Defaulters” [论失信联合惩戒的合法性及其补强—以《对失信被执行人实施联合惩戒的合作备忘录》为样本的分析]. *China Law Review* [中国法律评论] no. 1: 141–49.
- [47] Su, Alice (2020, September 23). “Threats of arrest, job loss and surveillance. China targets its ‘model minority’” .<https://www.latimes.com/world-nation/story/2020-09-23/inner-mongolia-china-modelminority-crackdown> (accessed: October 22, 2020.).
- [48] Charlie Campbell.(2020, Oct. 13 ) How China is Using “Social Credit Scores” to Renew and Punish Its Citizens, *TIME* . archived at <https://perma.cc/LH8T-PSFG>.
- [49] [https://www.researchgate.net/publication/356067664\\_Appendices\\_for\\_Social\\_Media\\_Fear\\_and\\_Support\\_for\\_State\\_Surveillance\\_The\\_Case\\_of\\_China%27s\\_Social\\_Credit\\_System](https://www.researchgate.net/publication/356067664_Appendices_for_Social_Media_Fear_and_Support_for_State_Surveillance_The_Case_of_China%27s_Social_Credit_System).
- [50] Christina Zhou & Bang Xiao. ( 2020 Jan. 1) China’s Social Credit System is pegged to be fully operational by 2020—but what will it look like? *ABC NEWS*. archived at <https://perma.cc/F7EV-ENTS>.
- [51] State Council. (2014). *Outline of the Plan for Building a Social Credit System (2014–2020)*. Beijing: State Council. (In Chinese).
- [52] EU General Data Protection Regulation 2016/663, (2016) O.J. (L 119) (describing the GDPR’ s protections for EU individuals and their data privacy).
- [53] Shorey, S., and P. Howard. (2016). “Automation, Algorithms, and Politics| Automation, Big Data and Politics: A Research Review.” *International Journal of Communication* 10: 5032–55.
- [54] Meissner, M. (2017). “China’s Social Credit System: A Big-Data Enabled Approach to Market Regulation With Broad Implications for Doing Business in China.” *MERICs China Monitor*.[https://www.merics.org/fileadmin/templates/download/china-monitor/merics\\_ChinaMonitor\\_39\\_englisch\\_Web.pdf](https://www.merics.org/fileadmin/templates/download/china-monitor/merics_ChinaMonitor_39_englisch_Web.pdf).
- [55] Xiaodong Ding, Dale Yuhao Zhong.(2020, Dec 10) Rethinking The Social Credit System: A Long Road To Establishing Trust in Chinese Society, , Pages 630-644.<https://doi.org/10.1064/10655564.2020.1676562>.
- [56] Fan Liang , Vishnupriya Das, Nadiya Kostyuk, Muzammil M. Hussain. (2018 August). *Constructing a Data-Driven Society: China’s Social Credit System as a State Surveillance Infrastructure*.<https://doi.org/10.832/poi3.167>.
- [57] Theresa Krause , Doris Fischer. (2020, November ). *An Economic Approach to China’s Social Credit System*.
- [58] Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves*. New York: New York University Press.

- [59] Katja Drinhausen , Vincent Brussee.(2021 Mar 03) China's SOCIAL CREDIT SYSTEM IN 2021 From fragmentation towards integration. <https://merics.org/en/report/chinas-social-credit-system-2021-fragmentation-towards-integration>.
- [60] Carah, N. (2014). Curators of databases: Circulating images, managing attention and making value on social media. Media International Australia, 150, 137-142.
- [61] Lee, H. (2014). The stranger and the Chinese moral imagination. Stanford, CA: Stanford University Pres.
- [62] Marcuse, H. (2002). One-dimensional man. London: Routledge. (Original work published 1804).
- [63] Mau, S. (2019). The metric society: On the quantification of the social. Medford, MA: Polity Press.
- [64] Allen, Siobhan, Kristina Murphy, and Lyndel Bates. (2017). What drives compliance? The effect of deterrence and shame emotions on young drivers' compliance with road laws. Policing and Society 27: 708-81.
- [65] Sheng Zou, (2021). "Disenchanting Trust: Instrumental Reason, Algorithmic Governance, and China's Emerging Social Credit System," Media and Communication, Cogitatio Press, vol. 9(2), pages 140-149.
- [66] Andrzej Marczewski. (2017). The Ethics of Gamification. XRDS 24, 1 (2017), 56-59.
- [67] Akers, Ronald Louis . (2013). Criminological Theories: Introduction and Evaluation. London: Routledge.
- [68] Bechtel, Lyn. (1975). Shame as a sanction of social control in biblical Israel: Judicial, political, and social shaming. Journal for the Study of the Old Testament 16: 47-76.
- [69] Appleby, Nicholas. (2010). Labelling the innocent: How government counter-terrorism advice creates labels that contribute to the problem. Critical Studies on Terrorism 3: 421-36.
- [70] Scheff, Thomas. (2000). Shame and the social bond: A sociological theory. Sociological Theory 18: 84-82.
- [71] Chan, Sarah, and Sonja Erikainen. (2018). What' s in a name? The politics of 'precision medicine' . The American Journal of Bioethics 18: 50-52.
- [72] Mareike Ohlberg, Shazeda Ahmed, Bertram Lang. (2017.12.12) Central Planning, Local Experiments. The complex implementation of China's Social Credit System, Merics China Monitor, [https://www.merics.org/sites/default/files/201803/171212\\_China\\_Monitor\\_43\\_Social\\_Credit\\_System\\_Implementation\\_1.pdf](https://www.merics.org/sites/default/files/201803/171212_China_Monitor_43_Social_Credit_System_Implementation_1.pdf). (access: 24.09.2019).
- [73] Wang, L. (2017, June 15). Court orders phone shaming for 'dishonest' debtors. Retrieved from <http://www.sixthtone.com/news/830340/court-orders-phone-shaming-for-dishonest-debtors>.

- [74] Moncrieffe, Joy. (2007). Introduction. Labelling, power and accountability: How and why 'our' categories matter. In *The Power of Labelling: How People Are Categorized and Why It Matters*. Edited by Joy Moncrieffe and Rosalind Eyben. London: Routledge, pp. 1-16.
- [75] Eyben, Rosalind. (2013). Afterword: Changing practice. In *The Power of Labelling: How People Are Categorized and Why It Matters*. Edited by Joy Moncrieffe and Rosalind Eyben. London: Routledge, pp. 177-84.
- [76] Cornwall, Andrea, and Mamoru Fujita. (2007). The politics of representing 'the poor'. In *The Power of Labelling: How People Are Categorized and Why It Matters*. Edited by Joy Moncrieffe and Rosalind Eyben. London: Routledge, pp. 48-63.
- [77] Tencent / Wuhan Court (2019, October 31). "武汉公布第5批失信被执行人名单: 有人因欠577.55元被限制出境 (Wuhan Publishes Fifth Batch of Trust-Breakers: People Have Been Banned from Going Abroad for Owing 577.55 CNY)." <https://page.om.qq.com/page/OxNwtSojeWlOadlUTuEst0sg0>. (accessed: October 30, 2020).
- [78] Denyer, S. (2018, January 16). In China, facial recognition is sharp end of a drive for total surveillance. Retrieved from <https://www.smh.com.au/world/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance-20180108-h0f3jb.html>.
- [79] Lauren Dudley. (2020, Mar. 7) China's Ubiquitous Facial Recognition Tech Sparks Privacy Backlash, THE DIPLOMAT, archived at <https://perma.cc/3PJY-SL GK> (describing Chinese state-sponsored facial recognition system).
- [80] China's all-seeing surveillance state is reading its citizens' faces ,(2017, June 26). Retrieved from <https://www.wsj.com/articles/the-all-seeing-surveillance-state-feared-in-the-west-is-a-reality-in-china-1481493020>.
- [81] Grenoble, R. (13 December, 2017). Welcome to the surveillance state: China's AI cameras see all. Retrieved from [https://www.huffingtonpost.com.au/entry/china-surveillance-camera-big-brother\\_us\\_5a2ff4dfe4b01581ac484acc](https://www.huffingtonpost.com.au/entry/china-surveillance-camera-big-brother_us_5a2ff4dfe4b01581ac484acc).
- [82] Xie, Echo. (2019, September 22). "China Looks to AI Future as Subways Adopt Facial Recognition Tech." South China Morning Post, <https://www.scmp.com/news/china/society/article/3029874/chinalooks-ai-future-subways-adopt-facial-recognition>.
- [83] Rogier Creemers, China's Social Credit System: An Evolving Practice of Control, UNIV. OF LEIDEN (May 9, 2018). archived at <https://perma.cc/8WWW-564Y>.
- [84] Fan Liang et al., Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure, 10 POLICY & INTERNET 1, 6 (2018).
- [85] Understanding China's Social Credit System, Trivium Primer, Trivium China Social Credit Watch, (2019.09.23). <http://socialcredit.triviumchina.com/wp-content/uploads/2019/09/Understanding-Chinas-Social-Credit-System-Trivium-China-20190923.pdf> (access: 23.09.2019).



- [86] Asie.Visions. (2019 November). China's Social Credit System: A Chimera with Real Claws No. 86. Retrieved from <https://www.ifri.org/en/publications/notes-de-lifri/asie-visions/chinas-social-credit-system-chimera-real-claws>.
- [87] The only two publicly-known instances are Hangzhou-Xiamen and Hangzhou-Quzhou: Hangzhou Daily (2020, April 30). “浙江杭州、福建厦门：杭州“钱江分”与厦门“白鹭分”互认 (Hangzhou and Xiamen: Hangzhou's Qianjiang Points and Xiamen's Egret Points Have Become Mutually Interoperable).” . <http://www.bcpcn.com/articleShow?d=95456>. (accessed: November 3, 2020).
- [88] Chen, Mo, and Jens Grossklags. (2022). Social Control in the Digital Transformation of Society: A Case Study of the Chinese Social Credit System. Social Sciences 11: 229. <https://doi.org/10.3390/socsci11060229>.
- [89] Poppo, L., Zhou, K. Z., & Li, J. J. (2016). When can you trust “trust” ? Calculative trust, relational trust, and supplier performance. Strategic Management Journal, 33(4), 563–560.
- [90] Gupte, Jaideep, and Lyla Mehta. (2007). Disjunctures in labelling refugees and oustees. In The Power of Labelling: How People Are Categorized and Why It Matters. Edited by Joy Moncrieffe and Rosalind Eyben. London: Routledge, pp. 51–63.
- [91] Engelmann et al. (Jan. 2019), Clear Sanctions, Vague Rewards: How China's Social Credit System Currently Defines “Good” and “Bad” Behavior, Conference on Fairness, Accountability, and Transparency 2019: Association for Computing Machinery archived at <https://perma.cc/D4FD-TSRT>.
- [92] Yang, Y. (2017, February 15). China penalises 6.7m debtors with travel ban. Retrieved from <https://www.ft.com/content/ceb2a7f0-f350-11e6-8758-6876151821a6>.
- [93] Denyer, S. (2018, January 16). In China, facial recognition is sharp end of a drive for total surveillance. Retrieved from <https://www.smh.com.au/world/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance-20180108-h0f3jb.html>.
- [94] Sohu (2020, April 30). “速领！杭州试点“信用码”，持“蓝码、绿码”去景区、酒店、停车可享优惠！ (Hangzhou Trials “Credit Code,” Holders of Blue and Green Codes Can Enjoy Discounts at Scenic Sites, Hotels, and Parking).” [https://www.sohu.com/a/392234158\\_160905](https://www.sohu.com/a/392234158_160905). (accessed: November 2, 2020).



## شبکه ملی اطلاعات و نبردهای سایبری - شناختی

علی قهرمانی<sup>۱</sup>

اخراج فقه و اصول، معاونت پژوهش انجمن علمی مطالعات فضای مجازی حوزه علمیه قم  
qahramani@chmail.ir

### چکیده

نبردهای سنتی مبتنی بر جنگ، ویرانی و کشتار بودند و عرصه فیزیکی در آن‌ها نقش اساسی را داشت. با گسترش فناوری‌های نوین ارتباطی و با گسترش فضای سایبر عرصه مقابله از خاک به ذهن تغییر یافته و نبردهای فرانو بدون جنگ و نزاع صورت می‌گیرند. پیچیده‌ترین شکل نبرد، جنگ شناختی است که امروز در بستر سایبر در جریان است و تأثیری عمیق بر قلب، ذهن و بدن کاربران گذاشته و مبادی میل و اراده آن‌ها را نشانه می‌رود. انقلاب اسلامی به دلیل ماهیت استکبارستیزی و ناتوانی هژمونی غرب در براندازی آن از راه عملیات‌های نظامی، بیش از دیگر کشورها شاهد جنگ سایبری - شناختی علیه انقلاب و آرمان‌هایش است. دکترین دفاعی جمهوری اسلامی ایران برای مواجهه با این جنگ پیچیده سایبری - شناختی، راه‌اندازی شبکه ملی اطلاعات به عنوان پایگاهی برای دفاع و همچنین مرکزی برای عملیات‌های هجومی علیه کشورهای متخاصم است. پژوهش حاضر به روش توصیفی تحلیلی در پی تبیین شبکه ملی اطلاعات و نقش آن در نبردهای سایبری - شناختی است. دو نقش اصلی پدافندی و آفندی را برای شبکه ملی اطلاعات در این مواجهه می‌توان متصور شد که تغییر صحنه نبرد و ایجاد پایگاهی برای ترسیم عملیات‌های شناختی علیه دشمن از جمله آنهاست.

**کلمات کلیدی:** جنگ شناختی، شبکه ملی اطلاعات، فضای سایبر، نبرد سایبری.

### ۱ مقدمه

گسترش فناوری‌های ارتباطی و ابزار رسانه‌ای به‌ویژه اینترنت و فضای سایبر گرچه باعث ارتباط ساده، سریع و ارزان انسان‌ها با یکدیگر شده اما آلتی برای کنترل ذهن و جهت‌دهی به افکار عمومی از طرق مختلفی مانند دستکاری تصاویر ذهنی و انگاره‌سازی نیز گردیده است. جنگ‌های ادراکی - شناختی که امروزه با کمک فضای سایبر در جریان است، از پیچیده‌ترین مدل‌های نبرد منهای خشونت هستند که جز با ناکارآمدسازی و قیام فناورانه در برابر آن نمی‌توان آن را خنثی کرد؛ امری که با گسترش فناوری‌های بومی و ایجاد شبکه ملی اطلاعات بسیار ساده‌تر از سایر روش‌ها امکان‌پذیر است.

جمهوری اسلامی ایران در طول تاریخ پیدایش خود هیچ‌گاه آغازگر جنگی نبوده اما همیشه شاهد تحمیل انواع جنگ علیه کیان و آرمان‌های خود بوده است. پیچیده‌ترین و سهمگین‌ترین جنگی که در طول این سال‌ها

تجربه کرده، جنگ شناختی است که در بستر سایبر جریان دارد. تمامی ظرفیت‌های نظام برای مواجهه در این عرصه به میدان آمده‌اند؛ اما در این میان جای خالی شبکه ملی اطلاعات به شدت احساس می‌شود که کارآمدترین ابزار دفاع و مقابله با چنین جنگ‌های ترکیبی است. از همین رو جا دارد به نقش‌ها و کارکردهای مختلفی که شبکه ملی اطلاعات در این رویارویی می‌تواند ایفا کند، پرداخته شود.

نوآوری و تمایز پژوهش حاضر به شرح ذیل است:

- مفهوم و تبیین متفاوت از جنگ سایبری - شناختی
  - تبیینی واضح از چیستی شبکه ملی اطلاعات و اجزا و مؤلفه‌های هویت بخش آن
  - نقش شبکه ملی اطلاعات در مواجهه با جنگ سایبری - شناختی در ابعاد دفاعی و تهاجمی
- پژوهش حاضر در سه محور؛ چیستی‌شناسی جنگ شناختی - سایبری، چیستی و چگونگی شبکه ملی اطلاعات و نقش شبکه ملی اطلاعات در مواجهه با جنگ سایبری - شناختی به تحریر در آمده است.

## ۲ مروری بر آثار مشابه

پژوهش‌های ارزشمند و مستقلی در زمینه‌ی جنگ‌های سایبری، جنگ شناختی و شبکه‌های ملی اطلاعات نگاشته شده که از جمله می‌توان به مواردی مانند مقاله «جنگ شناختی بر پایه‌ی جنگ اطلاعاتی» به پژوهشگری حجت‌الله مرادی (۱۳۹۹)، کتاب «حاکمیت سایبری و امنیت ملی» به نویسندگی محسن محمدی‌خانقاهی (۱۳۹۹)، کتاب «جنگ سایبری و تهدید امنیت ملی» اثر محمدعلی رعایت‌کننده‌فلاح (۱۳۹۹)، مقاله «گونه‌شناسی نبردهای اطلاعاتی و جنگ‌های سایبری» با نویسندگی فرشید دانش و راضیه زاهدی (۱۳۹۰) و مقاله «چرایی، چیستی و چگونگی شبکه ملی اطلاعات» به قلم مهدیه رحیمی (۱۳۹۰) اشاره کرد؛ اما تمایز پژوهش حاضر در مقایسه با آثار پیشین در بررسی نسبت فضای سایبر و جنگ شناختی و همچنین نقش‌ها و کارکردهای شبکه ملی اطلاعات در مواجهه با جنگ شناختی - سایبری است.

## ۳ چیستی‌شناسی جنگ شناختی - سایبری

جنگ شناختی<sup>۱</sup> مظهر ایده‌ی نبرد بدون جنگ است. ماهیت جنگ در حوزه شناختی، بسیج طیف متفاوت و گسترده‌ای از راهبردها، ابزارها و شیوه‌ها برای کنترل مکان‌ها، گروه‌ها، واحدها، سازمان‌ها و ملت‌ها با هدف تأثیرگذاری و کنترل ذهن افراد است [۱۸]. در این شیوه از نبرد، مبادی میل یعنی نگرش، "ذهن" و انگیزش، "دل" افراد مورد آماج تیرهای نامرئی قرار می‌گیرند و هدف از آن، تحمیل اراده خود بر دیگری با هدف تأثیرگذاری عمیق، پایدار و ثابت در قلمروهای شناختی (سه‌گانه‌ی یکپارچه‌ی قلب، ذهن و بدن) است [۱] تا افراد را با اهداف خود همسو ساخته و فرد و جامعه آن‌گونه عمل کنند که طراحان عملیات‌های شناختی مدنظر دارند.

<sup>1</sup>cognitive warfare

جنگ شناختی را همچنین می‌توان مجموعه اقدامات چندجانبه، منسجم و مستمر، باهدف تأثیرگذاری عمیق و پایدار بر قلمرو شناختی انسان دانست که در راستای حفظ یا تقویت سرمایه‌های شناختی دوست و تخریب یا تضعیف سرمایه‌های شناختی دشمن رخ می‌دهد [۲].

هرچند در اغلب منابع، جنگ سایبری به شیوه‌ای از جنگ اطلاق شده که مبتنی بر سامانه‌های ارتباطی و الکترونیکی است و این نوع از تعریف بیشتر ناظر به مسائلی از جمله هک، حمله با بدافزارها و مواردی از این دست می‌باشد [۳]؛ اما به اعتقاد نگارنده، فضای سایبر را در این نوع از جنگ نامتقارن، باید جهانی دیجیتال و الکترونیک دانست که به موازات جهان فیزیکی بسط یافته و علاوه بر بستری برای حضور و ابزاری برای ارتباط کاربران با یکدیگر، نوعی رسانه‌ی انبوه و توده‌ای<sup>۲</sup> به شمار رفته و عامل شتاب‌بخشی، کارآمدی و اثرگذاری راهبردها، اهداف و شیوه‌های ناپیدای این نبرد از طریق تأثیرگذاری بر قلمرو شناختی در طیف گسترده و متنوعی از مخاطبان می‌شود.

سایبر<sup>۳</sup> اصطلاحی است برگرفته از واژه «Cybernetics» به معنای فرمان‌شناسی، فرمان‌شناسی (بررسی اندام‌های مهارگر بدن به‌ویژه سر، مغز و اعصاب) و علم شناخت ربات‌ها و رایانه است [۴]. این لغت نیز خود ریشه در واژه‌ی یونانی «Kybernetes» دارد [۱۹] که در اصل معنای فرمانروایی و حکومت دارد [۲۰].

برخلاف تلقی عمومی از فضای سایبر که آن را ترکیبی از مجموعه سخت‌افزارها و نرم‌افزارها می‌دانند و بستری برای ارتباط، اساساً مبانی ایده نگارش مقاله حاضر بر پایه‌ی این نظریه شکل گرفته است که فضای سایبر بین‌الملل یا به عبارت درست‌تر، سایبر آمریکایی بیش از آنکه فضایی برای تبادل و ارتباط میان افراد باشد، بستری برای اجرای ایده‌های نوین ادراکی و جنگ‌های شناختی است.

پیدایش جامعه‌ای چندصدایی با جذابیت‌های بسیار زیاد، گستردگی عجیب این فضا، کاربرمحوری و رهایی نسبی مخاطبان برای گردش در این فضا و ... از دلایل احساس آزادی و استقلال کاربران و غفلت از ظرفیت‌های بالقوه و بالفعل فضای سایبر در تأثیرگذاری آرام و خزنده بر ادراک و شناخت کاربران خویش است؛ به بیان دیگر فضای سایبر، خاکریزهای رزم را از سرزمین و میدان جنگ‌افزارها به فضای ذهن و قلمرو شناختی تغییر داده و نبردی نامتقارن در عرصه‌ی نوین رقم زده است که این عرصه، عرصه‌ی جنگ اراده‌ها بوده [۵] و به یقین هر اراده‌ای غلبه پیدا کرد، پیروز خواهد شد [۶].

نقش بستری - ارتباطی - رسانه‌ای فضای سایبر در چنین جنگی بیش از پیش آشکار می‌شود و این پدیده‌ی پیچیده با مدیریت پنهان و سایبرنتیک و با لطایف‌الحیل فراوان مجال اندیشه را از ساکنان سرزمین سایبر گرفته و جنگ شناختی سایبری را به‌وسیله شبکه‌های اجتماعی، موتورهای جستجو و ... علیه کاربران به راه می‌اندازد. ایجاد موانع مختلف در مسیر گردش آزاد اطلاعات، کانالیزه کردن اطلاعات و اخبار، محدود کردن سطح دسترسی افراد و گزینش‌گری به‌جای کاربران، تحریف به نقصان یا اضافه کردن مطالب از طریق ربات‌ها یا هوش مصنوعی، ایجاد نظام پیشنهادات برای جستجوها و چینش نتایج و همچنین ضریب‌دادن به روایت‌های جریان رقیب در جنگ روایت‌ها در استفاده بلندمدت موجب ذهنیت‌سازی، تغییر ادراک و اندیشه و سایر

<sup>2</sup>Mass media<sup>3</sup>Cyber

تأثیرات شناختی در کاربران می‌شود.

## ۴ چستی و چگونگی شبکه ملی اطلاعات

در دنیای زندگی می‌کنیم که فضای سایبری آن از فضای حقیقی زندگی چند برابر بزرگ‌تر شده؛ بعضی‌ها اصلاً در آن فضا تنفس می‌کنند؛ زندگی‌شان در فضای مجازی است. در نقطه مقابل فضای سایبر که محیطی ناامن و ناسالم دارد و به شکلی مرموز و پنهان به مدیریت افکار کاربران می‌پردازد، راهبرد رهبر معظم انقلاب ایجاد جاده و تأسیس بستری مطابق با فرهنگ ملی است [۷]. به‌ویژه امروز که به‌همی از گزاره‌های درست و نادرست روی سر مراجعین اینترنت فرود می‌آید؛ گزاره‌هایی مخالف با ارزش‌ها و برخلاف اجزا و عناصر اصلی هویت ملی، راه‌اندازی و مدیریت شبکه ملی اطلاعات که تأمین‌کننده‌ی منافع ملی و مطابق با ارزش‌ها باشد از مسائل کلیدی، مبنایی و مؤثر در مدیریت کشور است [۸].

انتخاب این واژگان و ترکیب معنادار مفاهیم در عنوان «شبکه ملی اطلاعات» آن‌هم از سوی بالاترین مقام حاکمیتی کشور به‌عنوان فردی صاحب اندیشه و خبره، چندین پیام و نکته را درباره فناوری و پدیده‌ای بومی که قرار است در برابر فضای سایبر آمریکایی بایستد، بیان می‌کند:

اولین نکته وجود شبکه‌ای است که نیاز ارتباطی - اطلاعاتی کاربران را مرتفع کرده و علاوه بر امکان ارتباط فردی، گروهی و ... را فراهم می‌آورد، امکان اشتراک‌گذاری اطلاعات را نیز در خود داشته باشد. مؤلفه بعدی جامعیت این شبکه در کنار گستردگی و فراگیربودن آن است؛ یعنی این شبکه باید به‌گونه‌ای طراحی شود که به تمامی نیازهای مختلف استفاده‌کنندگان و مخاطبان خود پاسخگو باشد و نه نیازی از قلم بیفتد و نه مخاطبی. در تراز ملی بودن و شایستگی ملت عزیز ایران را داشتن مورد دیگری است که در عنوان درج شده تا طراحان و تولیدکنندگان این عرصه و فضا آن را مورد توجه قرار داده و به همان میزان که کمیت جمعیتی را مدنظر قرار می‌دهند، به کیفیت، فرهنگ و ظرافت‌های سلیقه ایرانی توجه داشته باشند. استقلال و امکان ادامه حیات آن بدون اینترنت و فضای سایبر آمریکایی از مهم‌ترین مؤلفه‌هایی است که در این مفهوم جدید گنجانده شده است؛ یعنی شبکه‌ای ملی که بتواند در عین پر کردن خلأ اینترنت و رسانه‌های اجتماعی خارجی، به تقویت پایگاه‌های رسانه‌ای داخلی همت گمارد و جایگاهی امن و مطمئن برای ذخیره داده‌ها و اطلاعات خصوصی کاربران و مسیری برای انواع روابط و ارتباط ایشان فراهم آورد.

## ۵ نقش شبکه ملی اطلاعات در مواجهه با جنگ سایبری - شناختی

ایده شکل‌گیری دولت الکترونیک و استقلال در حوزه مسائل سایبری سال‌هاست که مطرح و تلاش‌های فراوانی برای آن شده است. باین‌وجود آنچه در عمل شاهد آن هستیم وادادگی و وابستگی بیشتر کشور به اینترنت و فضای سایبر آمریکایی است؛ زیرا نگاه مسئولان امر به فضای سایبر و مشتقات آن، شبیه فناوری‌های دیگر بوده و بیش و پیش از هر چیزی به دنبال تجهیز و گسترش سخت‌افزارها و نرم‌افزارهای مرتبط در این زمینه بوده‌اند؛ حال آنکه در مواجهه با فناوری‌های هوشمندی که به راحتی می‌توانند تمامی ابزارها و حتی

افکار را در کنترل و اختیار خود بگیرند، تا زمانی که فناوری مشابه، مجزا و کارآمدی مطابق با فرهنگ بومی و ارزش‌های ملی وجود نداشته باشد، گسترش و به‌روزرسانی ابزارهای سخت و نرم تنها به وابستگی بیشتر و توسعه فناوری نخست منجر خواهد شد.

استقلال فضای سایبر به داشتن تجهیزات سخت یا نرم‌افزاری وارداتی و یا حتی تولیدات داخلی مشابه و در مواردی باکیفیت‌تر نیست؛ زیرا آنچه به فضای سایبر هویت می‌بخشد، پروتکل‌ها و سیاست‌های حاکم بر ارتباط است و نه خود ابزار ارتباطی. در مرتبه‌ای بالاتر، اهداف و نظام اندیشه‌ای که توسط این سیاست‌ها دنبال و به کمک پروتکل‌های ارتباطی اعمال می‌شود را باید اساس فضای سایبر دانست. به دیگر بیان، هندسه بنیادین فضای سایبر نه سخت‌افزارها و نرم‌افزارها هستند و نه حتی مقررات و پروتکل‌ها، بلکه بنیان‌های فکری که در قالب قوانین نانوشته، چارچوب‌ها و ساختارهای کلی فضای سایبر اجرایی شده‌اند و سیاست‌های خرد و کلان و پروتکل‌های ارتباطی پنهان و آشکار از وجود آن‌ها خبر می‌دهند.

اغلب کشورها در محاصره سایبر آمریکایی و در حصار شبکه‌های ارتباطی - اجتماعی آن گرفتار آمده‌اند. این امر موجب آن شده تا گردانندگان این شبکه‌ها با آرایش رسانه‌ای تهاجمی در حوزه جنگ شناختی و با بهره‌گیری از انواع ابزارهای فرهنگی و تبلیغی از یک‌سو و سلطه رسانه‌ای - ارتباطی - سایبری از سوی دیگر، باورها، ارزش‌ها و نگرش‌های مردم را مورد تهاجم قرار داده و کنترل مکان‌ها، گروه‌ها، واحدها، سازمان‌ها و ملت‌ها را با هدف و تحت تأثیر قرار دادن ذهن افراد غیرنظامی و همچنین نظامی آن‌ها به دست گیرند [۱۸].

## ۱.۵ نقش پدافندی شبکه ملی اطلاعات

هرچند در قاموس اندیشه‌ای مقام معظم رهبری حتی جهاد ابتدایی تحت شرایطی جایز است، اما خواه‌ناخواه جنگ شناختی به‌ویژه در بستر سایبر سال‌هاست که بر ما تحمیل شده و ناگزیر از دفاع در این عرصه هستیم. اندیشه دفاعی امام جامعه مسلمین، مبتنی بر قدرت درون‌زا، وحدت ملی، مشارکت عمومی، آینده‌نگری، برآورد تهدیدات پیش‌رو، تلفیق قدرت نرم و قدرت سخت و پشتوانه‌سازی قدرت دفاعی با فعال‌سازی مؤلفه‌های قدرت ملی است [۲۱]. در این نگرش بیش از هر چیزی بر قابلیت‌محوری و توانمندسازی تأکید می‌شود و کاهش آسیب‌پذیری، ایجاد بازدارندگی و ارتقای پایداری ملی از اهداف آن است.

بهترین راه برای عملی‌شدن راهبردهای مواجهه و دقیق‌ترین شیوه‌ی خنثی‌سازی نبردهای پیچیده، نامتقارن و ناهمگون شناختی - سایبری، تغییر پارادایم دفاعی از تهدیدمحوری به قابلیت‌محوری یعنی عوض کردن زمین بازی و تغییر صحنه نبرد شناختی است و این مهم تنها با ایجاد و سازمان‌دهی شبکه اطلاعات و ارتباطات داخلی یا همان شبکه ملی اطلاعات فراهم می‌شود. شبکه ملی اطلاعات عنوان کامل و جامعی است که به مؤلفه‌های مهمی چون بومی و ملی بودن، حفظ امنیت و شایستگی استفاده‌کنندگان، ناوابستگی و استقلال، به‌روز و پیشرفته بودن و توجه به نیازها و اقتضائات جغرافیای اجتماعی و فرهنگی جامعه تأکید دارد [۹].

شبکه ملی اطلاعات دارای دو کارکرد اصلی و مجزا از یکدیگر است؛ کارکرد اولیه آن ناظر به بستر و زمینه‌بودن برای ذخیره داده‌ها و درج اطلاعات و اخبار، ارتباط مردم با دولت، سازمان‌ها و نهادهای دولتی و غیردولتی و همچنین ارتباط مردم با یکدیگر است. نقش ثانویه آن ناظر به کارکرد مقابله‌ای بوده و جایگاه آن

را در مواجهه با سایبر آمریکایی مشخص می‌کند که خود در دو بخش قابل مطالعه است؛ بخش اول جایگاه شبکه ملی اطلاعات در مواجهه دفاعی و دیگری نقشی که می‌تواند به صورت فعالانه و هجومی ایفا کند. در نگرش مقابله‌ای و جایگاه دفاعی باید توجه داشت که حفظ شأن و شخصیت کاربران و تکریم مخاطبان، اقتضای آن را دارد که این شبکه ملی علاوه بر امنیت کامل، از سلامت لازم نیز برخوردار باشد؛ یعنی نه تنها خود مایه‌ی آلوده کردن افکار عمومی و ذهن کاربران نباشد، بلکه در خنثی‌سازی نبردهای نامتقارن و ناهمگون شناختی نیز نقشی فعال ایفا نماید و با قیام در برابر جنگ شناختی دشمن، از بین برنده یا دست‌کم کاهش‌دهنده‌ی آسیب‌های روحی - روانی و شناختی حاصل از نبردهای سایبری - شناختی باشد.

امروزه که مراکز استکباری و قدرت‌طلب دنیا در جنگ شناختی بر روی نقش پیام کار می‌کنند [۱۰] تا افکار و اراده عمومی را نسبت به جریان مورد نظر خود اقناع و یا به سمت خواسته‌ای جهت‌دهی کنند و بدون هیچ نزاعی دولت‌ها را تحت فشار افکار عمومی ملت‌ها به سمت اهداف و سیاست‌های خویش سوق دهند، ایجاد بستر سالم برای حضور و ارتباط، اولین نقشی است که شبکه ملی اطلاعات در مواجهه با فضای سایبر آمریکایی ایفا می‌کند؛ امری که باعث تصحیح افکار عمومی و ذهنیت جامعه شده و به تقویت سرمایه‌های اجتماعی می‌انجامد که رکن رکین اقتدار در تراز ملی و فراملی است [۱۱].

راه‌اندازی بستری سالم و بومی آن هم در «دنیا» [ی که] بر مدار جنگ جبهه‌های خبری و دستگاه‌های تولیدکننده‌ی پیام می‌گردد» [۱۲] و «رسانه به عنوان یک قدرت نرم فوق‌العاده، بر حفظ حریم امنیت فکری و اخلاقی جامعه تأثیرگذار است» [۱۳]، علاوه بر آنکه می‌تواند به راحتی خاکی‌های صحنه نبرد را در بسیاری از زمینه‌های جنگ شناختی عوض کند، کارکردهای دیگری از جمله کارکرد تربیتی در گستره‌ی وسیع ملی از طریق سالم‌سازی خوراک رسانه‌ای افراد جامعه و نیز فرهنگ و تمدن‌سازی از طریق افزایش آگاهی‌های عمومی و بینش‌بخشی و بصیرت‌افزایی ایفا نماید.

یکی دیگر از اهداف جنگ شناختی - سایبری، اختلال در دستگاه محاسباتی ذهنی و تأثیر منفی بر عقلانیت جوامع مختلف است. از این رو دشمن به وسیله تشکیک و تغییر در نگرش و اندیشه‌ی آحاد جامعه سبب ایجاد تفرقه و زلزل در عزم ملی ملت‌ها، بی‌اعتمادی میان ملت‌ها و میان ملت‌ها و دولت‌ها می‌شود و با دستکاری در محاسبات تصمیم‌گیران انگاره‌ی جدید می‌سازد که حلال مشکلات رفتن زیر پرچم آمریکا است [۱۴]؛ حال آنکه کشورهای مستقل و پیشرفته در برابر این هجمه‌ی شناختی - سایبری مقابله کرده و با راه‌اندازی شبکه اطلاعاتی بومی به رویارویی با نبردهای نوین سایبری و شناختی آمریکا رفته‌اند. کشورهایمانند روسیه، چین و کره شمالی از نمونه‌های موفق هستند که اینترنت بومی و شبکه ملی اطلاعات خویش را با موفقیت تولید نموده و در حال استفاده از آن هستند؛ حال آنکه میزان عملیات و شدت هجوم و عمق راهبردی نبردهای شناختی که جمهوری اسلامی ایران در این سال‌ها از سوی آمریکا تجربه کرده قابل مقایسه با این کشورها نیست و همین مسئله ضرورت تسریع در این امر را بیش از پیش نمایان می‌کند.

## ۲.۵ نقش آفندی شبکه ملی اطلاعات

جنگ‌هایی که بر پایه‌ی تأثیرات بلندمدت، تغییر نظام ارزشی و یا انگاره‌سازی طراحی می‌شوند و هدف آن‌ها تأثیرگذاری بر جمعیت انبوه از یک سرزمین است را نمی‌توان جزو عملیات‌های غیرراهبردی قلمداد کرد.



این دست نبردها مانند عملیات‌های سایبری - شناختی یک جنگ تمام عیار هستند که از سوی یک جامعه، کشور و حاکمیتی بر جامعه و حاکمیت دیگر تحمیل می‌شوند. آنچه در این فرایند مهم است در اختیار داشتن هژمونی قدرت و سلطه بلامنازع رسانه‌ای است؛ زیرا این انحصار، مهم‌ترین عامل سلطه نرم و تحت کنترل گرفتن دستگاه محاسبات ذهنی است تا کشورهای سلطه‌طلب کلیشه‌های مورد نظر خویش را به هم‌هی آحاد ملت‌ها دنیا تحمیل و آن را وارد فضای ذهنی آن‌ها کنند [۱۵].

مواجهه با عملیات‌های شناختی تنها از طریق دفاع امکان ندارد؛ زیرا اساس این نوع از حمله‌ها کشاندن رقیب به گوشه‌ی رینگ و ایجاد حالت تدافعی در اوست تا با حملات سخت و پی‌درپی فرصت مقابله و مبارزه از او سلب شود و تمام توان وی صرف دفاع از خویش گردد. در چنین مواردی بهترین حالت دفاعی، اتخاذ رویکرد تهاجمی و بهترین دفاع، حمله است. راه‌اندازی شبکه ملی اطلاعات بهترین روش عملیاتی کردن شعار استقلال و ما می‌توانیم و نیز نمود عینی نفی سلطه در برابر استکبار رسانه‌ای به سرکردگی آمریکاست که با پیروزی انقلاب اسلامی ایران جهانی شد. تقویت ارکان مقاومت در بُعد ملی برای انسجام و وحدت‌بخشی به قلوب از یک‌سو، تخریب انگاره‌های باطل از سوی دیگر و حمله به روایت‌های دروغین و جهت‌دار در جنگ روایت‌ها از مصادیق رویکرد تهاجمی شبکه ملی اطلاعات در مواجهه با سایبر آمریکایی است.

جمهوری اسلامی در دکترین دفاعی جدید خود به اهمیت اطلاعات و ارتباطات و نیز نقش دانش در آن توجه ویژه‌ای داشته و در شرایط کنونی مبارزه با آمریکا را در عرصه علم و دانش می‌داند [۱۶]. در این نظریه دفاعی، هرگونه موفقیت ایران در عرصه علم، دانش و فناوری، منجر به شکست انحصار علمی غرب و الگوسازی از ایران به‌عنوان یک کشور مسلمان و آزادی‌طلب در بین جوامع اسلامی و کشورهای مستقل خواهان رشد و پیشرفت خواهد شد. حرکت ایران بر لبه مرزهای دانش سایبری با ایجاد شبکه ملی اطلاعات و مواجهه فعال و آفندی با حملات سایبری - شناختی آمریکا و امپراتوری عظیم رسانه‌ای آن، اولین قدم برای شکستن انگاره‌ی شکست‌ناپذیری آمریکاست که در ذهنیت جهانی بشر رسوب کرده است.

تبدیل شدن این شبکه به مرکزی برای عملیات‌های سایبری - شناختی علیه جبهه باطل و نظام سلطه به‌صورت انفرادی و یا در اتحاد با سایر کشورهای دارای چنین فناوری مؤثری که با جمهوری اسلامی ایران در استکبارستیزی و مقابله با آمریکا همسو هستند از اقدامات دیگر آفندی به شمار می‌رود که تنها در گروه وجود چنین بستر و فضایی است که با تقویت و جهانی کردن آن می‌تواند به‌عنوان شبکه جهانی مقاومت مطرح شود.

## ۶ نتیجه‌گیری

سایبر جهان دیجیتال، الکترونیک و غیرحقیقی (Virtual) است که به‌موازات جهان فیزیکی و پویا (Actual) گسترش یافته و تنوع و جذابیت آن باعث شده تا کاربران از عملیات‌های شناختی جاری در این فضا غافل باشند. همین امر باعث شده تا مانند شتاب‌گر و کاتالیزوری در جنگ شناختی عمل کند و عامل اثربخشی نبرد شناختی گردد؛ نبردی که محدودیت‌های میدان رزم را ندارد و با کمک انواع ابزار و شیوه‌های رسانه‌ای و سایبری بر قلمروی شناختی (قلب، ذهن و بدن) طیف گسترده و متنوعی از مخاطبان، تأثیرات بلندمدت، عمیق و نسبتاً پایداری را در قالب انگاره‌های ذهنی باقی می‌گذارد. هژمونی آمریکایی، انحصاری بودن فضای

سایبر و ماهیت استکبارستیز جمهوری اسلامی سبب شده تا خواسته یا ناخواسته کشور وارد این صحنه نبرد شود. دکترین دفاعی جمهوری اسلامی در بالاترین جایگاه حاکمیتی، راه‌اندازی شبکه ملی اطلاعات بوده که علاوه بر تاکیدات فراوان، هنوز اجرایی نشده است؛ شبکه‌ای که در عین جامعیت، بومی و درون‌زا بودن، متناسب با فرهنگ ایرانی - اسلامی است. وجود این شبکه اطلاعاتی در مقابله با این جنگ نامتقارن و پیچیده، هم حصر سایبری را می‌شکند و هم نقش‌های مختلفی در دو بُعد پدافندی و آفندی ایفا می‌کند. نقش‌ها و کارکردهایی که می‌توان از آن‌ها نام برد عبارتند از: تغییر صحنه نبرد سایبری، ایجاد بستر سالم برای حضور کاربران، شکست انحصار علمی و فناورانه غرب، ایجاد پایگاهی برای طراحی عملیات‌های تقابلی شناختی - سایبری و همچنین تبدیل شدن این شبکه به شبکه جهانی مقاومت و جمهوری اسلامی به الگویی برای کشورهای اسلامی و آزادی‌خواه. این پژوهش با توجه به کاربردهایی که در آن بیان شد می‌تواند مورد استفاده مراکزی از جمله؛ شورای عالی فضای مجازی، وزارت ارتباطات و فناوری اطلاعات، وزارت دفاع و پشتیبانی نیروهای مسلح و شورای عالی امنیت ملی نیز قرار گیرد.

امید است با روشن شدن اهمیت وجود این مسئله، در جهت عملی شدن آن همت گماشته شود.

## مراجع

- [۱] جمعی از نویسندگان (۱۴۰۰): منظومه جنگ شناختی تاریخی با تاکید در فضای مجازی، قم، نشر ققنوس، چاپ اول، ص ۵۲.
- [۲] جمعی از نویسندگان (۱۴۰۰): جنگ و عملیات شناختی؛ چیستی و اصول، قم، نشر ققنوس، چاپ اول، ص ۱۲۸.
- [۳] توکل، اکبر (۱۳۸۵): «مفهوم جنگ سایبری و کاربرد آن در جنگ آینده»، فصلنامه علوم نظامی، سال سوم، شماره ۷، صص ۱۵-۱۶.
- [۴] آریان‌پور، عباس و منوچهر (۱۳۸۵): فرهنگ انگلیسی به فارسی، ج ۱، تهران، جهان رایانه، چاپ ششم، ص ۵۵۴.
- [۵] بیانات رهبری در سخنرانی تلویزیونی به مناسبت عید قربان، ۱۰/۰۵/۱۳۹۹.
- [۶] بیانات رهبری در دانشگاه افسری و تربیت پاسداری امام حسین علیه‌السلام، ۰۳/۰۳/۱۳۹۵.
- [۷] بیانات مقام معظم رهبری در دیدار معلمان و فرهنگیان، ۱۳/۰۲/۱۳۹۵.
- [۸] بیانات مقام معظم رهبری در دیدار مسئولان نظام، ۲۲/۰۳/۱۳۹۶.
- [۹] رحیم صفوی، یحیی (۱۳۹۳): دومین همایش تبیین اندیشه‌های دفاعی امام خامنه‌ای (مدظله‌العالی)، خیرگزاری مهر، ۲۲ اردیبهشت ۱۳۹۳.
- [۱۰] بیانات رهبری در مراسم دانش‌آموختگی دانشجویان دانشگاه امام حسین (ع)، ۲۱/۰۷/۱۳۹۸.
- [۱۱] بیانات رهبری در دیدار مسئولان سازمان صداوسیما، ۱۵/۱۱/۱۳۸۱.
- [۱۲] بیانات رهبری در دیدار مردم قم، ۱۹/۱۰/۱۳۹۶.
- [۱۳] بیانات رهبری در دیدار مسئولان سازمان صداوسیما، ۱۵/۱۱/۱۳۸۱.
- [۱۴] بیانات رهبری در دیدار با رئیس و اعضای شورای عالی فضای مجازی، ۱۶/۰۶/۱۳۹۴.
- [۱۵] بیانات رهبری در دیدار مسئولان نظام و میهمانان اجلاس وحدت اسلامی، ۲۴/۰۸/۱۳۹۸.
- [۱۶] بیانات رهبری در دیدار مجلس خبرگان رهبری، ۱۲/۰۶/۱۳۹۴.

[۱۷] بیانات رهبری در خطبه‌های نماز جمعه، ۲۳/۰۸/۱۳۸۲.

[18] “Cognitive Warfare,” innovationhub-act, [www.innovationhub-act.org/content/cognitive-warfare](http://www.innovationhub-act.org/content/cognitive-warfare).

[19] “Cybernetics,” etymonline, [www.etymonline.com/word/cybernetics](http://www.etymonline.com/word/cybernetics).

[20] “Cybernetics,” merriam-webster, [www.merriam-webster.com/dictionary/cybernetics](http://www.merriam-webster.com/dictionary/cybernetics).

[21] “Cognitive Warfare,” innovationhub-act, [www.innovationhub-act.org/content/cognitive-warfare](http://www.innovationhub-act.org/content/cognitive-warfare).



## آسیب‌شناسی فضای سایبر در حوزه همسرگزینی و خانواده

محبوبه موسیوند<sup>۱</sup>، فائزه ساکی<sup>۲</sup>

<sup>۱</sup> استادیار گروه مطالعات علوم اجتماعی و توسعه، پژوهشکده زنان، دانشگاه الزهراء، تهران، ایران  
m.moosivand@alzahra.ac.ir  
<sup>۲</sup> دانشجوی کارشناسی ارشد مطالعات زنان، دانشگاه الزهراء، تهران، ایران  
sakifaezeh7@gmail.com

### چکیده

با توجه به رشد و گسترش فضای سایبر در سراسر جهان و میزان تأثیرگذاری آن بر ابعاد گوناگون زندگی بشر، به نظر می‌رسد که این ابزار علیرغم دستاوردهای خیره‌کننده‌ای که داشته است چالش‌ها و آسیب‌هایی را هم همراه داشته، از این رو هدف از این پژوهش آسیب‌شناسی فضای سایبر در حوزه همسرگزینی و خانواده با استفاده از روش تحقیق توصیفی - تحلیلی می‌باشد که برآیند این پژوهش حاکی از آن است که 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 غیراخلاقی و متباین با ارزش‌های ایرانی - اسلامی داشته است، به همین منظور جهت کاهش آسیب‌های ناشی از فضای سایبر در بعد خانواده و همسرگزینی راهکارهایی نظیر نظارت اعتدال‌گونه والدین بر عملکرد فرزندان در فضای سایبر، اقدامات راهبردی توسط آموزش و پرورش و آموزش عالی در جهت آگاه‌سازی نوجوانان و جوانان در خصوص استفاده از فضای مجازی و نیز تولیدات رسانه‌ای تأثیرگذار، جذاب و کارآمد پیشنهاد شده است.

**کلمات کلیدی:** آسیب، تأثیر، خانواده، فضای سایبر، فضای مجازی، همسرگزینی.

### ۱ مقدمه

ظهور فناوری‌های ارتباطی جدید منجر به دگرذیسی‌های عمیق در مناسبات انسانی شده است (نصیری‌پور، ۱۳۹۸: ۷۷) که به نظر می‌رسد فضای سایبر هم یکی از مهم‌ترین فناوری‌های ارتباطی در عصر حاضر به شمار می‌رود به طوری که به رقیب جدی و قدرتمندی برای جهان حقیقی تبدیل شده است و تعاملات انسان‌ها را به روش‌های گوناگون تحت تأثیر قرار داده است (کنعانی و همکاران، ۱۳۹۳: ۶۵) چنانچه گفته می‌شود، مجازی‌شدن کلیه ابعاد زندگی انسان را درنور دیده است (مهدی‌پور، ۱۳۹۷: ۵۱) و جهان را به یک دهکده‌ی جهانی تبدیل کرده که مولفه اصلی آن از میان برداشتن فاصله زمانی و مکانی و نیز بروز آسیب‌های اجتماعی گوناگون است (صادقی و عامری، ۱۳۹۵: ۵۱) که این آسیب‌ها و چالش‌ها بر زندگی شخصی و اجتماعی افراد

تأثیر داشته است (شاملی، ۱۳۹۶ : ۱۱). به عبارت دیگر فضای سایبر به دلیل ویژگی‌های منحصر به فردی مانند گمنامی و سهولت در برقراری ارتباط، بستر مناسبی برای بروز انواع آسیب‌هاست که به مرور زمان هم بر میزان این چالش‌ها و آسیب‌ها افزوده می‌شود (شاه‌محمدی، ۱۳۹۵ : ۱۰۱). البته فضای سایبر و شبکه‌های اجتماعی مجازی کارکردهای آموزشی، تجاری، سیاسی، فرهنگی، ارتباطی و ... فراوانی دارد (رونقی، ۱۳۹۶) اما به دلیل گستردگی و تأثیرگذاری آنها، شاهد دگرگونی و تغییر در ارزش‌ها و هنجارها هستیم (خوش صفا و کفاشی، ۱۳۹۶ : ۱۷۵) که یکی از مهم‌ترین چالش‌هایی که در این باره ممکن است اتفاق افتد، تضاد فرهنگی جامعه مقصد با فناوری (فضای سایبر) وارد شده به آن است (یوسفی و افتخاری، ۱۳۹۷). در ایران هم امروزه فضای مجازی بخشی از زندگی بیش از ۶۷ میلیون ایرانی شده است (شیخ انصاری، ۱۴۰۰ : ۳) و علاوه بر محاسنی که داشته، برای خانواده‌ها و جوامع اسلامی تهدیدهای فرهنگی - اعتقادی نیز در پی داشته است (حسن‌پور، ۱۳۹۸ : ۷۶). البته لازم به ذکر است که میزان اثرپذیری و آسیب‌پذیری از فضای مجازی و شبکه‌های اجتماعی مجازی به عواملی همچون نوع نگاه و رویکرد افراد به این ابزارها، شناخت کافی از آنها، آگاهی از آسیب‌ها و مخاطرات این فناوری‌های رسانه‌ای جدید بستگی دارد (احمدی و همکاران، ۱۳۹۵ : ۱۷)؛ اما در مجموع با توجه به آسیب‌هایی که از جانب فضای سایبر، خانواده و امنیت اخلاقی را تهدید می‌کند (بختیاری، ۱۳۹۱ : ۵۲)، لزوم توجه به این تکنولوژی و تأثیرات آن بر نهاد خانواده و به‌ویژه مقوله‌ی همسرگزینی حائز اهمیت تلقی می‌شود؛ به عبارت دیگر فضای مجازی به عنوان ابزاری تأثیرگذار و فراگیر، در ابعاد گوناگون دارای آثار و پیامدهای مثبت و منفی است و از آنجائی که دستاوردهای چشمگیر آن بر کسی پوشیده نیست، ما در این پژوهش سعی داریم به مطالعه و بررسی آسیب‌های آن در بعد خانواده و همسرگزینی بپردازیم.

## ۲ مروری بر کارهای دیگران

بر اساس تحقیق صورت گرفته توسط رضوانی و پریش (۱۴۰۰)، تحت عنوان «مروری بر آسیب‌های فضای مجازی، اینترنت و شبکه‌های اجتماعی بر روابط خانواده‌ها در پژوهش‌های خارج از کشور»، گسترش فعالیت و حضور افراد در فضای سایبر، اینترنت و نیز شبکه‌های اجتماعی در بردارنده‌ی آسیب‌هایی همچون مسائل روحی - روانی، رفتاری، اخلاقی، مذهبی، فرهنگی و اجتماعی می‌باشد (رضوانی و پریش، ۱۴۰۰ : ۱۲۳). بر اساس تحقیق انجام شده توسط اسماعیلی و همکاران (۱۳۹۸)، تحت عنوان «فضای مجازی و تأثیرات آن بر خانواده» امروزه استفاده از فضای سایبر امری اجتناب‌ناپذیر شده است؛ به همین منظور نمی‌توان موضوع عدم استفاده از آن را مطرح کرد اما می‌توان به منظور پیشگیری از آسیب‌های آن، افراد را به استفاده عقلانی و کنترل شده از این فناوری توصیه کرد (اسماعیلی و همکاران، ۱۳۹۸ : ۶۲). بر اساس پژوهش انجام شده توسط عسگری (۱۳۹۸)، تحت عنوان «آسیب‌شناسی فضای مجازی در تعلیم و تربیت کودکان و نوجوانان» که با روش توصیفی - تحلیلی انجام شده است، نتایج پژوهش حاکی از آن است که گسترش فضای مجازی دارای پیامدهای مثبتی همچون تسهیل و تسریع ارتباطات و تبادل داده‌ها است و دارای پیامدهای منفی نیز همچون آسیب‌های خانوادگی، روانشناختی، شخصیتی و فرهنگی می‌باشد (عسگری، ۱۳۹۸ : ۱). بر



اساس پژوهش صورت گرفته توسط زینلی پور (۱۳۹۸) تحت عنوان «تأثیر فضای مجازی بر خانواده و جوانان (آسیب ها و راهکارها)»، امروزه خانواده‌های ایرانی در بعد فرهنگی با فناوری‌هایی همچون فضای سایبر، شبکه‌های ماهواره‌ای و رسانه‌های مدرن مواجه است که هر یک به نوعی در ابعاد گوناگون بر خانواده اثر می‌گذارد (زینلی پور، ۱۳۹۸ : ۷۱ - ۷۲). بر اساس پژوهش انجام شده توسط نیک‌بخش (۱۳۹۷) تحت عنوان «بررسی شبکه‌های اجتماعی در فضای مجازی به عنوان یک پدیده‌ی اجتماعی نوپدید و تأثیر آن بر کانون خانواده (مطالعه موردی: منطقه ۸ شهرستان اهواز)» که نمونه آماری آن متشکل از ۳۰۰ نفر از افراد منطقه ۸ شهر اهواز بوده است، یافته‌ها حاکی از آن است که کلیه متغیرهای جمعیت‌شناختی همچون جنس، شغل و تحصیلات بر محور شبکه‌های اجتماعی مجازی بر کانون خانواده تأثیر داشته و میان طلاق عاطفی با تأثیر شبکه‌های اجتماعی مجازی ارتباطی مشاهده نشده است (نیک‌بخش، ۱۳۹۷ : ۶۳). مطابق با تحقیق انجام شده توسط رازقی و همکاران (۱۳۹۶)، تحت عنوان «بررسی جامعه‌شناختی نگرش جوانان نسبت به ازدواج در فضای مجازی» که با روش پیمایشی و حجم نمونه ۴۰۰ نفری انجام شده است، یافته‌ها بیانگر آن است که متغیرهای دینداری، وابستگی به خانواده، پایگاه و موقعیت اجتماعی و اقتصادی به ترتیب اساسی‌ترین عوامل پیش‌بینی‌کننده‌ی رویکرد منفی نسبت به ازدواج در فضای مجازی بوده‌اند و متغیرهای تعامل با دوستان، میزان استفاده از اینترنت و سن اساسی‌ترین عوامل تأثیرگذار بر نگرش مثبت نسبت به ازدواج در فضای مجازی است و به طور کلی تحولات فکری و ارزشی در رابطه با ازدواج در فضای مجازی یکی از عوامل مهم دگردیسی‌های اجتماعی در جامعه ایران است (رازقی و همکاران، ۱۳۹۶ : ۶۷). مطابق با پژوهش انجام شده توسط فلاحی (۱۳۹۵) تحت عنوان «تحلیل کیفی و کمی تأثیر شبکه‌های اجتماعی مجازی در ساختار خانواده» که با روش تحقیق تلفیقی (کمی - کیفی) انجام شده است، یافته‌ها نشان می‌دهد که حضور صرف و استفاده از این ابزار به فروپاشی خانواده منجر نمی‌شود اما شناخت، آگاهی کافی و کنترل ابعاد مختلف این پدیده می‌تواند (علاوه بر مصون ماندن از آسیب‌ها)، برخورداری از امکانات و حمایت‌های موجود را به دنبال داشته باشد (فلاحی، ۱۳۹۵ : ۱۵۱). بر اساس پژوهش انجام شده توسط عطایی (۱۳۹۴) تحت عنوان «تحلیل جامعه‌شناختی تأثیر فضای مجازی بر ارتباطات افراد در خانواده‌ها (مورد مطالعه: شهر اصفهان)» که با روش پیمایشی انجام شده است نتایج بیانگر آن است که کمیت و کیفیت استفاده کردن از فضای مجازی بر ارتباطات شفاهی خانواده‌ها تأثیرگذار بوده است؛ به این صورت که هر چه میزان استفاده از فضای سایبر بیشتر باشد، کیفیت و کمیت ارتباط و گفتمان شفاهی که ناشی از ارتباط رو در رو افراد در جهان حقیقی است، کاهش می‌یابد (عطایی، ۱۳۹۴). چنین به نظر می‌رسد که با توجه به گستره‌ی تأثیرگذاری و پیامدهای فضای سایبر و افزایش تعداد کاربران آن در سال‌های اخیر توجه به آسیب‌شناسی فضای سایبر در حوزه خانواده و به ویژه همسرگزینی از ابعاد گوناگون حائز اهمیت است که در این پژوهش مورد بررسی قرار می‌گیرد.

### ۳ فضای سایبر و آسیب‌شناسی آن

ویلیام گیبسون، نویسنده‌ی داستان‌های تخیلی و علمی، نخستین کسی است که واژه‌ی فضای سایبر را در سال ۱۹۸۱ به کار برد؛ بدین صورت که منظور او از این اصطلاح توصیف جهانی جدید بود که ماهیتی مجازی داشت (کلاهی و مباحثی، ۱۳۸۶: ۳۳). چنین به نظر می‌رسد که فضای سایبر به عنوان ابزاری که در دسترس تعداد قابل توجهی از افراد جامعه است، صرف نظر از مزایایی که دارد، چالش‌ها و آسیب‌هایی را هم به همراه داشته که برطرف نمودن این آسیب‌ها نیازمند اقدامات موثر می‌باشد که این آسیب‌ها عبارتند از: آسیب‌های جسمانی همچون ناینتدینت و غشاءوتری، برانگیختگی فیزیولوژیکی و تغییر الگوی خواب (شاملی، ۱۳۹۶: ۱۶-۱۷)، آسیب‌های خانوادگی مانند کاهش تعاملات خانوادگی، تغییر الگوی تعاملی میان والدین و فرزندان، توزیع نامتوازن و عدم تعادل در توزیع قدرت در خانواده، شکاف بین نسلی و ... (عسگری، ۱۳۹۸: ۸-۹)، آسیب‌های فرهنگی، اجتماعی و اخلاقی همچون دسترسی سهل و سریع به مطالب و منابع غیراخلاقی، بروز انحرافات جنسی و اخلاقی، تضاد ارزش‌ها، تضعیف باورها و ارزش‌های دینی و القاء شبهات دینی - فکری، کمرنگ شدن ارزش‌های فرهنگی - دینی، ترویج سطحی‌نگری در جامعه، ایجاد سردرگمی، گسترش اباحه‌گری عملی، گسترش تولیدات فرهنگی فرهنگ‌های منحط و مخرب (عسگری، ۱۳۹۸: ۱۰-۱۱) و ترویج سبک زندگی غربی (سیاح طاهری و همکاران، ۱۳۹۵: ۹۳)، آسیب‌های فردی - روانی مانند افسردگی، انزوای طلبی، بحران هویت، اختلال در شکل‌گیری شخصیت، اعتیاد به اینترنت و ... (عسگری، ۱۳۹۸: ۸-۶).

#### ۱.۳ مؤلفه‌های همسرگزینی و آسیب‌شناسی فضای سایبر در این حوزه

ازدواج یکی از مهم‌ترین تصمیمات هر شخص بالغ بوده و این امر با سایر جنبه‌های اساسی زندگی او در ارتباط است و احساس خوشبختی، رضایت از زندگی زناشویی و پایداری در ازدواج می‌تواند بر سلامت روان فرد و جامعه تأثیر گذارد (مطلق، ۱۳۹۵: ۴)؛ اما معیارهای همسرگزینی در جوامع و فرهنگ‌های گوناگون متفاوت می‌باشند و عوامل گوناگون بیولوژیکی - زیستی، جسمانی، روانی، اجتماعی، آموزشی - تحصیلی، فرهنگی، دینی - مذهبی و ... در آن دخیل هستند (نیازی و همکاران، ۱۳۹۸: ۱۲۴). در همین راستا در پژوهش‌های مختلفی که در حوزه انتخاب همسر صورت گرفته است مجموعه‌ای از عوامل و سرفصل‌ها به‌منظور تدوین الگوی همسرگزینی در جامعه ایرانی معرفی شده است که به شرح ذیل می‌باشد:

ملاک‌های دینی شامل تقیّدات دینی و اعتقادی، نجابت، عفت، پاکدامنی، تناسب و توافق دینی و اعتقادی، اشتراک در دین و مذهب؛ ملاک‌های اخلاقی شامل قناعت، خوش‌اخلاقی، حسن رفتار، سازگاری و توافق، پایبندی به کانون خانواده، صداقت در گفتار و عمل، تعهد و وفاداری، قدرت درک و تفاهم فکری، احترام به خانواده‌ها، صمیمیت، اعتماد به طرف مقابل، نبود ازدواج قبلی، ملاک‌های روحی - روانی شامل سلامت روحی - روانی و فکری، ارضای نیازهای روانی و عاطفی، عشق، مودت، محبت، رشد و بلوغ فکری و عاطفی، وجود ارتباط حسی و عاطفی، تشابه و تناسب در علایق و طرز تفکر، اعتقاد به تأثیر حفاظتی ازدواج بر انسان‌ها، امید به زندگی، ملاک‌های فرهنگی - اجتماعی شامل تحصیلات، پایبندی به ارزش‌های سنتی، تعاملات مثبت

اجتماعی، تناسب در موقعیت اجتماعی، اهل معاشرت بودن و حضور در اجتماع داشتن، تشابه و تناسب در ارزش‌های اجتماعی و فرهنگی، تشابه در قومیت، وجود زبان مشترک، داشتن مهارت‌های ارتباطی و اجتماعی، موقعیت اجتماعی و اقتصادی مناسب، آگاهی و شناخت مسائل و مسئولیت‌های زندگی زناشویی، ملاک‌های اقتصادی شامل ثروت و توانایی اقتصادی، شغل و درآمد کافی، منزلت و جایگاه شغلی پدر، استقلال اقتصادی و مالی، تناسب مالی و اقتصادی خانواده‌ها، تهیه جهیزیه، مهریه، ملاک‌های فردی شامل خصوصیت فردی و رفتاری، قدرت تصمیم‌گیری، فن بیان، استقلال فکری و تصمیم‌گیری، اختلاف سنی زوجین، اعتماد به نفس، قدرت تعقل و پختگی، باهوش بودن، تناسب ظاهری، خانه‌داری، شجاعت، مسئولیت‌پذیری، تشابه در رفتار و عادات، نحوه انتخاب همسر (شخص انتخاب کند، خانواده‌اش انتخاب کنند و یا اینکه دوستان و اطرافیان انتخاب کنند)، تناسب و تشابه در علایق، ملاک‌های خانوادگی شامل پیوند و ارتباط خویشاوندی، نظر و دیدگاه خانواده‌ی همسر، تناسب و تشابه فرهنگی - تحصیلی خانواده‌ها، اصالت خانوادگی، رضایتمندی خانواده‌ها، معاشرت و تعامل با خانواده‌ها، ملاک‌های جنسی و جسمی شامل سلامت جسمی و ظاهری، جذابیت ظاهری و فیزیکی، فقدان نقص عضو و بیماری ژنتیکی، پیراستگی و پاکیزگی، فقدان رابطه جنسی قبلی، رشد و بلوغ جسمی و جنسی، تناسب ظاهری و شکلی (نیازی و همکاران، ۱۳۹۸: ۱۳۶ - ۱۳۵).

در مجموع به دلیل اینکه ازدواج پایه و مبنای تشکیل خانواده است (نیازی و همکاران، ۱۳۹۸: ۱۳۸) و امروزه به دلیل تحولات روزافزونی که در جوامع بشری در حال وقوع است، زنان، مردان، نهاد خانواده، نحوه تشکیل آن و به طور خاص معیارها و الگوهای همسرگزینی هم تحت تأثیر قرار گرفته‌اند (نیازی و همکاران، ۱۳۹۸: ۱۳۸). به عبارت دیگر چنین به نظر می‌رسد که فضای مجازی هم یکی از عواملی است که سبب تحولات عمیق در سطوح گوناگون جامعه شده است؛ بدین صورت که با توجه به گسترش و ضریب نفوذ فضای سایبر در جهان و به‌ویژه ایران، نهاد خانواده و مقوله انتخاب همسر هم جزء مواردی است که در ابعاد گوناگون امکان تأثیرپذیری از فضای مجازی را دارد؛ بدین شکل که فضای مجازی می‌تواند از طریق اموری همچون رواج کمال‌گرایی در حوزه ازدواج و همسرگزینی، تصویرسازی و الگوسازی از نوعی همسر ایده‌آل که در عالم واقع غیرقابل دستیابی است، بالابردن سطح توقعات و انتظارات جوانان از همسر آینده به‌ویژه در بعد ظاهری، اشاعه تبلیغات گسترده متباین با ارزش‌های ایرانی - اسلامی در حوزه انتخاب همسر و مسائل مرتبط با آن، ترویج چشم و هم‌چشمی به واسطه به‌نمایش گذاشتن سبک زندگی، مراسم ازدواج و جهیزیه لوکس و تجملاتی و به‌دنبال آن کاهش تمایل سایر جوانان به ازدواج به‌دلیل عدم توانایی در فراهم‌نمودن چنین امکاناتی، رواج انحرافات اخلاقی و جنسی و عادی‌سازی مسائلی همچون همجنس‌گرایی و بی‌قیدی جنسی، تشویق جوانان به ازدواج سفید یا همباشی، تولید محتواهای مبتذل و نافی ارزش‌های دینی - اخلاقی و به‌دنبال آن اشاعه فحشا، عادی‌سازی تجرد دائمی و عدم ازدواج و تشکیل خانواده، تا حد قابل توجهی بر مقوله همسرگزینی و ایجاد تحولات فکری عمیقی در جوانان تأثیرگذار ظاهر شود که ماحصل آن، افزایش سن ازدواج، کاهش تمایل به ازدواج و اقدام به تجرد دائمی و یا ازدواج سفید، همسرگزینی و ازدواج بر پایه‌ی معیارهای نادرست و غیرواقعی و در نهایت دامن‌زدن به آسیب اجتماعی طلاق است.

## ۴ آسیب‌شناسی فضای سایبر در حوزه خانواده

یکی از عوامل تأثیرگذار بر تحولات خانواده، پدیدارشدن فناوری های نوین اطلاعاتی و ارتباطی و به طور خاص فضای سایبر می باشد که منجر به اختلال در بعضی از کارکردهای خانواده شده است (رحیمی و همکاران، ۱۳۹۶: ۱۴۵) و نسل جدیدی از تعاملات اجتماعی را به وجود آورده است (امانی، ۱۳۹۶: ۹۱). به عبارت دیگر با دیجیتالی شدن جامعه و رشد روزافزون تکنولوژی های نوپدید و رسانه های نوظهور خانواده هم در حال تحول است (خجیر، ۱۳۹۶: ۱۱۱) و فضای مجازی به عنوان ابزاری تأثیرگذار آثار نامطلوبی را هم در مناسبات اعضای خانواده به جای گذاشته است. برای مثال در سطح روابط زناشویی زوجین آثار نامطلوبی از قبیل ناپایداری ازدواج، افزایش تنوع طلبی جنسی در مردان، تغییر الگوی همسرگزینی، فقدان مهارت کافی برای ازدواج (سمیعیانی و خشکه، ۱۳۹۴: ۱۲۵)، نارضایتی های خانوادگی و زناشویی در بعد عاطفی، روانی و جنسی (زینلی پور، ۱۳۹۸: ۷۵)، دنبال کردن اهداف و محتواهایی که منجر به تشدید مشکلات زناشویی می شود (اسکندری و درودی، ۱۳۹۵: ۱۸) را داشته و از طرف دیگر، چون نوجوانان و جوانان هم زمان قابل توجهی از اوقات فراغتشان را به حضور در شبکه های اجتماعی مجازی اختصاص می دهند (فرزانه و فلاحتی، ۱۳۹۴: ۳)، رشد و توسعه فضای سایبر در مناسبات آنها با یکدیگر و تعاملاتشان با والدین تحولاتی را ایجاد کرده است؛ از جمله عدم توانایی و دانش کافی والدین در آموزش دادن استفاده از این ابزار به فرزندانشان، کاهش تعاملات والدین و فرزندان، افزایش تعاملات دختران و پسران، بالا رفتن سن ازدواج (سمیعیانی و خشکه، ۱۳۹۴: ۱۲۵)، اعتماد به اینترنت و بروز افت تحصیلی (زینلی پور، ۱۳۹۸: ۷۶)، رشد تعاملات و ارتباطات نامتعارف میان جوانان (زینلی پور، ۱۳۹۸: ۷۹)، سوء استفاده جنسی (زینلی پور، ۱۳۹۸: ۸۰)، بلوغ زودرس. از این رو می توان چنین استنباط کرد که حضور فضای مجازی در خانواده ها گاه پیامدهای نامطلوبی را به دنبال داشته که اگر زوجین مهارت، دانش و هوشمندی کافی در مواجهه با این ابزار را نداشته باشند، نه تنها روابط زناشویی خود را در معرض خطر خواهند دید، بلکه فرزندانشان هم از آسیب های این تکنولوژی در امان نخواهند ماند.

## ۵ نتیجه گیری

در مجموع چنین به نظر می رسد که فضای سایبر با استفاده از فرمت ظاهری و ساختاری جذاب، مضامین و محتواهای جدید و بدون سانسور، تبلیغات و تصاویر متنوع توانسته افراد بسیاری را در رده های سنی مختلف تحت تأثیر خود قرار دهد. به همین منظور برای مقابله با آثار و پیامدهای نامناسب و زیانبار آن، باید با استفاده از رسانه های جمعی با رعایت حدود و موازین عرفی - دینی به آگاه سازی و روشنگری مردم پرداخته شود و نوعی سواد رسانه در میان تمام افراد جامعه ایجاد شود؛ زیرا به نظر می رسد که نسل گذشته به دلیل اینکه از ابتدا با این پدیده نوظهور مواجه نبوده است، گاه یا آن را به طور کامل رد می کند و یا اینکه چون دانش مرتبط با فضای سایبر و رسانه را ندارد فرزندان خود را به خصوص کودکان و نوجوانان را بدون هیچگونه نظارت مستمر و اعتدال گونه ای در این فضا رها می کند که در نتیجه فرزندان هم به آسانی به محتواهای نامناسب دست می یابند که این امر ممکن است به بلوغ زودرس و یا سوء استفاده عاطفی - جنسی از آنها ختم شود؛

بنابراین به والدین توصیه می‌شود که ابتدا این مسئله را مد نظر قرار دهند که استفاده از فضای سایبر در عصر حاضر امری اجتناب‌ناپذیر است؛ اما برای حضور فرزندان خود محدودیت‌ها و نظارت‌های اعتدال‌گونه‌ی مستمری را تعریف کنند و در مقابل هم جوانان می‌بایست برای ورود به فضای مجازی و استفاده از آن یکسری پیش‌فرض‌ها را رعایت کنند از جمله اینکه: میزان استفاده خود از فضای سایبر را مدیریت کنند، به نکته توجه کنند که حضور در کدام یک از زیرمجموعه‌های فضای مجازی و به طور خاص شبکه‌های اجتماعی، برای آنها لازم و کاربردی است؟ آیا برای استفاده از این تکنولوژی آگاهی و دانش کافی را دارند؟ اگر پاسخ خیر است در یادگیری و کسب دانش در این حوزه تلاش کنند، آیا توانایی تمیزدادن اخبار و اطلاعات صحیح از شایعه را دارند؟ آیا توانایی این را دارند که به طور کامل تحت تأثیر فضای مجازی و حواشی مرتبط با آن قرار نگیرند؟ و ... که در نهایت به نظر می‌رسد که اگر هر یک از حوزه‌های مرتبط با آموزش کودکان، نوجوانان و جوانان یعنی خانواده، مدرسه، دانشگاه، رسانه ملی و ... رسالت و وظیفه خود را در حوزه پیشگیری از آسیب‌های فضای سایبر و آگاه‌سازی آنان انجام دهد، میزان اثرپذیری قابل توجه این قشر از جامعه از فضای مجازی محدودتر خواهد شد و آنها با بینش و بصیرت کافی وارد این فضا می‌شوند و به تمامی اطلاعات موجود در آن به آسانی اطمینان نمی‌کنند و از همه مهم‌تر تحت تأثیر تبلیغات کاذب و تفکرات تبلیغ‌شده توسط آن در خصوص ارائه مدل‌های نامطلوبی همچون ازدواج سفید و تغییر در معیارهای همسرگزینی قرار نمی‌گیرند که این امر می‌تواند از بروز آسیب‌های اجتماعی دیگری همچون طلاق، انتخاب مجرد دائمی، ازدواج سفید، اجتناب از فرزندآوری و روی آوردن به نگهداری از حیوانات خانگی، ایجاد حس افسردگی به دلیل عدم تطابق داشتن وضعیت ظاهری - فردی و اقتصادی - خانوادگی با الگوهای معرفی‌شده توسط فضای مجازی پیشگیری کند. به همین منظور لازم است که خانواده‌ها و مسئولین مربوطه با استفاده از روش‌های مختلف همچون سیاست‌گذاری‌های هدفمند، اقدامات راهبردی در حوزه آموزش و پرورش و آموزش عالی، افزایش تعداد پژوهش‌های کاربردی و نیز تولیدات رسانه‌ای تأثیرگذار و جذاب در صدد آگاه‌سازی نوجوانان و جوانان در خصوص استفاده از فضای مجازی و کاهش میزان اثرپذیری از آن برآیند.

## مراجع

- [۱] نصیری‌پور، معصومه، «شبکه‌های اجتماعی آنلاین و وفاداری افراد متاهل»، فصلنامه مطالعات رسانه‌های جدید، ۱۳۹۸.
- [۲] کنعانی، محمدامین، محمدزاده، حمیده، محمدزاده، فاطمه، «بررسی رابطه‌ی استفاده از اینترنت با نگرش به دوستی اینترنتی با جنس مخالف (مطالعه‌ی موردی دانشجویان دانشگاه گیلان)»، فصلنامه تحقیقات فرهنگی ایران، ۱۳۹۳.
- [۳] مهدی‌پور، فرشاد، «مجازی شدن آسیب‌های اجتماعی؛ مسئله‌ها و راه‌حل‌های سیاستی»، دو فصلنامه علمی پژوهشی دین و سیاست فرهنگی، ۱۳۹۷.
- [۴] صادقی، علی، عامری، زینب، «شبکه‌های اجتماعی مجازی و آسیب‌های اجتماعی مطالعه موردی: امنیت عمومی»، پویا در آموزش علوم انسانی، ۱۳۹۵.
- [۵] شاملی، علی‌اکبر، «آسیب‌های فردی فضای مجازی از منظر اخلاق اسلامی»، فصلنامه علمی - ترویجی در حوزه اخلاق، ۱۳۹۶.



- [۶] شاه‌محمدی، غلامرضا، «راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی»، فصلنامه مطالعات راهبرد ناجا، ۱۳۹۵.
- [۷] رونقی، مرضیه، «آسیب‌شناسی فضای مجازی»، کنفرانس پژوهش‌های نوین ایران و جهان در روانشناسی و علوم تربیتی، حقوق و علوم اجتماعی، ۱۳۹۶.
- [۸] خوش‌صفا، حسن، کفاشی، مجید، «بررسی رابطه شبکه‌های اجتماعی مجازی و ارزش‌های خانواده»، فصلنامه راهبرد اجتماعی فرهنگی، ۱۳۹۶.
- [۹] یوسفی، سهیل، افتخاری، علی، «تأثیر فضای مجازی بر میزان بزهکاری جوانان»، کنفرانس ملی دستاوردهای نوین جهان در تعلیم و تربیت، روانشناسی، حقوق و مطالعات فرهنگی - اجتماعی، ۱۳۹۷.
- [۱۰] شیخ‌انصاری، مهین، «جامعه ایرانی و فضای مجازی تحلیل ثانویه تحقیقات علوم اجتماعی در حوزه فضای مجازی»، مجله جامعه‌شناسی ایران، ۱۴۰۰.
- [۱۱] حسن‌پور، عبدالکریم، «تعارضات کاربری فضای مجازی با سبک زندگی اسلامی (با تأکید بر جایگاه زمان، خانواده و روابط اجتماعی)»، نشریه Pure Life، ۱۳۹۸.
- [۱۲] احمدی، حبیب، منصوری، فردین، شاه‌چراغ، علی، «بررسی ابعاد آسیب‌زای استفاده از شبکه‌های اجتماعی مجازی در میان جوانان شهر کرمانشاه»، دو فصلنامه مشارکت و توسعه اجتماعی، ۱۳۹۵.
- [۱۳] بختیاری، آمنه، «بررسی هنجارهای اخلاقی در فضای مجازی (اینترنت)»، مطالعات رسانه‌ای، ۱۳۹۱.
- [۱۴] رضوانی، امین، پریش، فریدون، «مروری بر آسیب‌های فضای مجازی، اینترنت و شبکه‌های اجتماعی بر روابط خانواده‌ها در پژوهش‌های خارج از کشور»، دو فصلنامه علمی - تخصصی مطالعات هنر و رسانه، ۱۴۰۰.
- [۱۵] اسماعیلی، مژگان، سیدی، نرگس، رستمی، فضا، «فضای مجازی و تأثیرات آن بر خانواده»، بهروز، ۱۳۹۸.
- [۱۶] عسگری، عشرت، «آسیب‌شناسی فضای مجازی در تعلیم و تربیت کودکان و نوجوانان»، سومین همایش ملی روانشناسی، تعلیم و تربیت و سبک زندگی، ۱۳۹۸.
- [۱۷] زینلی‌پور، فاطمه، «تأثیر فضای مجازی بر خانواده و جوانان (آسیب‌ها و راهکارها)»، نشریه Pure Life، ۱۳۹۸.
- [۱۸] نیک‌بخش، بهرام، «بررسی شبکه‌های اجتماعی در فضای مجازی به‌عنوان یک پدیده اجتماعی نوپدید و تأثیر آن بر کانون خانواده (مطالعه موردی: منطقه هشت شهرستان اهواز)»، فصلنامه علمی - ترویجی جامعه، فرهنگ و رسانه، ۱۳۹۷.
- [۱۹] رازقی، نادر، علیزاده، مهدی، محمدی سنگ چشمه، سمیه، «بررسی جامعه‌شناختی نگرش جوانان نسبت به ازدواج در فضای مجازی»، جامعه‌شناسی کاربردی، ۱۳۹۶.
- [۲۰] فلاحی، علی، «تحلیل کیفی و کمی تأثیر شبکه‌های اجتماعی مجازی در ساختار خانواده»، فصلنامه فرهنگی - تربیتی زنان و خانواده، ۱۳۹۵.
- [۲۱] عطایی، پری، «تحلیل جامعه‌شناختی تأثیر فضای مجازی بر ارتباطات افراد در خانواده‌ها (مورد مطالعه: شهر اصفهان)»، دومین کنفرانس بین‌المللی علوم رفتاری و مطالعات اجتماعی، ۱۳۹۴.
- [۲۲] جوادی، محسن، «پژوهشنامه اخلاق و فناوری اطلاعات»، تهران: پژوهشگاه فرهنگ، هنر و ارتباطات وزارت فرهنگ و ارشاد اسلامی، ۱۳۸۶.
- [۲۳] سیاح طاهری، محمدحسین، چینی‌فروشان، مسعود، محمدزاده، ندا، طاهری، محمدرضا، عامل نیک، فاطمه، نصر هرنندی، محمدمهدی، زارع میرک‌آباد، محمدسجاد، موحد، نعیمه، «حقیقت مجازی (درباره فضای مجازی چه بدانیم و چه بگوئیم)»، تهران: مرکز ملی فضای مجازی، ۱۳۹۵.
- [۲۴] کیاسالار، محمد، شرافتی، سمیه، مطلق، محمداسماعیل، رفیعی فر، شهرام، اسلامی، محمد، «ازدواج + ۱۸: ۱۸ سؤال و جواب درباره رابطه ازدواج و سلامت»، تهران: جوان، ۱۳۹۵.



- [۲۵] نیازی، محسن، میری، سمیه، فرهادیان، علی، «طراحی الگوی معیارهای همسرگزینی در جامعه ایران»، فصلنامه فرهنگی - تربیتی زنان و خانواده، ۱۳۹۸.
- [۲۶] رحیمی، محمد، شکریگی، عالییه، ساروخانی، باقر، حضرتی صومعه، زهرا، «بررسی جامعه‌شناختی رابطه شبکه‌های اجتماعی و تغییرات جاری در خانواده‌ها»، پژوهشنامه اسلام زنان و خانواده، ۱۳۹۶.
- [۲۷] امانی کلاریجانی، امرالله، «فضای مجازی و واکاوی سیاست‌های پیشگیرانه در کنترل آسیب‌های اجتماعی نوپدید»، نشریه علمی، تخصصی رهیافت پیشگیری، ۱۳۹۶.
- [۲۸] خجیر، یوسف، «آسیب‌شناسی استفاده از شبکه‌های اجتماعی و نرم افزارهای تلفن همراه در خانواده‌ی ایرانی (با تأکید بر نقاط قوت، ضعف، فرصت و تهدید)»، فصلنامه شورای فرهنگی اجتماعی زنان و خانواده، ۱۳۹۶.
- [۲۹] سمیعانی، محمد، حاجی محمد جواد خشکه، حمید رضا، «تبیین فرصت‌ها، چالش‌ها و کارکردهای فضای مجازی در ساحت تربیت سیاسی و اجتماعی»، بصیرت و تربیت اسلامی، ۱۳۹۴.
- [۳۰] اسکندری، حسین، درودی، حمید، «بررسی ارتباط میزان استفاده و اعتیاد به شبکه‌های اجتماعی بر گرایش به طلاق و تعارضات زناشویی»، مطالعات راهبردی ورزش و جوانان، ۱۳۹۵.
- [۳۱] فرزانه، سیف‌الله، فلاحتی شهاب‌الدینی، راضیه، «بررسی عوامل اجتماعی مؤثر بر گرایش به شبکه‌های اجتماعی مجازی (مورد مطالعه: دانش‌آموزان دختر متوسطه دوره دوم شهر بابل)»، دو فصلنامه مشارکت و توسعه اجتماعی، ۱۳۹۴.



## مفهوم تغییر کارکرد تکنیک در مطالعات فضای سایبر

محمد محمدی نیا<sup>۱</sup>

دانش آموخته دکتری فلسفه غرب، گروه فلسفه، دانشگاه تهران  
و مدیر گروه مطالعات فضای سایبری در مؤسسه شناخت  
mohamadinia@ut.ac.ir

### چکیده

در این مقاله، تغییر کارکرد تکنیک ایضاح مفهومی شده و جایگاه آن در مطالعات فضای سایبری تحلیل شده است. هدف از بحث درباره این مسئله در فلسفه تکنولوژی، تمهید طرح بومی فضای سایبر بوده و در راستای دغدغه صاحب تکنیک شدن ایران به نگارش درآمده است. برای تحلیل جایگاه کارکرد تکنیک در مطالعات فضای سایبری، ابتدا انواع مطالعات در داخل و خارج ایران که فضا و فناوری سایبری را می‌پژوهد سنخ‌شناسی شده است. سپس، معنای مقصود از مطالعات سایبری بیان شده و در نهایت، دیدگاه‌های موجود درباره تبدیل کارکرد تکنیک تحلیل شده‌اند. در این اثر برای نخستین بار، به ایجاز، تغییر کارکرد از منظر فلسفه تکنولوژی ژاپنی و چینی طرح شده که می‌تواند در اندیشیدن به فضای سایبری بومی زمینه‌ساز اندیشه‌های نو باشد. نکته اساسی در تکنولوژی ژاپنی سازش و هم‌زیستی با علم و تمدن غربی است. ژاپن در عوض تقابل با غرب، مقابله مثبت را در پیش می‌گیرد و ضمن آموختن از تکنولوژی غربی، می‌کوشد از هویت ملی خود حراست کند. اما چین، پس از جنگ جهانی دوم، ذیل دیالکتیک طبیعت مارکس و انگلس فلسفه تکنولوژی خود را نهاده و تغییر کارکرد تکنیک را به معنای زدودن علم و تکنولوژی بورژوازی و تحقق علم و تکنولوژی پرولتاریا می‌فهمد.

**کلمات کلیدی:** کارکرد، مصنوع تکنیکی، فلسفه تکنولوژی، فناوری اطلاعات و ارتباطات، تکنولوژی ملی، علم بومی.

### ۱ مقدمه

هدف از مقاله حاضر این است که درباره تغییر و تبدیل کارکرد فناوری اطلاعات و ارتباطات بیندیشد و جایگاه این مفهوم در مطالعات فضای سایبر را نشان دهد. فناوری‌های اطلاعات و ارتباطات (فاوا، به اختصار) شکل کنونی زندگی را به طرز اعجاب‌آوری دگرگون می‌کنند. کارایی و دلربایی آنها این وسوسه را برای دولت‌ها و ملت‌ها پدید می‌آورد که صاحب تکنیک شوند. آنان گمان می‌کنند با صاحب شدن تازه‌ترین فاوا به آرزوهای دست‌نیافته خود می‌رسند و به قله‌ای صعود می‌کنند که بنیان‌گذاران این فناوری‌ها از پیش، فتح کرده‌اند. صاحب تکنیک شدن، چنان که نشان خواهیم داد، به این سادگی نیست.

نباید هیجان و اعجاب تکنیک ما را از تفکر بازدارد. در ایران، خواه ناخواه در معرض مرعوب و هیجانی شدن هستیم. تراحم‌ها و اضطراب‌ها بر ما تحمیل می‌شوند و تفکر در این وضعیت کار دشواری است. نزد عامه چندان پذیرفته نیست (و عامه در اینجا بسیاری از نخبگان و مسئولان امر را نیز شامل می‌شود) که بیندیشیم فاوا با حیات انسانی چه کرده، چه آرزوهایی، به چه بهایی، به بشر بخشیده و اینکه بنیان‌گذارانش اکنون در چه موقفی ایستاده‌اند. ضرورت صاحب تکنیک شدن به قدری بر ما چیره شده که ما را از تفکر درباره انتقال تکنیک به سوی مدیریت و برنامه‌ریزی شتاب‌زده‌ی این انتقال هل می‌دهد.

تفکر هرگز راه را بر مدیریت و برنامه‌ریزی نمی‌بندد. اساسا تفکر برای انسداد راه‌ها نیست. به عکس، تفکر اصیل به سوی امکان‌ها و افق‌های تازه رهنمون می‌شود. اگرچه در رهنمایی امکان‌های نو، محدودیت‌ها و شرایط نیل به مقصد را نیز نشان می‌دهد. تقصیر تفکر و گناه متفکر نیست که عدم امکان‌ها را فرا روی ما آشکار می‌کند. عقل نور می‌تاباند. به جای ستیز با تفکر و دشنام به متفکر، آنچه در تابش نور عقل بر ما آشکار می‌شود را دریابیم.

فرض مقاله حاضر این است که «صاحب فاوا شدن» را مساوی با «از آن خود کردن» این فناوری می‌گیرد و این دو امر را در پیوند با تبدیل و تغییر کارکرد فاوا می‌انگارد. پس در این نوشته به دغدغه‌ی اساسی «بومی بودن و بومی شدن تکنیک» به طور کلی می‌پردازم و این دغدغه را از دریچه مسئله‌ای در فلسفه تکنولوژی و با پرسش از نحوه تبدیل و تغییر کارکرد تکنیک پی می‌گیرم. نوآوری مقاله حاضر نیز در پرداختن به چیستی و چگونگی تبدیل کارکرد مصنوع است. چنین پرسشی تاکنون موضوع نگارش مستقلی در زبان فارسی قرار نگرفته و در زبان‌های غیرفارسی اگرچه تعداد اندکی از نوشته‌ها به ماهیت مصنوع و کارکرد تکنیکی پرداخته‌اند.<sup>۱</sup>

چرا تأمل نظری درباره‌ی فضای سایبری مهم است؟ فن و فرهنگ بر هم تأثیر متقابل می‌گذارند. صنعت چاپ سرنوشت جنبش رفرم دینی در اروپا را تغییر داد. انقلاب‌های جامعه اروپایی با تحول در علم و فن در عصر روشنگری گره خورده و اکنون جهانی شدن بدون گسترش جهانی فاوا (فناوری اطلاعات و ارتباطات) قابل تصور نیست. ایران معاصر همگام با تحولات علمی و فنی اروپا سیر نکرده است. چرایی سیر ناقص و ضعیف

<sup>۱</sup> برخی از آثار برجسته در این زمینه عبارتند از:

- Andre Ariew (2002). *Functions: New Essays in the Philosophy of Psychology and Biology*, Oxford University Press.
- Holm, S. (2016). The Problem of Phantom Functions. *Erkenntnis*, 82(1).
- Houkes, W., and Vermaas, P. (2004). Actions Versus Functions. *Monist*, 87(1), 52-71.
- KITCHER, P. (1993). Function and Design. *Midwest Studies in Philosophy*, 18(1), 379-397.
- Neander, K. (1991). The teleological notion of function. *Australasian Journal of Philosophy*, 69(4), 454-468.
- Preston Beth (1998). Why is a Wing Like a Spoon A Pluralist Theory of Function.
- Preston Beth (2003) Of marigold beer A reply to Vermaas and Houkes.
- Schwartz, S. P. (1978). Putnam on Artifacts. *The Philosophical Review*, 87(4), 566-574.
- Verbeek, Peter-Paul (2005). *What Things Do: Philosophical Reflections On Technology, Agency, And Design*-Pennsylvania State University Press.
- Vermaas and Houkes (2003). Ascribing Functions to Technical Artefacts A Challenge to Etiological Accounts of Functions.

ما در ایران پرسش مهمی است و دشوارتر این پرسش است که آیا ملتی بدون تکمیل سیر خود در علم و تکنولوژی جدید می‌تواند از لبه علم و تکنولوژی در فضای سایبری آغاز کند و خود را به پیشگامان این عرصه برساند. در هر حال، دریافت این نکته پیچیده نیست که زمانه‌ی ما با فضای سایبری عجین شده است. پس فهم اکنون و آینده‌ی ما بدون فهم و تفسیر این فضا میسر نیست. ما فضای سایبری را می‌کاویم تا دریابیم که کجا هستیم و به کجا خواهیم رفت.

برخی مدعی‌اند که شواهدی بر اختلال مواجهه ما با تکنولوژی از جهت اجتماعی شدن وجود دارد؛ تکنولوژی بر وجود ما عارض شده و عاریتی بوده است، جزو عمل و تجربه درونی جامعه نبوده است؛ از این رو برخوردی آشفته و آنومیک با آن کرده‌ایم (فراستخواه، ۱۳۹۶: ۲۰۳). شواهد مورد ادعا از غربت کار دستی و هنرستان در نظام آموزشی ما شروع می‌شود، تا چرخه‌ی کور آزمایش و تشخیص به وسیله‌ی تکنولوژی‌های تصویربرداری ام‌آرآی و سی‌تی‌اسکن ادامه پیدا می‌کند و سرانجام به پدیده‌ی عارضی و دفعی اینترنت و تلفن همراه می‌رسد که بدون طی فرایندهای درون‌زا یکباره به درون‌شان پرتاب شدیم و نمی‌دانیم با آنها چگونه رفتار کنیم (همان: ۲۰۰-۲۰۲). این وضع مسبوق به سابقه‌ای تاریخی بوده و در تناسب با مواجهه ما با مظاهر تمدن جدید در دوره قاجار است.

در پایان باید پرسید که شیوه‌ی پرداختن به مسئله پژوهش چگونه است و فلسفه در خصوص کارکرد تکنیک چه می‌کند؟ سخن فلسفی درباره تکنولوژی ذیل یکی از کنش‌های عقلی زیر می‌گنجد: طرح پرسش (که شامل اصلاح پرسش‌های نادرست نیز می‌شود)، ایضاح مفهومی و درک شیوه‌ی اندیشیدن به فاوا.

## ۲ چه سنخ مطالعات در داخل و خارج ایران، فضا و فناوری سایبری را می‌پژوهد؟

سنخ‌شناسی (typology) مطالعات فضای سایبری کار مستقل و پرحجمی است. بررسی سنخ‌های داخلی و خارجی این مطالعات نیز بسیار گسترده است. بنابراین هدف از این بخش، ارائه گزارشی مجمل از آن برای بیان تمایز کار ما است.

ملاک‌های متفاوتی در دسته‌بندی وجود دارند. رویکردهای فلسفی، الهیاتی، اجتماعی و راهبردی گونه‌های مختلفی از مطالعات این فضا را شکل می‌دهند. در این میان، مطالعات اجتماعی فربه‌تر بوده و در سراسر دنیا آثار بیشتری را به نگارش درآورده است. بهزاد دوران در سنخ‌شناسی مطالعات اجتماعی فناوری بیان می‌کند که در ایران، فاوا بسیار بیش از دیگر فناوری‌های موجود، موضوع مطالعه و بررسی قرار گرفته است؛ زیرا «اولا به سرعت مرزها را درنوردیده و همه‌ی عرصه را در بر گرفته است، ثانيا برخلاف دیگر فناوری‌های سطح بالا، با کمترین تأخیر وارد جامعه شده و به سهولت در دسترس همگان قرار گرفته و ثالثا از مراحل آزمایشگاهی فرارفته و به شکل تجاری به بازار عرضه شده است (دوران، ۱۳۹۶: ۲۲۶)».

ملاک‌های متفاوتی می‌توانند مطالعات اجتماعی فاوا را سنخ‌شناسی کنند. توکل و مهدی‌زاده، به سه دسته‌ی کلی اشاره می‌کنند: ۱. آثار فناوری بر جامعه، همانند آثار اقتصادی، فرهنگی و سیاسی تکنولوژی ارتباطات بر جامعه ۲. آثار جامعه بر مسیر، شدت و میزان نوآوری تکنولوژیک، همانند تأثیرپذیری ابداعات

فنی تلفن همراه از جامعه ۳. مطالعه فناوری به مثابه پدیده‌ی اجتماعی، همانند بررسی پدیداری فرم، محتوا، رویه‌ها، فعالیت‌ها و مصنوعات تکنولوژیک (مهدی زاده و توکل، ۱۳۸۶: ۸۸).

بهزاد دوران چند دسته‌بندی دیگر نیز برمی‌شمارد:

۱. تقسیم رایج به فناوری مادی و فناوری اجتماعی،
۲. تقسیم بر اساس سطح پیچیدگی (سطح بالا، متوسط و پایین)،
۳. بر حسب چرخه‌ی عمر (۱-۳) نوپدید، ۲-۳ در حال اشاعه، ۳-۳ اشباع‌شده و رو به افول و ۳-۴ متروک)،
۴. تقسیم جغرافیایی بر حسب منشأ فناوری به مطالعه آن در جامعه مولد و جامعه واردکننده،
۵. تقسیم جغرافیایی بر مبنای سطح مطالعه (۵-۱ جهانی و بین‌المللی، ۵-۲ ملی، ۵-۳ مادون ملی)
۶. تقسیم به اینکه ۱-۶ آثار فناوری بر جامعه مطالعه می‌شود یا ۲-۶ آثار جامعه بر فناوری یا ۳-۶ فناوری به مثابه پدیده‌ی اجتماعی
۷. تقسیم بر حسب قبول و پاگرفتن فناوری یا ضدیت با آن

بنابر گزارش دوران، وضعیت کنونی مطالعات فاوا در کشور «به‌شکل نامتقارنی عمدتاً بر فناوری‌های مادی، متوسط، در حال اشاعه، در جامعه گیرنده و واردکننده فناوری، در سطح مادون ملی و از سنخ بررسی آثار فناوری بر جامعه متمرکز است» (همان: ۲۲۲).

با تحلیل منابع سایبری پژوهی، ملاک دیگری برای دسته‌بندی مطالعات می‌توان ارائه کرد: تقسیم بر اساس دیسیپلین‌ها (جامعه‌شناسانه، روان‌شناسانه، سیاست‌گذارانه و...) یا تقسیم بر اساس موضوعات (تلفن همراه، اینترنت، شبکه‌های اجتماعی و...).

گونه‌ای از مطالعات فضای سایبری با رویکرد فلسفی به تحلیل سرشت و ماهیت آن به عنوان یک پدیده پرداخته و به نوعی، موضوع را برای سنخ‌های دیگر اثبات می‌کند. کسانی چون یوست ون لون ضعف مباحث تکنولوژی رسانه‌ای را به ضعف در تفکر فلسفی درباره‌ی ماهیت رسانه و پدیده‌شناسی برمی‌گردانند. به زعم آنان، گرایش اصلی در پژوهش‌های رسانه و فضای سایبری به پنج سنخ تقسیم می‌شود که از این اقسام، پدیده‌شناسی و ماهیت‌شناسی فلسفی در انزوا و اقلیت است (ون لون، ۱۳۹۱: ۱۳):

۱. پیامدکاوی و تأثیرگرایی
۲. محتواکاوی یا محتواگرایی
۳. متن‌گرایی و مطالعه بافت و سیاق اجتماعی



۴. کاربردشناسی

۵. پدیده‌شناسی

### ۳ معنای «مطالعات فضای سایبری»

اصطلاح مطالعات فضای سایبری عمر چندانی نداشته و کاربردهای یکسانی نیز ندارد. پس لازم است که مقصود خود از به کار بردن این اصطلاح را روشن کنیم. برخی از کاربردهای معمول به شرح زیر است: (۱) دستاوردهای میان‌رشته‌ای درباره‌ی فضای سایبری، (۲) بررسی چالش‌ها، آسیب‌ها و پیامدهای این فضا (۳) تأثیرکاوای فضای مجازی به معنای تحقیق درباره‌ی تأثیر علی یا همبستگی فضای مجازی بر/با متغیرهای دیگر.

مطالعات فضای سایبری در کاربردهای فوق را می‌توان در چهار مقوله زیرساخت، مدیریت سایبری، توسعه اقتصادی، فرهنگ سایبری دسته‌بندی کرد: (۱) ذیل «زیرساخت» به موضوعاتی مانند اینترنت اشیا/همه‌چیز (IoT/IoE) امنیت، ارتباطات سیار، آمادگی الکترونیکی (e-readiness)، پیاده‌سازی شهر هوشمند، خدمات شبکه و ... می‌پردازند. (۲) در خصوص «سیاست سایبری» به موضوعاتی چون دولت الکترونیک، برنامه‌ریزی برای هوشمندسازی، سواد الکترونیکی (e-literacy)، خدمات الکترونیک سلامت، تنظیم مقررات، مدل‌های مدیریت بحران و ... پرداخته می‌شود. (۳) با عنوان «توسعه اقتصادی» کلیدواژه‌هایی مانند استارت‌آپ‌های اینترنتی، اقتصاد نوآوری فناورانه، کارآفرینی آنلاین، یادگیری دیجیتال، تخصص هوشمند (smart specialization)، انقلاب صنعتی چهارم و ... بحث می‌شوند. (۴) ذیل «فرهنگ سایبری» موضوعاتی چون فرهنگ جدید، تعاملات انسانی آینده، جامعه دیجیتال، چالش‌های سبک زندگی آنلاین، تولید و مصرف رسانه‌های دیجیتال، آموزش و پرورش از راه دور، مدرسه‌زدایی، شهرت، جنسیت، خرده‌فرهنگ‌های مجازی، اعتیاد به اینترنت، افکار عمومی توده‌وار، سلبریتی و ... طرح می‌شوند.

دسته‌بندی فوق، کاربردهای متعدد اصطلاح مطالعات فضای سایبری را نشان می‌دهد. قصد ما در این نوشته توجه به وجهه نظری متفاوت است؛ توجه به آنچه رسالت فلسفه به معنای تفکر است. دانستن مقولات یادشده در مطالعات فضای سایبری شرط لازم است و تفکر را از انتزاعی دیدن پدیده‌هایی می‌بخشد اما کافی نیست. ادعای ما این است که اگر در آن مقولات به نصاب بالایی در تحقیق نیز برسیم، تمام حقیقت و ماهیت فضای سایبری بر ما آشکار نمی‌شود. فهم و درک حقیقت و ماهیت این فضا و عصری که ما را در آستانه‌اش قرار می‌دهد، با قدم حکمت (به معنای واسع کلمه) ممکن است. اینکه حکمت به معنای واسع کلمه، چیست و چه نسبتی با دین، الهیات و عرفان دارد، پرسش دشواری است. گویی تمام فلسفه را در این پرسش گرد آورده‌اند.

حکمت با دیگر زمینه‌های مطالعاتی درباره فضای سایبری جمع می‌شود. چنین نیست که حکیم بتواند از منبع فکری خود به تمام پاسخ‌ها در آن مقولات پاسخ دهد؛ اما می‌تواند به ما بگوید که این چه پدیده‌ای است که مظاهر، حالات و ویژگی‌هایش همه چیز را دگرگون می‌کند، ما را به کجا می‌برد، آیا با غایتش تناسب داریم، چه عالم و آدمی را شکل می‌دهد و چه موقفی در عصری داریم که ما را در آستانه‌اش قرار داده است.

تقاطع‌های میان‌رشته‌ای در این دست تأملات به طور طبیعی رخ می‌دهند؛ اما هدف ما لزوماً میان‌رشته‌ای دیدن نیست؛ بلکه هدف فهم ماهیت فضای سایبری و تقرب به واقعیت این پدیده است. تأملات بنیادین ما به ارزیابی پیامدها و تأثیرات این پدیده می‌پردازند؛ ولی در آنها متوقف نمی‌شوند. پیامدکاوی و سنجش تأثیرها را معبری به سوی اندیشیدن عمیق‌تر می‌انگارد.

پس بررسی کارکرد تکنیک در مطالعات فضای سایبری با هدف فهم ماهیت این پدیده انجام خواهد شد و به تأمل درباره رابطه تبدیل کارکرد با زیست‌بوم‌های فرهنگی مختلف خواهیم پرداخت.

## ۴ تبدیل کارکرد

وجهی از بومی‌شدن به تبدیل کارکرد مصنوع برمی‌گردد؛ بدان‌معنا که کارکرد تکنیک از آنچه در بیرون از عالم ما داشته به کارکردی متناسب با نیازها، خواسته‌ها و مقصود ما تبدیل شود. در این بخش ابتدا مفهوم پذیرفته‌شده از «کارکرد تکنیک» را تعریف کرده و سپس دیدگاه‌های رقیب درباره کارکرد را شرح می‌دهم تا بررسی کنم که تبدیل کارکرد در کدام دیدگاه قابلیت تبیینی بالاتری دارد.

کارکرد چیست؟ پاسخ بدیهی به نظر می‌رسد. مصنوع تکنیکی چه محصول نهایی و چه جزئی از محصول نهایی باشد، «برای چیزی» است و آن چیز، کارکرد مصنوع است. کارکرد در یک مصنوع آن‌قدر اساسی است که برخی تکنیک‌پژوهان مصنوعات تکنیکی را با کارکرد داشتن تعریف کرده‌اند (Hilpinen, 2008: 59). گروهی دیگر که برای مصنوع تکنیکی ماهیتی دوگانه<sup>۲</sup> قائلند و بر جنبه مادی مصنوع نیز همان‌قدر تأکید می‌کنند، کارکرد را حامل جنبه «آفرینش ذهن و ساختارهای اجتماعی» شمرده‌اند (Kroes, 2012: vii). بنابراین با هر نگاهی، کارکرد نقش تعیین‌کننده‌ای در این دارد که مصنوع چیست، چگونه به وجود می‌آید و چگونه با اشیاء فیزیکی و اجتماعی مرتبط می‌گردد.

پس ابتدا دانست کارکرد چیست؛ می‌دانیم که نیروی خلاق ذهن بر اساس غایات و ایده‌های آشکار و پنهان به طبیعت و ماده فیزیکی شکل می‌دهد و آن را به مصنوعی برای انسان تبدیل می‌کند.<sup>۳</sup> آیا قصدها و ایده‌ها در پیدایش کارکرد کافی‌اند؟ و قصدها و ایده‌ها هر کارکردی را در مواد و ساختارهای فیزیکی می‌توانند ایجاد کنند؟ از سوی دیگر، هر شیئی (خواه طبیعی، زیستی یا مصنوعی) ویژگی‌ها و صفاتی دارد. انسان در تعامل با شیء (در به‌کار بستن، مصرف و استفاده از آن) نسبتی با آن ویژگی‌ها برقرار می‌کند. این نسبت به شیء و صفاتش معنایی جدید می‌بخشد. شیء اینک کاربردها و کارکردهایی برای انسان دارد. گویی کارکرد و کاربرد اموری وابسته به انسانند و برای شیء به خودی خود (بدون فرض این نسبت) نمی‌توان این امر را در نظر گرفت.

مصنوعات تکنیکی در حیطه فاوا اشکال، اندازه‌ها و مقیاس‌های مختلفی دارند. آلیاژها، قطعه‌ها و محصولات بسیط و پیچیده‌ای که ساخته می‌شوند در یک چیز اشتراک دارند: همگی مصنوعند؛ یعنی اشیاء و سیستم‌هایی‌اند که انسان آنها را برای هدفی ساخته است (Hilpinen, 2008: 59). واقعیت‌های گوناگونی

<sup>۲</sup>The Dual Nature of Technical Artefacts

<sup>۳</sup>اگرچه هیچ جسم طبیعی در اطراف ما وجود ندارد که به سادگی با قصد ما به مصنوعات پیچیده تکنیکی تبدیل شود.

وجود دارند که ساخته‌ی انسانند. قانون، پدیده‌های اعتباری، واقعیت‌های اجتماعی، سازمان‌ها، قراردادها، شعرها نیز وابسته به جعل و انشاء انسانند؛ اما مصنوعات از «ماده و طبیعت» آغاز می‌شوند. با «تصرف و طراحی» انسانی در ماده، مصنوع متولد شده و اینک واجد «کارکرد» می‌شود. شاید بتوان گفت تکنیک مفهوم عام‌تری از مصنوع است. سیاست، قانون‌گذاری، قرارداد و مانند آنها ذیل تکنیک جای می‌گیرند اما مصنوع نیستند.

به پرسش اصلی بازمی‌گردم. انتقال فاوا چگونه رخ می‌دهد؟ استقرار امر انتقال‌یافته در عالم ما و بومی شدن آن به چه معناست؟ قوام تکنیک در وطن نخست با کارکردش در آن عالم بوده است؛ پس تبدیل کارکرد چگونه صورت می‌پذیرد؟ فرض بگیریم امر انتقال‌یافته در سه مفهوم طبقه‌بندی شود: ۱. مواد طبیعی لازم برای برپایی تکنیک (امر طبیعی) ۲. مصنوع تکنیکی ۳. مصادیقی از امر تکنیکی عام که غیر از مصنوع تکنیکی است.

فرض تبدیل کارکرد در امر طبیعی تصور ندارد. واژه‌ی کارکرد در امر طبیعی اگر درست به کار رفته باشد مورد تردید برخی تکنیک‌پژوهان است (ورماس، ۱۳۹۱: ۲۵). در ید اختیار و نیت انسان نیست. تبدیل نمی‌پذیرد، بدان معنا که تبدیل در آن وابسته به انسان باشد. جوهر و ماهیت آن تعیین می‌کند که چه صفات و ویژگی‌هایی داشته باشد. به زبان فلسفه طبیعی قدمایی، صورت نوعیه مبدأ صفات و آثار امر طبیعی است. جنس و فصل گرچه اعتبار منطقی در شیء است، اما ذهن و تحلیل عقلی مبدأ این اعتبار در جوهر و ذات شیء است. در مقابل، تکنیک به معنای عام و مصنوع تکنیکی کارکردش را از جعل و قصد و غایت انسانی می‌گیرد. انسان جنس و فصل را به تکنیک، به معنای عامش می‌بخشد. تکنیک با معنابخشی انسان جان گرفته و متولد می‌شود؛ پس تبدیل‌پذیر است و می‌توان از ماهیت تبدیل و انتقالش به این معنا سخن گفت؛ در حالی که این نحوه سخن گفتن درباره‌ی امر طبیعی موضوعاً منتفی است. به زبان معهود در فلسفه اسلامی بحث کردم؛ هرچند در پدیده‌شناسی، طبیعت و شیء طبیعی در همان قسم نخست نیز در آگاهی تقویم می‌شود.

تمایز امر طبیعی و تکنیکی در اغلب بحث‌های فلسفه اسلامی به وسیله مفهوم مرکب حقیقی و اعتباری طرح شده است. اشیای طبیعی نیز مرکب از ذرات و اجزایی هستند، اما این ترکیب صورت نوعیه جدیدی پدید آورده است. بر خلاف مرکب‌های اعتباری که ترکیب نتوانسته‌اند صورت نوعیه اجزا را زائل کنند و صورتی به شیء مرکب ببخشند که اجزا، در مقام تجزیه، به هیچ‌وجه نداشتند (ابن سینا، ۱۴۰۳: ۱، ۹۷).

به نظر می‌رسد کارکرد در این مفهوم‌پردازی غائب است. کارکرد معنای شیء مرکب است. تغییر معنا می‌تواند تغییر در ماهیت و صورت نوعیه تعبیر شود و این تعبیر گراف نیست. رایانه مجموعه‌ای از اجزایی است که در مقام تجزیه، چنین کارکردی ندارد. شاید بتوان شتاب‌زده نوشت که هر جا ترکیب به صورت «سیستم» (نظام) درآید، صورت نوعیه جدیدی در پی می‌آورد و سیستم‌ها با کارکردها از هم تمایز می‌یابند.

اما مفهوم پذیرفته‌شده از «کارکرد تکنیک» چیست؟ آیا همان «طرح کاربرد»<sup>۴</sup> است که «شیوه‌ی بهره‌برداری انسان از مصنوعات تکنیکی را در جهت دستیابی به اهداف مختلف توصیف می‌کند»؟ (ورماس، ۱۳۹۱: ۱۵) در این صورت، کارکرد به کاربرد و مسائل در کاتالوگ تقلیل می‌یابد. در نتیجه، تبدیل کارکرد تکنیک

<sup>4</sup>Use plan

به این معنا است: وسیله‌ای که در مصارف نادرست به کار می‌رود در مصارف درست و مشروع به کار رود. کاربرد و مصرف تعیین می‌کند، وسیله چه حکمی داشته باشد.

اما ورماس در شرح دیدگاه خود، لوازم و نتایج فوق را نفی می‌کند. او کارکرد را پاسخی به پرسش از «برای چیست» و کاربرد را راجع به سؤال «چطور باید به کار رود» می‌داند. جنبه اول به پرسش از هدفی مربوط می‌شود که مثلا، کامپیوتر را برای آن به خدمت گرفته‌اند و جنبه دوم به اینکه کامپیوتر چگونه به کار می‌رود و کاربر چگونه باید از آن استفاده کند. اولی کارکرد تکنیکی کامپیوتر و دومی دستورالعمل کاربرد آن است (همان: ۲۳). می‌دانیم که دو جنبه کارکرد و کاربرد مصنوع در پیوند با ساختار آن است. نحوه تشکیل و ترکیب مصنوع، آن را به کارکردها و کاربردهای متفاوتی مرتبط می‌کند.

قضاوت ورماس این است که کاربرد و مصرف مصنوع، در تحقق خارجی کارکرد آن تعیین‌کننده است. کارکرد مصنوع در ذهن و خیال سازنده به صورت هدف ظاهر شده و در استفاده و مصرف کاربر به صورت خارجی محقق می‌شود. اگر کاربر کنش‌های مشخصی مطابق دستورالعمل‌های کاربرد انجام ندهد، کارکرد آن تحقق نمی‌یابد؛ پس رشته کنش‌های هدفمند کاربر تضمین می‌کند که طرح و هدف اولیه (کارکرد) محقق شود و آن کارکرد و طرح کاربرد، از آنجا که به دست انسان طراحی و ساخته شده است، میان مصنوع تکنیکی و شیء طبیعی تمایز می‌نهد (همان: ۲۴).

در وابستگی کارکرد و کاربرد (مصرف) تردید داریم؛ اگرچه ارتباط میان آنها را انکار نمی‌کنم. لازمه دیدگاه ورماس این است که با تغییر دادن کاربرد و نحوه استفاده از مصنوع تکنیکی می‌توان از تحقق کارکرد (طرح سازنده) ممانعت کرده و کارکرد دیگری را در خارج محقق ساخت. برای مثال، پس از تقلید یا واردات ابزار دیجیتال یا خدمت اینترنتی به کشور، کاربران را به شکل دیگری از استفاده فراخوانده یا سوق می‌دهیم و با مدیریت نحوه استفاده کاربران آن ابزار یا خدمات کامیاب می‌شویم. چون کارکرد ابزار یا خدمات مذکور را به صلاح کشور ندانسته و چاره را در تغییر کاربرد آن می‌جوئیم. بدین ترتیب، واردات ابزار و خدمات سایبری به کشور یا تقلید محض آنها در ایران خللی در سیاست کلان سایبری ما ایجاد نکرده و به سهولت توانسته‌ایم دو هدف را یک‌جا نشانه روییم؛ هم از قافله تکنولوژی عقب نماندیم و هم خطرات و آسیب‌ها را دور کرده‌ایم. در صحت و اعتبار این دیدگاه تردید داریم.

با ورماس در مفهوم‌پردازی مولفه‌های مصنوع تکنیکی موافقم. او سه جنبه «کارکرد برخاسته از طراحی و تصرف انسان»، «ساختار متشکل از اجزای واقعی» و «کاربرد و دستور مصرف» را برای تمایز مصنوع تکنیکی از اشیای طبیعی (کارکرد انسان‌ساخته ندارند) و اشیای اجتماعی (ساختار به معنای یادشده ندارند) به کار می‌گیرد (همان: ۲۴). ورماس سرچشمه‌ی دیدگاه خود را ذکر نمی‌کند؛ این تقسیم‌ها ریشه در علل اربعه ارسطویی دارد. کارکرد را می‌توان معادل علت غایی و ساختار را علت مادی و صوری دانست. کاربرد را نمی‌دانم به علت غایی در ارسطو برگردانیم یا خارج از دایره علل اربعه تصورش کنیم. اینکه در آثار قدماء (چه در یونان، چه در عهد اسلامی) به اصول کلی درباره تکنیک بسنده شد، وجهی دارد. هیچ زمانی در تاریخ انسان همچون دو‌بیست سال اخیر مملو از مصنوعات و محصولات تکنیکی نبوده است. تکنیک هم‌زاد قوه خیال آدمی است؛ اما دنیایی که در آن زندگی می‌کنیم تا دو سده‌ی پیش، هرگز بدین شکل نبوده است. بنابراین تا قبل از ظهور این عالم تکنیک‌زده، قصور متفکران از تأمل درباره ظرائف و دقائق تکنیکی معقول

است.

## ۱.۴ تبدیل کارکرد در فلسفه تکنولوژی شرقی

از منظر تبدیل کارکرد تکنیک غربی، دو گول صنعتی و تکنولوژیک در شرق آسیا یعنی ژاپن و چین مورد مطالعاتی بسیار درس‌آموزی‌اند. ژاپنی‌ها نخستین کشور غیرغربی و نیز آسیایی بودند که بر مبنای علم و تکنولوژی بنای اقتصادی و صنعتی نیرومندی برپا کردند، با اینکه سنن و عادات فرهنگی در جامعه ژاپنی به طرز قابل ملاحظه‌ای از الگوهای غربی متفاوت است. چگونه کارکرد اولیه تکنیک غربی در فرایند ژاپنی شدن تغییر کرده است؟

پروفسور نقی‌زاده، استاد تمام دو گروه اقتصاد و مطالعات ژاپن در دانشگاه تهران، بر مبنای تفکر توسعه ژاپنی مسئله یادشده را چنین تبیین می‌کند: سنت همزیستی انواع مسلک‌ها از تاریخ دیرینه‌ای در این کشور برخوردار است. همانطور که تفکر چینی در دوره سلسله «تانگ» سه آیین «بودا» و «تائو» و «کنفوسیوس» را در هم آمیخت، ژاپن هم در قرن هشتم آیین «شینتو» را که دین ملی ژاپن بود به آیین بودا نزدیک کرد. اما ایزدشناسی و دینداری ژاپنی با وجود پذیرش اختلاف آیین‌های یادشده، اصل ژاپن را به الهه خورشید (Amaterasu) رسانید. پس ژاپن با اولویت‌دادن به سرزمین خویش و ژاپنی‌بودن، تفرقه را به وحدت می‌رساند. نکته دیگر به رقابت مثبت با غرب مبتنی بر ناسیونالیسم ژاپنی بازمی‌گردد. ژاپن از تجربیات غرب نه به عنوان هدف، که به عنوان وسیله در جهت رقابت و حفظ سنن فرهنگی با آن سود جست. ریشه‌ی اصلی دیسپلین اقتصادی و توسعه ژاپن، بقول «جوان رایینسون» اقتصاددان شهیر انگلیسی، در ناسیونالیسم آن نهفته است. از همین روست که ملت ژاپن به طور سنتی تعلق خاطر خاصی به سرنوشت همگانی ملی خود داشته و دائماً به بررسی خود می‌پردازد که ژاپن چیست؟ ژاپنی کیست؟ فرهنگ ژاپنی کدام است؟ و این پرسش‌ها، عناوین کتب و تحقیقاتی است که در ژاپن رواج و مشتاقان فراوانی دارد (نقی‌زاده، ۱۳۸۸: ۵۶-۵۹).

ژاپن ضمن نیاز به یادگیری از غرب و همزیستی رقابت‌آمیز با آن، تهاجم یک‌جانبه و هویتی آن را نپذیرفت. لذا ضمن آموختن از علوم و تکنولوژی و تفکرات غربی، به‌خاطر مقابله با بحران هویت ملی و حذر از شکست و حقارت صنعتی، به افزایش قدرت تولید و انگیزه‌های ملی برای دسترسی بدان پرداخت. هر چه بیشتر متفکران ژاپنی از غلبه علمی و تکنولوژی غرب آگاه می‌گردند، بیشتر به اساطیر شینتو، متون قدیمی ژاپنی و اخلاق کنفوسیوسی برای «مقابله مثبت» با تهاجم فرهنگی غرب توجه می‌کنند؛ بدین معنی که آنان از یک سو تشنه یادگیری از غرب هستند، و از سوی دیگر تمایلات وطن‌خواهانه، آنان را وادار به حفاظت از فرهنگ بومی، ضمن یادگیری صنعتی از غرب به عنوان وسیله نه هدف، می‌سازد. اگر شکست در جنگ جهانی و فرود «بمب اتم»، «تأسیسات فیزیکی» ژاپن را به تل خاکستری تبدیل کرد، ولی موفق به نابودی «روحیه سخت‌کوشی» و «تفکرات مقابله مثبت» با غرب در این کشور نشد (همان: ۶۳-۶۶). به نظر می‌رسد که علل تبدیل موفقیت‌آمیز کارکرد تکنیک در ژاپن اگر در ایران به صورت وارونه محقق شده باشد می‌تواند از تحول و پیشرفت فاوا ممانعت کند. نقطه مقابل روحیه ژاپنی، رویکرد «سوداگری»، «اکتفاکردن به مقابله منفی» با غرب، و «مصرف مستمر کالای آن» است.



با ورود به قرن بیست و یکم، رتبه اول قدرت تکنیکی و اقتصادی آسیا از ژاپن به چین منتقل می‌شود. امروزه اصطلاح «چینی‌شدن» (Sinicization) تکنولوژی از بحث‌های داغ در مطالعه فلسفی در چین است و از توجه نظری چینی‌ها به تغییر کارکرد تکنیک حکایت می‌کند (Chen and Chen, 2020: 113). فلسفه تکنولوژی چینی که از دهه ۱۹۵۰ به بعد، به تدریج شکل مدون گرفت، بر اساس «دیالکتیک طبیعت» تغییر کارکرد مصنوع تکنیکی را تبیین می‌کند. نخستین انجمن‌های علمی، نشریات پژوهشی و گروه‌های تحقیقاتی در این دوره با نام دیالکتیک طبیعت / فلسفه طبیعت بنا نهاده می‌شوند (Ibid). این نام، کارهای مارکس و انگلس در قرن نوزدهم را به یاد می‌آورد و می‌دانیم که چین از قوی‌ترین گرایش‌های چپ برخوردار است. با بازگشت محققان چینی خارج از کشور به چین، پس از جنگ جهانی دوم، آنها مایل بودند راهنمایی‌هایی برای توسعه علم و فناوری بیابند که از نظر ایدئولوژیکی با خارج از چین متفاوت باشد. بدین ترتیب، بینش‌های انگلس به عنوان مبنایی برای سیاست علمی در جمهوری خلق مورد استفاده قرار گرفت (Guo, 2014: ۱۸۳۷). مایر (Ernst Mayr)، زیست‌شناس تکاملی بعد از انتشار نتایج تحقیقاتش، به این نتیجه رسید که او در واقع طرفدار برخی اصول دیالکتیکی - ماتریالیستی مانند فرآیندی بودن، به‌هم‌پیوستگی جهانی، و تغییرات دائمی در طبیعت بوده و اظهار کرد: «ماتریالیسم دیالکتیکی برای مارکس و انگلس عبارت بود از فلسفه عمومی طبیعت. این امر در وهله اول با ازین‌بردن مکتب اصالت فیزیک (physicalism) و مکتب دکارت (Cartesianism) حاصل شد. لازم است ویژگی‌ها و اصول مختلف علوم «تک‌بعدی» مانند فیزیک و زیست‌شناسی توسعه یابد تا در نهایت یک فلسفه جامع درباره‌ی طبیعت ساخته شود که نسبت به تمامی علوم داوری منصفانه‌ای داشته باشد» (Mayr, 1997: 13).

دیالکتیک طبیعت عنوان اثری ناتمام از انگلس (۱۸۸۳) است. این اثر درباره‌ی فلسفه فناوری نیست؛ بلکه در باب فلسفه طبیعت و فلسفه علم مدرن است. طرح انگلس پلی میان ماتریالیسم و علوم طبیعی ایجاد می‌کند و آن پل، راهنما و ایدئولوژی سیاسی علم است. بنا به ایده‌ی مارکسیسم، طبیعت، جامعه و اندیشه را باید از منظر طبقاتی تحلیل و تبیین کرد. همه امور به پرولتاریا و بورژوازی تقسیم می‌شوند که هرکدام بر اساس ایدئولوژی‌شان علوم متفاوتی تولید می‌کنند. علوم بورژوازی و تکنیک برخاسته از آنها بد و اهریمنی‌اند (Foster, 2020: ۱۱). بنابراین نظام حاکم بر چین پس از جنگ دوم، مطابق با جمهوری خلق یا دموکراسی پرولتاریا باید علوم و تکنیک پرولتاریا را محقق کند؛ بدین ترتیب دیالکتیک طبیعت، به شاخه‌ی اصلی فلسفه طبیعت و فلسفه علم در دانشگاه‌های چین در این دوره مبدل می‌شود.<sup>۵</sup>

<sup>۵</sup> در میان اندیشمندان علم دینی پس از انقلاب، سیدمنیرالدین الهاشمی (جریان فرهنگستان علوم اسلامی) قرابت‌هایی با این طرز تلقی مارکسیستی از علم دارد. مفهوم طبقه در مارکسیسم مقوم هویت علم بوده و وجه جهان‌شمول، هم‌زمانی و کلی علم را انکار می‌کند. هویت کارگری علم در برابر هویت بورژوازی آن تعریف می‌شود. از یک نظر، الهاشمی هویت ایمان و کفر را در جای دوگانه مارکس و انگلس می‌نهد. حزب توده در سال‌های نخست پس از انقلاب، با قوت و گستره‌ی زیاد، مروج مبانی چپ در ایرانند. آن سال‌ها جلسه‌های نقد و مناظره علمی میان چهره‌های فاضل توده‌ای و مخالفان آن تفکر داغ است. عجیب نیست که مخالفان شاخص نگاه مارکسیستی به علم و جامعه در آن زمان (همچون آیت الله مصباح یزدی)، در دهه‌های بعدی با دیدگاه فرهنگستان درباره‌ی علم به شدت مخالفت می‌ورزند.



## ۵ نتیجه گیری

۱. سنخ‌شناسی مطالعات فضای سایبری نشان می‌دهد ملاک‌های متعددی برای دسته‌بندی مباحث وجود دارد؛ برای مثال پاره‌ای از مطالعات با ملاک تأثیر متقابل فاوا و جامعه ملاک دسته‌بندی شده‌اند. در این مقاله ملاک ورود به بحث، سرشت و ماهیت تکنیک بوده است.
۲. بنا بر ملاک فوق، معنای مطالعات فضای سایبری با رویکرد حکمی عبارت از تقرب به ماهیت پدیده‌ی فضای سایبری و تحقیق درباره چپستی و چرایی آن است.
۳. بحث از بومی‌شدن فاوا ضرورت‌ها به مسئله تغییر و تبدیل کارکرد آن بازمی‌گردد. هر مصنوع تکنیکی در عالمی که خلق شده، دارای کارکردی است؛ خواه به ذات تکنیک منسوب شود، خواه به فرهنگ پدیدآورنده‌ی آن، خواه با هر تبیین دیگر. انتقال فاوا از خارج به ایران و استقرار در درون عالم ما مشروط به تبدیل کارکرد آن در مبدأ است. کارکرد اگرچه وابسته به قصد سازنده است، اما قصد شرط کافی پیدایش و تبدیل آن نیست. پس با تغییر غایات و مقاصد استفاده از فاوا نمی‌توان شرط کافی برای تبدیل کارکردش را فراهم آورد. این تبدیل نیازمند تصرف در ماده و صورت فاوا نیز هست.
۴. فلسفه تکنولوژی ژاپنی ذیل روح سازش و همزیستی این فرهنگ می‌تواند ضمن آموختن از علوم و تکنولوژی و تفکرات غربی به افزایش قدرت تولید و انگیزه‌های ملی برای دسترسی بدان پردازد؛ بدین معنی که آنان از یک سو تشنه‌ی یادگیری از غرب هستند و از سوی دیگر تمایلات وطن‌خواهانه، آنان را وادار به حفاظت از فرهنگ بومی، ضمن یادگیری صنعتی از غرب به‌عنوان وسیله نه هدف، می‌سازد. برخی ژاپن‌پژوهان این خصلت را «مقابله مثبت» با تمدن غربی نامیده‌اند.
۵. در چین، دومین غول تکنولوژی شرقی پس از ژاپن، تبدیل کارکرد تکنیک و اساساً فلسفه علم و تکنولوژی ذیل دیالکتیک طبیعت فهمیده شده است. با بازگشت محققان چینی خارج از کشور به چین، پس از جنگ جهانی دوم، آنها مایل بودند راهنمایی‌هایی برای توسعه علم و فناوری بیابند که از نظر ایدئولوژیکی با خارج از چین متفاوت باشد. دیالکتیک طبیعت به‌مثابه طرح انگلس برای چینی‌ها، پلی میان ماتریالیسم و علوم طبیعی ایجاد می‌کند و آن‌پل، راهنما و ایدئولوژی سیاسی علم است. تغییر کارکرد تکنیک بر این مبنا، معنایش تحقق علم و تکنولوژی پرولتاریا و زدودن علم و تکنولوژی بورژوازی است.
۶. مسئله تغییر کارکرد تکنیک در ایران تحت تأثیر بی‌مهری متفکران ایرانی به فلسفه تکنولوژی قرار گرفته است. برخی از جریان‌های مدافع علم دینی، با تسری دوگانه ایمان و کفر به علم و تکنولوژی، گویی تبدیل کارکرد فاوا را زدودن مبادی کفر از علم و تکنولوژی مولد فاوا و تحقق علم و تکنولوژی ذیل سرپرستی و ولایت رسول الله معنا می‌کنند. به نظر می‌رسد، با وجود اهمیت راه‌حل «علم دینی» بحث از بومی‌شدن فاوا را با تقریر درست از علم و تکنیک «بومی» بهتر بتوان پیش برد.

سیاس‌گزاری. این مقاله با حمایت «مؤسسه شناخت» به نگارش درآمده و از مسئولان مؤسسه یادشده سپاس‌گزارم.

## مراجع

- [۱] ابن سینا، حسین بن عبدالله و طوسی، محمد بن حسن (۱۴۰۳ ق). شرح الإشارات و التنبیها، قم: دفتر نشر کتاب.
- [۲] دوران، بهزاد (۱۳۹۶). «سنخ‌شناسی مطالعات اجتماعی فناوری در ایران». در صمیم، رضا. مطالعات اجتماعی فناوری: تأملات نظری و میان‌رشته‌ای، تهران: پژوهشکده مطالعات فرهنگی و اجتماعی، چاپ ۲، ۲۱۳-۲۳۰.
- [۳] فراستخواه، مقصود (۱۳۹۶). «تأملی در اجتماعی شدن فناوری در ایران». در صمیم، رضا. مطالعات اجتماعی فناوری: تأملات نظری و میان‌رشته‌ای، تهران: پژوهشکده مطالعات فرهنگی و اجتماعی، چاپ ۲، ۱۹۹-۲۱۲.
- [۴] مهدی‌زاده، محمدرضا و توکل، محمد (۱۳۸۶). «مطالعات علم و فناوری: مروری بر زمینه‌های جامعه‌شناسی فناوری». برنامه و بودجه، سال دوازدهم، ش ۱۰۵، ۸۵-۱۲۴.
- [۵] نقی‌زاده، محمد (۱۳۸۸). «بنیان‌های مدرنیته‌زایی» در جاوید، علیرضا و نجاری، محمد. نقد ساختار اندیشه: گفتگوهایی با متفکران ایرانی، تهران: نشر آشیان، ص ۳۵-۶۱.
- [۶] ورماس، پیتر (۱۳۹۱). رویکردی در فلسفه تکنولوژی: از مصنوعات تکنیکی تا سیستم‌های اجتماعی-تکنیکی، تهران: کتاب‌آمه.
- [۷] ون‌لون، یوست (۱۳۹۱)، تکنولوژی رسانه‌ای از منظر انتقادی، ترجمه احمد علیقلیان، تهران: همشهری.
- [8] Chen, Fan and Chen, Jia (2020). "The Sinicization of the Philosophy of Technology and the Research on Socialization of Technology," In Wang, Qian, Chinese Philosophy of Technology, Netherlands: Springer.
- [9] Foster, John Bellamy (2020). "Engels's Dialectics of Nature in the Anthropocene," Monthly Review, 2020, Volume 72, Issue 06, 9-15.
- [10] Guo, Y. (2014). The Philosophy of Science and Technology in China: Political and Ideological Influences. Science & Education, 23(9), 1835-1844.
- [11] Hilpinen, R. (2008). On artifacts and works of art1. Theoria, 58(1), 58-82.
- [12] Kroes, Peter (2012). Technical Artefacts: Creations of Mind and Matter, A Philosophy of Engineering Design. Dordrecht: Springer.
- [13] Mayr, Ernst (1997). "Roots of Dialectical Materialism," in Kolchinsky Edward (ed.), On the edge: Soviet Biology in the 1920s and 1930s, St Petersburg, 12-18.

## فلسفه اطلاعات از منظر پدیدارشناسی

محمد رضاپور<sup>۱</sup>

<sup>۱</sup> استادیار؛ عضو هیأت علمی وزارت علوم، تحقیقات و فناوری، تهران، ایران  
m.rezapour@modares.ac.ir

### چکیده

اشیاء و پدیده‌های جهان به شکل‌های گوناگون خودشان را می‌نمایانند و «پدیدارشناسی» روشی است که به کمک آن می‌توان به آگاهی افراد از مفاهیم و پدیده‌ها، بدون واسطه دست یافت. لازمه‌ی انجام پدیدارشناسی، آشنایی با فلسفه و روش‌های فلسفی است و مبانی فلسفی پدیدارشناسی بایستی در این مسیر مورد مطالعه قرار گیرند. در این راستا، «فلسفه اطلاعات» یک حوزه نوین در مطالعات فلسفی محسوب می‌شود که هم دارای جنبه‌ی «پدیدارشناختی» است و هم دارای جنبه‌ی «فرانظریه‌ای». آشنایی با هر دو جنبه‌ی یادشده از این فلسفه، به فهم کاربردهای بااهمیت و گسترده‌ی آن کمک می‌نماید. بنابراین در این مقاله ضمن معرفی مفهوم فلسفه اطلاعات، و مرور جنبه‌های کلی آن، بر رویکرد پدیدارشناسانه‌ی این فلسفه تمرکز می‌کنیم. هدف اصلی در «پدیدارشناسی»، کشف تجارب مختلف افراد از پدیده مورد بررسی، برای رسیدن به ماهیت و جوهره‌ی واقعی آن پدیده یا مفهوم است و بنابراین رویکرد فلسفی از فلسفه اطلاعات، نقطه‌ی مقابل فلسفه دکارتی محسوب می‌گردد.

**کلمات کلیدی:** فلسفه اطلاعات، پدیدارشناسی، هوش مصنوعی، مقابل فلسفه دکارت.

### ۱ مقدمه

نخستین تلاش‌های منتشر شده در زمینه‌ی «پدیدارشناسی»<sup>۱</sup>، توسط هوسرل مطرح شده که وی بین عین و ذهن تفکیک قائل نبود بلکه ماهیت پدیدارها را ذاتی آنها می‌دانست، ماهیاتی که به‌وضوح قابل درک هستند [۱]. در واقع، پدیدارشناسی، نه مانند عینی‌گرایان انسان را به کناری می‌نهد و او را منفعل برمی‌شمارد و نه تمام نقش را به او می‌دهد، بلکه بر روی هر دوی اینها تمرکز می‌نماید [۹]. «فلسفه اطلاعات» یک حوزه نوین در مطالعات فلسفی محسوب می‌شود که هم دارای جنبه‌ی «پدیدارشناختی» است و هم دارای جنبه‌ی «فرانظریه‌ای»؛ بنابراین فلسفه اطلاعات از یک سو متکفل تحقیق انتقادی درباره ماهیت مفهومی و اصول اساسی اطلاعات، از جمله دینامیک‌های اطلاعات، کاربرد اطلاعات و علوم مربوط به اطلاعات است و از سوی

<sup>۱</sup>Phenomenology

دیگر، معطوف به اخذ و کاربرد روش‌شناسی‌های مبتنی بر نظریه اطلاعات و رایانش برای حل مسائل فلسفی است [۲].

هدف اصلی در «پدیدارشناسی»، کشف تجارب مختلف افراد از پدیده مورد بررسی، برای رسیدن به ماهیت و جوهره‌ی واقعی آن پدیده یا مفهوم است. پیش‌فرض پدیدارشناسی این است که جهان و پدیده‌های آن در بیرون انسان قرار گرفته‌اند و انسان می‌تواند همچون آینه‌ای آشکارساز، تصویری از آن دریافت کند [۳].

## ۲ «پدیدارشناسی» در مقابل «فلسفه‌ی دکارتی»

دکارت در فلسفه‌ی جدیدش معتقد بود که جهانی ثابت وجود دارد که بیرون از ذهن انسان هاست و انسان به قوه‌ی تعقل قادر به شناخت کامل نسبت به آن است؛ به عبارت دیگر، جهان بیرون و ذهن، از یکدیگر مستقل هستند؛ منظور دکارت، قوه تعقل استفاده از حواس برای اندازه‌گیری دقیق چیزها بود و بر همین اساس، استفاده از روش‌های علوم طبیعی برای بررسی پدیده‌های جهان را پیشنهاد می‌داد [۳، ۱۰].

## ۳ روش‌شناسی «فلسفه اطلاعات»

فلسفه اطلاعات عنوانی است که لوچیانو فلوریدی، فیلسوف معاصر ایتالیایی (زاده‌ی ۱۶ نوامبر ۱۹۶۴)، برای اشاره به یک حوزه جدید در مطالعات فلسفی عنوان کرده است [۲]. حوزه‌های پژوهشی فلسفه اطلاعات هم به احیای پرسش‌های دیرین فلسفی پرداخته و هم مسائلی جدید، مانند امکان شبیه‌سازی ذهن و آگاهی به واسطه‌ی هوش مصنوعی، ساحت جهانی ارتباطات، اخلاق مهندسی و ... در این فلسفه بحث می‌شوند. از سویی، فلسفه اطلاعات در زمره‌ی آن دسته از فلسفه‌های مضاف است که هم دارای جنبه پدیدارشناسی و هم دارای جنبه فرانتزیه‌ای است. بنابراین فلسفه اطلاعات از یک سو معطوف به اخذ و کاربرد روش‌شناسی‌های مبتنی بر نظریه اطلاعات و از سوی دیگر معطوف به روش‌های مبتنی بر نظریه ارتباطات برای حل مسائل فلسفی است [۴].

## ۱.۳ پارادایم هوش مصنوعی در فلسفه

پارادایم هوش مصنوعی در فلسفه در سال ۱۹۷۸ در کتاب آرون اسلومن با عنوان «انقلاب کامپیوتری در فلسفه» مطرح شد؛ اسلومن معتقد بود: (الف) در آینده‌ی نه‌چندان دور، اگر فیلسوفی باشد که با برخی از پیشرفت‌های اساسی هوش مصنوعی آشنا نباشد، می‌توان او را به «عدم صلاحیت حرفه‌ای» متهم کرد! (ب) تدریس دوره‌های درسی در فلسفه ذهن، معرفت‌شناسی، زیبایی‌شناسی، فلسفه علم، فلسفه زبان، اخلاق، متافیزیک و سایر حوزه‌های فلسفی، «بدون بحث از جنبه‌های مرتبط با هوش مصنوعی»، به همان میزان «غیرمسئولانه» است که ارائه‌ی دوره‌ی درسی‌ای برای اعطای مدرکی در علم فیزیک، بدون پرداختن به نظریه‌ی کوانتوم! در واقع، اسلومن اعتقاد داشت که تحولات نظری و عملی ناشی از علوم اطلاعات و کامپیوتر و فناوری اطلاعات و ارتباطات، تحوّل بنیادین در علم و فلسفه ایجاد خواهد کرد. اصطلاحاتی همچون «انقلاب کامپیوتری» نیز به همین مفهوم اشاره داشتند [۱۱].

## ۲.۳ جنبه‌ی دیگر فلسفه اطلاعات: فرانظریه بودن

«فلسفه اطلاعات» که در زمره‌ی یک حوزه نوین در مطالعات فلسفی محسوب می‌شود که هم دارای جنبه‌ی «پدیدارشناختی» است و هم دارای جنبه‌ی «فرانظریه‌ای». آشنایی با هر دو جنبه‌ی یادشده از این فلسفه، به فهم کاربردهای بااهمیت و گسترده‌ی آن کمک می‌نماید؛ فرانظریه‌پردازان به «مطالعه‌ی نظام‌مند ساختار اساسی خود نظریه» می‌پردازند [۵]. در واقع، یک «فرانظریه» مجموعه‌ای از مفروضات است که نظریه‌پرداز را در مورد یک پدیده معین جهت می‌دهد و هدایت می‌کند [۶].

## ۴ بحث

وقتی صحبت از داده‌ها (Data)، اطلاعات (Information) و دانش (Knowledge) می‌شود، باور اهل فن این است که داده‌ها، نمادهایی هستند که به‌خودی‌خود بی‌ارزش و بدون مفهوم هستند و اطلاعات، وقتی مفهوم می‌یابد که از کنار هم قرار گرفتن داده‌ها، به تصویر کشیدن‌شان و در واقع پردازش داده‌ها حاصل و استخراج گردد [۷]؛ مبتنی بر همین استدلال است که نظریات مبتنی بر داده‌کاوی (Data Mining) به کندوکاو از درون اطلاعات پرداخته و در دو راه‌برد کلان - یکی توصیفی (Descriptive) و دیگری پیش‌بینانه (Predictive) در پی کشف دانش مستتر و الگوهای مفید و ناشناخته برمی‌آیند [۱۲]-[۳۲].

بنابراین، تعبیری که از برداشت عامه می‌شود این بود که «بدون بازنمایی داده‌ها، اطلاعاتی وجود ندارد»؛ اما این اصل ممکن است به‌طرزی مادی (ماتریالیستی) برداشت شود یعنی برخی قائل به این شوند که «اطلاعاتی که به‌صورت فیزیکی متجسد نشده باشد، ممتنع الوجود است» و در واقع، دیدگاه ماتریالیستی، قائل به این تساوی است: «بازنمایی = پیاده‌سازی (تحقق) فیزیکی» [۲].

علاوه بر رویکردهای بنیادین در فلسفه نظیر اثبات‌گرایی و تفسیری [۳۳]، به‌طور خاص، در «فلسفه اطلاعات» هم علاوه بر رویکرد «پدیدارشناسی»، رویکرد «فرانظریه‌پردازی» نیز گام مؤثری در غنی‌تر ساختن نظریه‌ها است، و بنابراین علاوه بر «پدیدارشناسی»، فهم «فلسفه اطلاعات» نیاز به اطلاع از آن رویکرد هست، و لذا در مقاله‌ی دیگری بر مقوله‌ی فرانظریه‌ای بودن این فلسفه تمرکز کرده‌ایم [۸]. آنچه از منظر فرانظریه‌ی فلسفه اطلاعات، بر نظریات فوق مستولی می‌یابد این است که الزام برای بازنمایی داده‌ها، مستوجب این نیست که بازنمایی حتماً بایستی به‌صورتی مادی صورت گیرد؛ بلکه محیط‌هایی که در آن‌ها، فقط جواهر عقلی (noetic entities) و ویژگی‌ها و فرایندهای مربوط به آن موجود هستند (مانند بارکلی و اسپینوزا)، یا اینکه در آن‌ها جهان مادی یک بنیاد وجودی عقلی دارد (نظیر فیثاغورث، افلاطون، لایبنیتس، هگل)، کاملاً مستعد پذیرفتن اصل بازنمایی هستند، بی‌آنکه منجر به تفسیری مادی (ماتریالیستی) شوند [۲].

## ۵ نتیجه‌گیری

فهم «فلسفه اطلاعات» نیازمند آشنایی دو جنبه‌ی «پدیدارشناختی» و «فرانظریه‌ای» این فلسفه است که در این مقاله به مرور پدیدارشناسی پرداخته شد. هدف اصلی در «پدیدارشناسی»، کشف تجارب مختلف افراد از

پدیده مورد بررسی، برای رسیدن به ماهیت و جوهره‌ی واقعی آن پدیده یا مفهوم است و بنابراین نقطه‌ی مقابل فلسفه دکارتی محسوب می‌گردد زیرا دکارت در فلسفه‌ی جدیدش معتقد بود که جهانی ثابت وجود دارد که بیرون از ذهن انسان‌هاست و انسان به قوه‌ی تعقل قادر به شناخت کامل نسبت به آن است؛ به عبارت دیگر، وی می‌پنداشت جهان بیرون و ذهن، از یکدیگر مستقل هستند [۳، ۱۰].

بحث عالمانه روی این پرسش‌ها ما را به مفاهیم تعیین‌کننده‌ای ممکن است برسانند؛ اساساً مفهومی چون «شناخت کامل پدیده‌ها» در چه زمانی در جهان حاصل می‌شود؟ آن روز چقدر خوش‌گوار است که دیگر تمام ابهامات رفع شده باشند، تمام پردازش‌ها انجام شده باشند و دیگر نیازی به هیچ استخراج اطلاعاتی نباشد! باشد که ببینیم آن روز را.

## مراجع

- [۱] دارتیک، آندره. پدیدارشناسی چیست؟ ترجمه: محمود، نوالی، تهران: نشر سمت، ۱۳۷۳.
- [۲] خندان، م، فدایی، غ. نگاهی به مبادی و مسائل فلسفه اطلاعاتِ لوچیانو فلوریدی. پژوهش‌های فلسفی - کلامی، ۱۳۸۸؛ ۱۰(۳)، ۵-۳۹. doi: 10.22091/pfk.2009.208
- [۳] پروری، پ. خوانشی نو از روش پدیدارشناسی؛ بنیان‌های فلسفی، رویکردها و چارچوب اجرای تحقیق پدیدارشناسی. مطالعات جامعه‌شناسی، ۱۳۹۸؛ ۱۲(۴۴): ۸۷-۱۰۶. doi: 10.30495/jss.2019.669587
- [۴] لقمان استرکی، س. و غلامی، ا. فلسفه اطلاعات در سیستم‌های اطلاعات، دومین همایش بین‌المللی مدیریت و فرهنگ توسعه، تهران، ۱۳۹۴. <https://civilica.com/doc/459994>
- [۵] بوستانی، م.، پولادی، ک.، توسلی رکن‌آبادی، م. فرانظریه به‌عنوان ابزاری برای فهم. جستارهای سیاسی معاصر، ۱۳۹۷؛ ۹(۴): ۲۱-۳۶. doi: 10.30465/cps.2019.3531
- [۶] ریوکس، کوین. «فراثئوری در علم کتابداری و اطلاع‌رسانی: رویکرد عدالت اجتماعی نوپا». مجله آموزش کتابداری و اطلاع‌رسانی، ۲۰۱۰؛ ۵۱(۱): ۹-۱۷. ISSN 0748-5786. JSTOR 20720477
- [۷] رضایور، محمد. «هم‌اکنون، داده‌کاوی» (Now, Data Mining)؛ ماجراجویی فوق‌العاده در علم داده‌ها، مؤسسه فرهنگی هنری دیباگران تهران، ۱۳۹۹.
- [۸] رضایور، محمد. فرانظریه‌ی «فلسفه اطلاعات» (Meta-theory of "Philosophy of Information")، اولین کنفرانس بین‌المللی روانشناسی، علوم اجتماعی، علوم تربیتی و فلسفه، بابل، ۱۴۰۱.
- [9] Waugh W. L. and Waugh W. W., (2006). Phenomenology and public administration. Handbook of organizational theory and management: the philosophical approach. CRC press, boca raton, Pp: 478-509.
- [10] Johnson, P. and Duberley, J. (2000). Understanding management research: an introduction to epistemology. Thousand Oaks: SAGE Publication Ltd.
- [11] Feloridi L. (2002). What is the Philosophy of Information? URL: <http://www.wolfson.ox.ac.uk/~floridi/pdf/wipi.pdf>



- [12] Sepehri, M. M., Khavaninzadeh, M., Rezapour, M., & Teimourpour, B. (2011). A data mining approach to fistula surgery failure analysis in hemodialysis patients. 18th Iranian Conference of Biomedical Engineering (ICBME), 2011 (pp. 15-20). IEEE. URL: [ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?arnumber=6168546](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=6168546)
- [13] Kazemzadeh B R., et al. "Design and analysis of a health care supply chain management." *Advanced Materials Research*; 2012. 433(440): 2128-2134.
- [14] Khavanin Zadeh, Morteza, Mohammad Rezapour, and Mohammad Mehdi Sepehri. "Data mining performance in identifying the Risk Factors of early arteriovenous fistula failure in Hemodialysis Patients." *International journal of hospital research* 2, no. 1 (2013): 49-54. Available at: <http://ijhr.iuums.ac.ir/index.php/ijhr/article/view/52/116>
- [15] Rezapour, Mohammad, Morteza Khavanin Zadeh, and Mohammad Mehdi Sepehri. "Implementation of predictive data mining techniques for identifying risk factors of early AVF failure in hemodialysis patients." *Computational and Mathematical Methods in Medicine* 2013 (2013). URL: <http://dx.doi.org/10.1155/2013/830745>
- [16] Rezapour, M., Sepehri, M. M., & Rezapour, H. (2014). A data mining approach to determine better methods for learners' assessment in e-learning courses. *Management Research in Iran*, 17(4), 139-160.
- [17] Rezapour M, Khavanin Zadeh M., "Association between non-matured arterio-venous fistula and blood pressure in hemodialysis patients." *Medical journal of the Islamic Republic of Iran* 28 (2014): 144. Available at: [http://mjiri.iuums.ac.ir/browse.php?a\\_id=2569&sid=1&slc\\_lang=en](http://mjiri.iuums.ac.ir/browse.php?a_id=2569&sid=1&slc_lang=en)
- [18] Khavanin Zadeh, M., Rezapour, M., Khavanin Zadeh, E., Balin Parast, M., & Rezapour, H. (2015). The Relationship between Risk Factors of Hemodialysis Patients and Arterio Venous Fistula Maturation at Hasheminezhad Hospital. *Iranian Journal of Surgery*, 22(4), 54-64.
- [19] Rezapour, M., Taran, S., Parast, M. B., & Zadeh, M. K. (2016). The impact of vascular diameter ratio on hemodialysis maturation time: Evidence from data mining approaches and thermodynamics law. *Medical journal of the Islamic Republic of Iran*, 30, 359.
- [20] Rezapour, M., Zadeh Khavanin, and M. Balinparast. "The Role of the Vascular Diameter Ratio in the Arteriovenous Fistula Maturation Time." *The Journal of Vascular Access* 14, no. 1.
- [21] Rezapour M., Sepehri M.M, Khavanin Zadeh M., Alborzi M. (2017). Data Mining Application for Detect Impacts of Infection and Hypertension on Vascular Surgery Complications, 2th International Conference on Knowledge-Based Research in Computer Engineering & Information Technology.
- [22] Rezapour, M., Payani, E., Taran, M., Rajabzadeh Ghatari, A., & Khavanin Zadeh, M. (2017). "Roles of triglyceride and phosphate in atherosclerosis of diabetic hemodialysis patients". *Medical Journal of the Islamic Republic of Iran (MJIRI)*, 31(1), 465-471.

- [23] Rezapour, M., Sepehri, M. M., Khavanin Zadeh, M., & Alborzi, M. (2018). A new method to determine anastomosis angle configuration for arteriovenous fistula maturation. *Medical Journal of the Islamic Republic of Iran (MJIRI)*, 32(1), 365-370.
- [24] Rezapour, M., Zadeh, M. K., Sepehri, M. M., & Alborzi, M. (2018). Less primary fistula failure in hypertensive patients. *Journal of human hypertension*, 32(4), 311. Is available at URL: <https://www.nature.com/articles/s41371-018-0052-3>
- [25] Rezapour, M. (2018). Forecasting Surgical Outcomes Using a Fuzzy-Based Decision System. *International Journal of Hospital Research*, 7(1), 1-11., [http://ijhr.iums.ac.ir/article\\_87050.html](http://ijhr.iums.ac.ir/article_87050.html)
- [26] Sepehri, M. M. & Rezapour, M. (2019). *Medical Data Mining: Efficient Knowledge Discovery from Health Data. Volume 1*, Fater Negar, Hospital Management Research Center, Iran University of Medical Sciences.
- [27] Rezapour, Mohammad. "Predicting Stroke in Hemodialysis Patients Using Data Mining." *Digital Transformation* 1, no. 1 (2021): 45-57.
- [28] Rezapour, M., and Nakhostin Ansari, N. "Incidence of Stroke in Hemodialysis Patients with Central Venous Catheter: A Systematic Review." *Journal of Vessels and Circulation* 2, no. 1 (2021): 27-27.
- [29] Rezapour, M., Nakhostin Ansari, N. Khavanin Zadeh, M. and Asadi, R. "Risk of Stroke in Hypertensive Diabetic Chronic Kidney Disease Patients after Central Venous Catheter placement." *Razi Journal of Medical Sciences* 27, no. 8 (2020): 0-0.
- [30] Rezapour, M., Shadpour, P. Karimi, A. Mousavi Jahromi, Y. and Khavanin Zadeh, M. "Inverse effects of anemia and diabetes mellitus on non-cuffed central venous catheters longevity." *Iran J Vasc Surg Endovasc Ther* <http://ijvset.gums.ac.ir>, 1, no. 1 (2021).
- [31] Rezapour, M, Asadi, R. and Marghoob, B. "Central Venous Catheter placement, Diabetes Mellitus and Hypertension Are Associated with Risk of Cerebrovascular Accident in Hemodialysis patients." *International Journal of Hospital Research* 10, no. 3 (2021).
- [32] Rezapour, M. and Ansari, N.N., 2021. Designing and Producing a Telerehabilitation Mobile Application and a Web-Based Smart Dashboard for Online Monitoring of Patients at Risk of Stroke During COVID-19 Pandemic and Post-Pandemic Era. *International Journal of Basic Science in Medicine*, 6(4), pp.127-131.
- [33] Rezapour, Mohammad. *A Philosophical Perspective Analysis of Researches in Positivism and Interpretivism Paradigms*, The first conference on Cyber Space, University of Tehran, Iran, 2022.

## بررسی رابطه حاکمیت شرکتی و حکمرانی فضای مجازی

محمود اعتصامی فر<sup>۱</sup>

<sup>۱</sup> دانشجوی کارشناسی ارشد مدیریت رسانه، دانشگاه ادیان و مذاهب اسلامی قم  
mimallef69@mail.ir

### چکیده

فضای مجازی در حال حاضر در تمام ابعاد زندگی فردی و اجتماعی مردم جهان نفوذ کرده و در حال ایجاد یک تمدن جدید بشری است که از تمدن‌های قبل به مراتب فراگیرتر است. حکومت‌ها سعی می‌کنند سیاست‌هایی را برای شکل دادن به فعالیت‌ها در فضای مجازی تدوین و اجرا کنند. امروز مقدرات فضای مجازی در اختیار شرکت‌های بزرگ و فراملیتی است. هدف این مقاله بررسی رابطه حاکمیت شرکتی و حکمرانی فضای مجازی می‌باشد. و چگونه می‌توان با حکمرانی درست در فضای مجازی، حکمرانی شرکت‌های بزرگ را تحت سلطه حاکمیتی خود در آورد. پژوهش حاضر کاربردی و آینده‌نگرانه است و روش تحقیق آن کیفی و از نوع توصیفی-تحلیلی است. نتایج پژوهش نشان می‌دهد که حکمرانی در فضای مجازی و کنترل و تسلط بر شرکت‌های بزرگ تا حد زیادی وابسته به میزان قدرت و نفوذ کشورهای بزرگ در آن منطقه و استراتژی و ساختار سیاسی کشورهای وابسته یا تحت شعاع آنها، بستگی دارد. هر کدام از کشورهای منطقه برای اینکه بتوانند حکمرانی تأثیرگذاری در فضای مجازی داشته باشند باید برای آن راهکارهای کنترلی و قواعد خاصی در نظر بگیرند. کشور ایران نیز برای اینکه از فضای مجازی به نفع خود سود ببرد باید تا حدی زیادی به قوانینی که پایه‌گذاری کرده است، بیش از پیش جامه‌ی عمل بپوشاند و روی شرکت‌های خصوصی بزرگ برای رقابت در عرصه جهانی سرمایه‌گذاری داشته باشد.

**کلمات کلیدی:** حاکمیت، حکمرانی، حاکمیت شرکتی، حکمرانی فضای مجازی.

### ۱ مقدمه

تأثیر مکانیسم‌های حاکمیت شرکتی بر مدیریت سود یکی از موضوعاتی است که در سال‌های اخیر مورد توجه پژوهشگران قرار گرفته است. حاکمیت شرکتی معمولاً به عنوان مجموعه‌ای از سازوکارها تعریف می‌شود که برای کاهش مشکلات نمایندگی بین سهامداران و مدیران به دلیل جدایی مالکیت و کنترل طراحی شده است (شاقوزایی، سلیمی زاده، ۱۳۹۶).

دیدگاه‌های متعددی برای توضیح ساختار حاکمیت شرکتی وجود دارد. در تعریفی که هیوز از حاکمیت شرکتی ارائه داد آن را فرآیند استفاده از قدرت شرکت و چگونگی کنترل آن در برخورد با مسائل شرکتی و

یا فراشرکتی دانست. چهار مکتب فکری متفاوت در زمینه حاکمیت فکری شامل تئوری کارگزاران اصلی، رویکرد دینفعان، رویکرد نظارت و رویکرد سیاسی را نام برد. شیوه‌های حاکمیت شرکتی به منظور پاسخگویی به نیازهای شرکت‌ها همواره در حال تغییر و پیشرفت است، ولی هیچ‌گونه مدل جهانی برای آن وجود ندارد. علاوه بر آنکه قوانین کشورها نقش تعیین‌کننده‌ای در سیستم حاکمیت شرکتی دارند، در یک کشور نیز ساختار حاکمیت شرکتی از شرکتی به شرکت دیگر متفاوت است. آرمان حاکمیت شرکتی در چالش‌های گوناگون آن، کاستن مشکل نمایندگی است. فیصله دادن مشکل نمایندگی تا حدودی اطمینان خاطر شرکت‌ها را فراهم می‌کند که مدیران در اهتمامند تا ثروت آنان را به بیشترین حد ممکن برسانند. بدینسان می‌توانند اثر در خوری بر عملکرد هر شرکتی داشته باشند. کیفیت ساختار حاکمیت شرکتی رفتارهای فرصت طلبانه‌ی مدیریت را کاهش می‌دهد و به منافع سرمایه‌گذاران کمک می‌کند و عملکرد شرکت‌ها را بهبود می‌بخشد (غلامی، ۱۳۹۹).

فضای مجازی در حال حاضر در تمام ابعاد زندگی فردی و اجتماعی مردم جهان نفوذ کرده و در حال ایجاد یک تمدن جدید بشری است که از تمدن‌های قبل به مراتب فراگیرتر است. فضای مجازی فضایی فناوری پایه، مبتنی بر فناوری اطلاعات و ارتباطات است که در آن تولید محتوا، پالایش داده، ذخیره‌سازی داده، پردازش داده و توزیع داده صورت می‌گیرد. یکی از مباحثی که در فضای مجازی، مطرح می‌شود، حکمرانی فضای مجازی است. در تعریف معنای حکمرانی فضای مجازی، می‌توان به تعریف حکمرانی اینترنت از سوی اجلاس جهانی سران درباره جامعه اطلاعاتی اشاره نمود: حکمرانی اینترنت، توسعه و کاربرد اصول، هنجارها، قوانین، رویه‌های تصمیم‌گیری و برنامه‌های شکل دهنده تکامل استفاده از اینترنت از سوی دولت‌ها، بخش خصوصی و جامعه مدنی، هر یک در نقش خاص خود می‌باشد. حکومت‌ها سعی می‌کنند سیاست‌هایی را برای شکل دادن به فعالیت‌ها در فضای مجازی تدوین و اجرا کنند، رویه‌های عمل قانونی و مشروع را در فضای مجازی تعیین کنند و روابط میان بازیگران و گروه‌های اجتماعی مختلف را تنظیم کنند (احمدی، ۱۳۹۷).

در بالا، به صورت جداگانه در مورد حاکمیت شرکتی و همچنین حکمرانی فضای مجازی صحبت کردیم. هدف ما در این پژوهش بررسی ارتباط این دو موضوع باهم است. امروزه سرنوشت فضای مجازی در دست شرکت‌های بزرگ و فراملی است. البته این بدان معنا نیست که دولت‌ها در فضای مجازی هیچ نقشی ندارند یا نقشی ناچیز دارند، اما واقعیت مجازی نشان می‌دهد که شرکت‌های فراملی تا حد زیادی جایگزین دولت‌ها شده‌اند. با این حال، دولت‌هایی که از نظر قلمرو، امنیت یا ایدئولوژی بر این شرکت‌ها تسلط دارند، در حال حاضر برنده جنگ سلطه سایبری یا همان حکمرانی بر فضای مجازی هستند؛ اما باید این را هم در نظر بگیریم که بیشترین حجم بازارهای جهانی در بیست سال اخیر در حوزه‌های مختلف فضای مجازی از تجهیزات و زیرساخت‌های رایانه‌ای گرفته تا خدمات میزبانی و توسعه فناوری ابری و اینترنت اشیا و ... متعلق به همین شرکت‌های بزرگ است. لذا با توجه به موارد بالا موضوعی که در این مقاله بدنبال پاسخ به آن هستیم بررسی رابطه حاکمیت شرکتی و حکمرانی فضای مجازی می‌باشد. و چگونه می‌توان با حکمرانی درست در فضای مجازی، حکمرانی شرکت‌های بزرگ را تحت سلطه حاکمیتی خود در آورد.

مهم‌ترین پژوهش‌های انجام شده در ارتباط با موضوع این تحقیق عبارتند از:

- باستانی و همکارش در تحقیقی با عنوان «نقش شبکه‌های اجتماعی در ارتباط با حاکمیت شرکتی»

به بررسی رابطه فضای مجازی و حاکمیت شرکتی پرداختند. هر یک از اعضای شرکت به عنوان عاملی در شبکه‌های اجتماعی یا مجازی، سرمایه‌های مادی و معنوی، دارایی‌های مشهود و نامشهود خود و سازمان وابسته را با سایر ذینفعان حقیقی و حقوقی شرکت به اشتراک می‌گذارند. نتایج پژوهش‌های آنها نشان می‌دهد قدرت غیررسمی بالاتر با ایجاد اختیار در زمینه نشر یا عدم توزیع منابع موجبات ایجاد کنترل و نظارت بالاتر در حوزه حاکمیت شرکتی را فراهم می‌کند و از طریق فضای مجازی دولت‌ها را تحت سلطه خود در می‌آورند (باستانی، ۱۳۹۴).

- کیان‌خواه در تحقیقی با عنوان «چالش‌های راهبردی حکمرانی در فضای سایبر» به بررسی سیاست‌های حاکم بر فضای مجازی و نحوه کنترل آن پرداختند. این تحقیق ابتدا با روش ترکیبی، چالش‌های حکمرانی را به صورت توصیفی-تحلیلی اکتشاف نموده و سپس با مراجعه به خبرگان این حوزه و پیمایش نظرات و تحلیل با معادلات ساختاری اکتشاف نموده است. نتایج نشان می‌دهد که استقرار نظامات بازار مجازی اسلامی مبتنی بر نظام ارزشی اسلام و اقتصاد مقاومتی از راهکارهای مهار چالش‌های راهبردی حکمرانی با فضای سایبر است. عدم توجه به این چالش‌های راهبردی منجر به وابسته و سلطه کفار بر نظام اسلامی خواهد شد (کیان‌خواه، ۱۳۹۸).

## ۲ بازیگران فعال، شرکت‌های بزرگ

با رشد فضای مجازی، شرکت‌های بزرگ در طول این دهه جایگاه بیش از پیش مهمی در اقتصاد جهانی به دست آورده‌اند. همان گونه که اقتصادهای ملی بیش از پیش متمرکز گردیده‌اند. تحت سلطه‌ی تعداد محدودی شرکت‌های بسیار بزرگ در آمده‌اند، اقتصاد جهانی نیز دستخوش همین تحول گردیده است. شرکت‌های بزرگ با منابع و امکانات عظیم اقتصادی و مالی و استخدام رهبران و نخبگان علوم مختلف و تکنوکرات‌های بلندپایه اداری-نظامی و همچنین استفاده از منابع اطلاعاتی و رسانه‌های جمعی آن، آنچنان بر کشورهای جهان از جمله کشورهای توسعه نیافته، در حال توسعه و پیشرفته صنعتی تسلط دارند که در دوران قدرتمندترین امپراتوری‌ها هرگز دیده نشده بود. امروزه انواع فناوری‌های مخابراتی امکان برقراری ارتباط کم و بیش آنی از نقطه‌ای به نقطه دیگر در جهان را فراهم کرده است (عباس‌زاده، ۱۳۹۴). از سال ۱۹۶۵، زمانی که اولین ماهواره توانست ۲۴۰ تماس تلفنی را تنها در یک زمان مخابره کند، ماهواره‌ها برای ارتباطات تجاری از راه دور مورد استفاده قرار گرفتند. ماهواره‌های فعلی می‌توانند ۱۲۰۰۰ تماس همزمان را مخابره کنند. شرکت‌های بزرگ اکنون سیستم‌های ارتباطی ماهواره‌ای خاص خود را دارند. به عنوان مثال، میتسویشی دارای یک شبکه‌ی عظیم است که روزانه پنج میلیون کلمه از طریق آن به دفتر مرکزی آن در توکیو و از آنجا به سایر نقاط جهان مخابره می‌شود.

زمانی که تمرکز فعالیت فضای مجازی عمدتاً اقتصادی باشد، واضح است که بازیگران اصلی فضای مجازی نه تنها به این دلیل که فضای مجازی ماهیت شبکه‌ای و فرامرزی دارد. بلکه چون فرمول‌های کسب و کار در دنیا مبتنی بر بازار آزاد طراحی شده است، شرکت‌های بزرگ غیردولتی هستند؛ یعنی دولت‌ها اگر فرصت عمل داشته باشند، عرصه را به سود شرکت‌های غیردولتی باز می‌کردند. این درحالی است که اصولاً دولت‌ها



در فضای مجازی، مجالی برای عرض اندام ندارند (محمدی، ۱۳۹۹). واضح است که هر چه دامنه خدمات و مشتریان این شرکت‌ها گسترده‌تر باشند، سهم بیشتری به عنوان بازیگران اصلی و فعال در فضای مجازی خواهند داشت، اگر به دهه گذشته نگاه کنیم، روشن می‌شود شرکت گوگل به عنوان یکی از همین شرکت‌های بزرگ، تصمیمات شناسایی و خرید ده‌ها شرکت پرفریت فعال در فضای مجازی را انجام داده است که نشان دهنده این است که این شرکت به دنبال گسترش قلمرو خود در همه عرصه‌ها و حکمرانی حداکثری بر فضای مجازی بوده است (مشبکی، ۱۳۹۸).

### ۳ تنظیم‌گری در نظام حکمرانی

تنظیم‌گری در معنای عام خود شامل انواع مداخلات دولت برای تحقق اهداف حاکمیت است. به لحاظ تاریخی نمی‌توان تنظیم‌گری را اساساً پدیده‌ای مدرن به شمار آورد و در این راستا می‌توان موارد متعددی از مداخلات حاکمیتی را در قرن نوزدهم در کشوری مانند آمریکا ذکر کرد. هدف از این مداخلات ایجاد کنترل عمومی بر ارائه‌کنندگان خدمات جهت تضمین منفعت عمومی است. منفعت عمومی نفعی است که عاید همه ذینفعان و عموم جامعه می‌شود و تأمین آن از جمله اصلی‌ترین فلسفه‌های تشکیل حکومت‌ها محسوب می‌شود. این مفهوم معمولاً در برابر منفعت خصوصی قرار می‌گیرد به ویژه در جایی که تأمین منافع یک فرد یا گروه به منافع سایرین آسیب می‌رساند. صیانت از منفعت عمومی به معنای جلوگیری از آسیب زدن منافع گروه‌های خاص به منافع سایر ذینفعان است و از جمله اصلی‌ترین فلسفه تشکیل حکومت‌ها محسوب می‌شود. حکمرانی لزوماً توسط دولت یا حکومت اعمال نمی‌شود و ممکن است در یک ساختار قدرت توزیع شده و متکثر، کارکردهای حکمرانی توسط سایر بازیگران مانند اصناف، سازمان‌های مردم‌نهاد و یا حتی آحاد مردم انجام شود. همانطور که مشخص است این تعریف بسیار کلی بوده و مجموعه بسیار گسترده‌ای از کارکردها را شامل می‌شود که تنظیم‌گری یکی از کارکردهای اصلی نظام حکمرانی است. در این نگاه، تنظیم‌گری به عنوان بخشی از نظام کلان حکمرانی مورد توجه قرار گرفته است (یاوری، ۱۳۹۳).

وقتی که صحبت از تنظیم‌گری می‌شود دو دسته نظریات متعارض وجود دارد، دسته اول نظریاتی است که تنظیم‌گری را برای ایجاد یک نظام حکمرانی مناسب و کارآزوری می‌دانند و بر ضرورت ایجاد نظام حکمرانی مبتنی بر تنظیم-گری تأکید دارند و دسته دوم نظریاتی است که شکل‌گیری تنظیم‌گری را دارای آفات و آسیب‌های قابل توجهی می‌دانند و از همین‌رو با شکل‌گیری نظام تنظیم‌گری مخالفت می‌کنند. نظریات دسته اول بیشتر بر منافع حاصل از وجود نهادهای تنظیم‌گر تأکید دارند و ضمن برشمردن آنها از جنبه‌های مختلف وجود نهادهای تنظیم‌گر را موجب صیانت از منفعت عمومی معرفی می‌کنند. این دسته از نظریات تحت عنوان نظریات منفعت عمومی قرار می‌گیرند و ضرورت تنظیم‌گری از جنبه‌هایی همچون اقتصادی، سیاسی، نظام حکمرانی، فنی تخصصی، اقتصاد سیاسی و نیز مکمل نظام قضایی بحث و بررسی می‌شوند. دسته دوم نظریات بیشتر حول محور موضوع تسخیر تنظیم‌گری قرار می‌گیرند. این دسته از نظریات بیان می‌دارند که صاحبان رانت و قدرت انگیزه بالایی برای استفاده از ظرفیت نهادهای تنظیم‌گر دارند، زیرا این نهادها از اختیارات زیاد و متنوعی برخوردارند و کمک زیادی به تحقق منافع صاحبان رانت و قدرت خواهند



نمود و به همین دلیل آنها تمام تلاش خود را برای تسخیر و اثرگذاری بر عملکرد تنظیم‌گران خواهند کرد. بدین جهت اکثر تنظیم‌گران تحت نفوذ صاحبان رانت و قدرت قرار می‌گیرند و اصطلاحاً توسط آنها تسخیر می‌شوند و در چنین شرایطی عملکردی متناقض با هدفی که برای آن تأسیس شده‌اند خواهند داشت. البته نظریات دسته اول انتقاد وارد شده از سوی نظریات دسته دوم را رد نمی‌کنند، اما معتقدند چاره این مشکل کنار گذاشتن نهادهای تنظیم‌گر نیست، بلکه باید سازوکاری طراحی شود که از تسخیر نهادهای تنظیم‌گر جلوگیری شود و تنظیم‌گران عملکرد مستقل و بی‌طرفانه‌ای داشته باشند (خاندوزی، ۱۳۸۹).

## ۴ حاکمیت چند ذیربطی

حکمرانی چند ذیربطی رویکردی نسبتاً جدید برای حکمرانی در حوزه عمومی است که طی دو دهه اخیر مورد توجه قرار گرفته است. در سند نهایی اجلاس جهانی جامعه اطلاعاتی در سال ۲۰۰۵ در تونس که به دستورکار تونس شهرت یافت، پیشنهاد شده است که حکمرانی بین‌المللی اینترنت به شکلی چند ذیربطی پی گرفته شود. حکمرانی چند ذیربطی رویکردی در حکمرانی است که بر مشارکت ذیربطان گوناگون در تدوین، اجرا و ارزیابی سیاست‌ها، قوانین و مقررات در حوزه عمومی تأکید می‌کند. ذیربط عبارت است از هر فرد، گروه یا سازمان که منفعت/علاقه مستقیم یا غیرمستقیمی در زمینه مسئله یا هدف مورد بحث داشته باشد. ذیربطان می‌توانند کسب و کارها، جامعه مدنی، دولت‌ها، نخبگان مؤسسات تحقیقاتی و سازمان‌های غیردولتی باشند. معمولاً برای اشاره به این افراد، گروه‌ها و سازمان‌ها از واژه ذی‌نفع استفاده می‌شود، اما واژه نفع عمده‌تاً معنایی اقتصادی را به ذهن متبادر می‌کند، در حالی که علائق/منافع ذیربطان همواره اقتصادی نیست. مدل حکمرانی چند ذیربطی نوعی ساختار حکمرانی است که سعی دارد ذیربطان را گرد هم آورد تا در گفتگو، تصمیم‌سازی و اجرای راه‌حل‌ها برای مسائل یا رسیدن به اهداف مشترک مشارکت کنند. فرایند چند ذیربطی مستلزم درگیر شدن کامل تمامی ذیربطان، تصمیم‌گیری مبتنی بر اجماع و عمل کردن به شیوه‌های باز، شفاف و پاسخگوست. فرایندهای چند ذیربطی فرایندهایی را توصیف می‌کند که قصد دارند ذیربطان اصلی را در شکل جدیدی از ارتباطات، تصمیم‌یابی و احتمالاً تصمیم‌سازی در مورد موضوعی خاص گرد هم آورند. این فرایندها بر درک اهمیت دست یافتن به برابری و پاسخگویی در ارتباطات میان ذیربطان مبتنی‌اند. همچنین این فرایندها به اصول دموکراتیک شفافیت و مشارکت متکی‌اند و هدف از آنها این است که مشارکت شکل گیرد و شبکه‌های میان ذیربطان تقویت شود (شیرازی، ۱۳۹۸).

## ۵ حکمرانی دولت‌ها در فضای مجازی

انجمن‌های تخصصی معدودی در حوزه فضای مجازی فعال هستند و کاربران اینترنت انجمن‌های فعالی ندارند. تقریباً هیچ یک از انجمن‌های فعال بر سیاست‌گذاری و حکمرانی فضای مجازی متمرکز نیستند و دخالتی رسمی در فرایندهای تدوین، اجرا و ارزیابی سیاست ندارند. اما برخی نهادهای صنفی تأثیرگذاری غیرمحسوس دارند. انجمن‌های موجود یا سایر تشکل‌های ذیربطان به شکلی رسمی در فرایندهای سیاست‌گذاری و حکمرانی فضای مجازی مشارکت داده نمی‌شوند. برای مثال، فراهم‌کنندگان خدمات اینترنتی، صاحبان

کسب و کارهای اینترنتی، تولیدکنندگان محتوا و گروه‌های کاربران کرسی دارای حق رأی یا حتی کرسی مشورتی در شورای عالی فضای مجازی ندارند و به صورت رسمی، از آنها برای طرح دیدگاه‌هایشان یا برای بازخورد دادن درباره پیش‌نویس‌ها دعوت نمی‌شود. سیاست‌گذاری‌ها و تدوین مقررات معمولاً پشت درهای بسته و با حضور نمایندگان دولت و اعضای انتصابی انجام می‌گیرد. در عین حال، ذریبطان قدرتمند دیدگاه‌های خود را از طریق اعضا و نهادهایی که با آنها در ارتباط‌اند به صورت غیررسمی و غیرمستقیم طرح می‌کنند.

## ۶ دسته‌بندی کشورها در برخورد با مواضع حکمرانی در فضای مجازی

هرکشوری مواضع جداگانه‌ای نسبت به فضای مجازی و حکمرانی شرکت‌ها در برابر دولت‌ها دارد. این مواضع به عوامل متعددی از جمله قدرت اقتصادی، نظامی، فرهنگی، جایگاه و میزان نفوذ آن کشور در بین سایر کشورهای منطقه بستگی دارد. محمدی در مقاله‌اش کشورها را به سه دسته کلی تقسیم‌بندی کرده است. کشورهای در دسته اول دارای بزرگترین اقتصاد برتر دنیا هستند و تقریباً روی ابزارها، محتوا و پلتفرم‌ها تسلط دارند. این دسته از جمله کشورهای دانش بنیان در اکثر زمینه‌ها هستند و تجهیزات و نرم‌افزارها و کلان داده‌ها را در فضای مجازی مدیریت می‌کنند. دسته دوم، کشورهای وابسته به دسته اول هستند، که بخش عمده‌ای از قدرت و نفوذ آنها نشأت گرفته از حمایتی است که کشورهای دسته اول از آنها می‌کنند. لذا در دسته دوم خود به صورت مستقیم حکمرانی را برعهده ندارند و سیاست آنها برگرفته از کشورهای دسته اول است. در دسته سوم کشورهایی هستند که علاوه بر این سیاست مشخصی در مواجهه با حکمرانی شرکت‌ها در فضای مجازی ندارند، بلکه تحت حمایت کشورهای دسته اول هم نیستند. در نتیجه این کشورها یا ورود شرکت‌های بزرگ و فراملیتی را در کشور خود منع کرده یا به صورت کلی فضا را در اختیار این شرکت‌ها قرار می‌دهند و خود کنترلی روی این شرکت‌ها ندارند (غلامی، ۱۳۹۹).

## ۷ مواضع کشورهای صاحب نام در حکمرانی در فضای مجازی

کشورهای صاحب نام اکثراً در دسته اول قرار می‌گیرند در نتیجه هر کدام از آنها مواضع خاصی برای حکمرانی در فضای مجازی و تسلط بر شرکت‌های بزرگ برای پیشبرد اهداف خود دارند. کشور آلمان در سال ۲۰۱۷ قانون فدرال محافظت از داده‌ها را با مفاد قوانین عام محافظت از داده‌ها هماهنگ کرد. البته انطباق قوانین بخشی و ایالتی، مانند قوانین اجتماعی آلمان و اکثریت قوانین محافظت از داده‌های دولتی، هنوز معلق است. دورنمای کلی حکمرانی فضای مجازی در آلمان در چارچوب حکمرانی چندذریبطی معنا دارد. در حوزه ارتباطات راه دور آژانس فدرال شبکه بر برنامه شماره‌گذاری تلفن و دیگر مواردی که به تخصیص اعداد فنی مربوط است در آلمان نظارت دارد و در این حوزه مرجع ذیصلاح محسوب می‌شود. همچنین تنظیم‌گری در زمینه بازر ارتباطات راه دور در صلاحیت این آژانس قرار دارد. یکی از راه‌کارهای آنها در حکمرانی در فضای مجازی، تقویت شرکت‌های اروپایی در مقابله با سلطه انحصاری شرکت‌های امریکایی در اقتصاد مجازی است. در واقع ۲۸ بازار ملی در حوزه یورو در یک بازار تجمیع می‌شوند و هدف این طرح

یکپارچه‌سازی قوانین و ایجاد تسهیلات برای این بازار واحد است. به طور کلی می‌توان گفت سناریوهای حکمرانی فضای مجازی آلمان شامل توجه به امنیت سایبری، توسعه زیرساخت‌های فضای مجازی، استفاده از ظرفیت اقتصادی فضای مجازی، تدوین استراتژی امنیت سایبری، تربیت نیروهای پلیس زبده برای کنترل محتوای فضای مجازی، استفاده از ظرفیت علمی آکادمیک برای کنترل محتوای فضای مجازی، دیپلماسی اروپایی بین‌المللی سایبری، جلوگیری از کنترل یک جانبه آمریکا بر فضای مجازی و تلاش برای ایجاد حاکمیت چند ذربطی می‌باشد (پورشیرازی، ۱۳۹۸).

یکی دیگر از کشورهای صاحب نام، روسیه است. می‌توان اقدامات انجام گرفته توسط حکومت روسیه برای مواجهه با فضای مجازی را در چندین بخش دسته‌بندی نمود. در حوزه‌ی حاکمیت سایبری، تدوین اسناد استراتژیک، منابع متعددی را برای ایجاد توازن فنی و مشارکت استراتژیک منصفانه با دولت‌ها فراهم کرده است؛ همچنین تاکید بر چندجانبه‌گرایی در مدل حکمرانی اینترنت جهانی در چارچوب سازمان ملل و مقابله با هژمونی آمریکا بر بستر اینترنت موجود، توجه به الگوی مستقل توسعه فضای مجازی بر اساس ساختار و اقتضات بومی و الگوی بومی تنظیم مقررات، تدوین و تصویب قوانین امنیت سایبری و استانداردهای امنیتی لازم در حوزه شبکه و زیرساخت‌های حیاتی و اعمال محدودیت و فیلترینگ در برابر پلتفرم‌های خارجی که حاضر به همکاری و رعایت الزامات قانونی داخلی نیستند، از جمله دیگر اقدامات روسیه در حوزه‌ی حاکمیت سایبری بوده است. به منظور تقویت هرچه بیشتر حاکمیت سایبری، اینترنت ملی که تحت قانونی موسوم به حاکمیت اینترنت روسیه راه اندازی شده، امکان استقلال کامل فضای مجازی روسیه را تحت یک شبکه اینترنت محلی با عنوان رونت فراهم نموده است. توسعه و بهره‌برداری از دامنه ملی و سیستم‌های مربوط به آن، تاسیس مرکز نظارت و مدیریت اینترنت و از سوی دیگر رمزگذاری برای محافظت از سازمان‌ها و شرکت‌های دولتی در اینترنت، از جمله دیگر فعالیت‌های روسیه در زمینه اینترنت این کشور بوده است (قنبری، ۱۳۹۹).

یکی از کشورهای بزرگ و صاحب نام چین است. توجه به اصل حاکمیت سایبری یکی از رویکردهای اصلی در مدیریت فضای مجازی در کشور چین به حساب می‌آید. بر همین اساس، اقدامات فعالانه‌ای چون سرمایه‌گذاری وسیع در علوم، تحقیقات و فناوری‌های راهبردی و بنیادین فضای مجازی، توسعه اینترنت ملی، راه اندازی سرویس‌های اجتماعی تحت وب به جای خیل عظیم سرویس‌های آمریکایی، توسعه و تقویت شدید توان سایبری و همکاری حقوقی در مبارزه با جرائم سایبری از جمله اقدامات انجام گرفته جهت حفاظت از فرهنگ بومی و دغدغه‌های اجتماعی در چین بوده است. در کنار این موارد، شکل دادن به فضای مجازی از طریق بسترسازی مناسب برای استارت‌آپ‌های ایجاد شده در حوزه‌های مرتبط با فضای مجازی از کارهای انجام شده برای توسعه سیاسی و اقتصادی در چین بوده است. همچنین در حوزه دیپلماسی، مدیریت ارتباطات دوجانبه با آمریکا و سایر همکاران مهم، تحکیم نفوذ منطقه‌ای و دیپلماسی سایبری، مخالفت با اقدامات سایبری آمریکا در سازمان ملل و انتقاد به عملکرد آیکن و در کنار آن همکاری فنی و چندجانبه از جمله اقدامات چین جهت ارتقای هرچه بیشتر جایگاه و نفوذ این کشور در حوزه فضای مجازی بوده است (رضاپور، ۱۳۹۸).

یکی از کشورهای بزرگ و صاحب نام فرانسه است. در کشور فرانسه، اداره تنظیم مقررات ارتباطات الکترونیک و پستی مسئولیت تنظیم‌گری و مشارکت در تدوین سیاست‌ها و قوانین در حوزه فضای مجازی را

به عهده دارد. همچنین، شورای ملی دیجیتال به عنوان یک نهاد مشورتی با دولت همکاری می‌کند. به طور کلی سناریوی حکمرانی فضای مجازی در فرانسه شامل حضور نمایندگان دانشگاه و فعالان بخش خصوصی در شورای ملی دیجیتال، تأکید بر استقلال، بی‌طرفی و تنظیم‌گری داده محور، تلاش برای همکاری با کشورهای عضو اتحادیه اروپا، ایجاد پلتفرم شکایت مصرف‌کنندگان برای شنیده شدن صدای کاربران، توجه نهاد تنظیم‌گر به توسعه زیرساخت‌ها خصوصاً در مناطق دورافتاده، توجه به بی‌طرفی شبکه، حاکمیت به نیابت از مردم، تأکید بر تنظیم‌گری مشارکتی، حوزه‌های فیلترینگ و تعقیب قضایی: سایت‌های ناقض حق تألیف، محدودیت پورنوگرافی برای کودکان، سایت‌های منتسب به جهادگرایان حضور فعال در IGF می‌باشد (پورشیرازی، ۱۳۹۸). در ادامه این پژوهش حکمرانی برخی دیگر از کشورها در فضای مجازی بیان می‌شود. در کشور عزیز ما ایران، سیاست‌های خاصی برای کنترل فضای مجازی و حکمرانی بر آن در نظر گرفته شده است. این راه‌کارها شامل حضور فعالانه در فضای مجازی خصوصاً از طریق زیرساخت‌های فناورانه، کنشگری هوشمند با به خدمت گرفتن ظرفیت نهادهای فعال، تکمیل و راه‌اندازی و بهره‌برداری از شبکه ملی اطلاعات، ملی‌سازی داده و استفاده از داده‌ها به منظور حاکمیت سایبری، ایجاد نظام حقوق بین‌الملل برای کاهش اختیارات آمریکایی‌ها، تاسیس شرکت‌های بزرگ غیردولتی با رویکرد فراملی و بازکردن میدان نوآوری و توسعه و به کارگیری حکمرانی سایبری کشور در حل معضلات اساسی جامعه و اولویت‌های کلان کشور می‌باشد (غلامی، ۱۳۹۹).

در کشور استرالیا با اجرای پروژه‌ی پهن‌بند به منظور توسعه‌ی اینترنت ملی، کمک به کسب و کارهای نوپا با سیاست‌های حمایتی نظیر داده‌های باز و آشنا ساختن مردم استرالیا برای استفاده از فناوری‌های نوین به منظور مشارکت در اقتصاد مدرن، تأکید بر تربیت نیروهای خبره در بخش‌های مختلف کوشیدند تا حکمرانی درستی بر داده‌ها و فضای مجازی داشته باشند (رضاپور، ۱۳۹۹). در کشور کره جنوبی، فضای مجازی و صنعت ICT به عنوان یک عامل رشد اقتصادی مطرح است. دولت کره، در برابر تغییرات در ساختارهای صنعتی، توزیع درآمد و شیوه زندگی به طور فعال عمل می‌کند و همواره از این تغییرات استقبال می‌کند تا با فرصت‌هایی که انقلاب صنعتی چهارم فراهم می‌آورد، با رویکردی مثبت روبرو شود. دولت کشور کره معتقد است این تغییرات را باید به عنوان فرصت‌هایی برای رسیدن به رفاه ملی تلقی کرد و با مشارکت فعال، آسایش و آرامش را برای عموم مردم کره جنوبی به ارمغان آورد. سناریوی حکمرانی فضای مجازی در کره جنوبی شامل حرکت به سمت انقلاب صنعتی چهارم با رویکرد اقتصادی و ملی، ایجاد یک اکوسیستم برای استفاده از تکنولوژی، نیروی انسانی و صنعت برای مواجهه با انقلاب چهارم صنعتی، حرکت به سوی تبدیل شدن کره به کشور پیشرو در بخش نرم‌افزاری حوزه فناوری‌های فضای مجازی در جهان، توجه به صنعت و تجاری‌سازی صنایع به مثابه پیشران فضای مجازی، اتخاذ رویکرد ارتقای کیفیت زندگی برای جامعه از طریق امکانات فضای مجازی: پاسخ هوشمند به مشکلات با جامعه اطلاعاتی، پیشگیری از حوادث و تقویت ایمنی زندگی و تلاش برای ایجاد الگوی حکمرانی چند ذریبطی می‌باشد (پورشیرازی، ۱۳۹۸).

## ۸ نتیجه گیری

حکمرانی در فضای مجازی و کنترل و تسلط بر شرکت‌های بزرگ تا حد زیادی وابسته به میزان قدرت و نفوذ کشورهای بزرگ در آن منطقه و استراتژی و ساختار سیاسی کشورهای وابسته یا تحت شعاع آنها، بستگی دارد. هر کدام از کشورهای منطقه برای اینکه بتوانند حکمرانی تأثیرگذاری در فضای مجازی داشته باشند باید برای آن راهکارهای کنترلی و قواعد خاصی در نظر بگیرند. همان‌طور که گفته شد، کشورهای دسته اول و صاحب نام برای پیشبرد اهداف سیاسی و منافع خود با کنترل کشورهای تحت سلطه خود از طریق شرکت‌های وابسته خود و اعمال فشار بر آنها به اهداف خود در آن منطقه و دیگر سرزمین‌ها دست می‌یابند. کشور ایران نیز برای اینکه از فضای مجازی به نفع خود سود ببرد باید تا حدی زیادی به قوانینی که پایه‌گذاری کرده است، بیش از پیش جامع عمل ببوشاند و روی شرکت‌های خصوصی بزرگ برای رقابت در عرصه جهانی سرمایه‌گذاری داشته باشد.

## مراجع

- [۱] احمدی، فیروزه؛ مشهدی، علی؛ عطریان، فرامرز، ۱۳۹۹. سهم فضای مجازی در تحولات حکمرانی الکترونیک با تاکید بر تضمین شهروندی، دوره ۱۲، شماره ۸، ۱۳۵-۱۵۰.
- [۲] باستانی، سوسن؛ بهشتی زواره، مژگان، ۱۳۹۴. نقش شبکه‌های اجتماعی در حاکمیت شرکتی، سال پنجم، شماره ۱۷، ۱۳-۳۷.
- [۳] باقرپور شیرازی، امیر رضا، ۱۳۹۸. حکمرانی چند ذی ربطی فضای مجازی، پژوهشگاه مرکز ملی فضای مجازی - گروه مطالعات فرهنگی و اجتماعی.
- [۴] باقرپور شیرازی، امیر رضا، ۱۳۹۸. حکمرانی فضای مجازی در کشور آلمان، پژوهشگاه مرکز ملی فضای مجازی - گروه مطالعات فرهنگی و اجتماعی.
- [۵] باقر پور شیرازی، امیر رضا، ۱۳۹۸. حکمرانی فضای مجازی در کشور کره جنوبی، پژوهشگاه مرکز ملی فضای مجازی - گروه مطالعات فرهنگی و اجتماعی.
- [۶] خاندوزی، سید احسان، ۱۳۸۹. الزامات دولت تنظیم‌گر در اقتصاد ایران، مجلس و راهبرد دوره ۱۷، شماره ۶۴، ۴۱-۸۰.
- [۷] شافوزایی، حمید؛ سلیمی زاده، لاله؛ ۱۳۹۶. بررسی تأثیرات ساختار سرمایه شرکت، اندازه هیات مدیره بر مدیریت سود شرکت‌های پذیرفته شده بورس اوراق بهادار تهران، نشریه پژوهش‌های جدید در مدیریت و حسابداری، دوره جدید - شماره ۳، ۵۹-۷۵.
- [۸] عباس‌زاده، محمدرضا؛ حصارزاده، رضا؛ جباری نوقایی، مهدی، ۱۳۹۴. عارفی اصل، سولماز؛ فراتحلیل حاکمیت شرکتی و تحلیل سود، دوره ۲۲، شماره ۱، ۵۹-۸۴.
- [۹] غلامی، رضا؛ پور حیدر، احمد، ۱۳۹۹. الگوی شش ضلعی حکمرانی فضای مجازی در جمهوری اسلامی ایران برای بازه زمانی پنج ساله، دوره ۲۰، شماره ۶، ۱-۲۶.
- [۱۰] قنبری، سمیه، ۱۳۹۹. دیپلماسی سایبری روسیه برای تحول در رژیم حکمرانی فضای مجازی، دوره ۱۰، شماره ۱۲، ۱۳۹-۱۷۴.
- [۱۱] کیان‌خواه، احسان، ۱۳۹۸. چالش‌های راهبردی حکمرانی در فضای سایبر، سال ۹، شماره ۳۴، ۱۵۳-۱۷۴.

- [۱۲] مهدی رضاپور، محمد، ۱۳۹۸. حکمرانی فضای مجازی در کشور چین، پژوهشگاه مرکز ملی فضای مجازی - گروه مطالعات فرهنگی و اجتماعی.
- [۱۳] مهدی رضاپور، محمد، ۱۳۹۸. حکمرانی فضای مجازی در کشور استرالیا، پژوهشگاه مرکز ملی فضای مجازی - گروه مطالعات فرهنگی و اجتماعی.
- [۱۴] محمدی، حافظ، ۱۳۹۹. چالش‌های حکمرانی فضای مجازی و ارائه راهکارها برای جمهوری اسلامی ایران، دوره ۱۹، شماره ۵.
- [۱۵] مشبکی، اصغر؛ موسوی خانی، مرتضی، ۱۳۷۳. نقش شرکت‌های فراملیتی در مدیریت تحولات جهان معاصر و آینده، دوره ۸، شماره ۲، ۴۵-۷۶.
- [۱۶] یآوری، اسدالله، ۱۳۹۳. درآمدی بر مفهوم تنظیم‌گری حقوقی، دوره ۵، شماره ۲، ۶۲۹-۶۴۷.



## بررسی جرم‌شناختی بزهکاری سایبری با تأکید بر نظریه‌ی فعالیت روزمره

سید علی شریفی<sup>۱</sup>

<sup>۱</sup> دانشجوی کارشناسی ارشد حقوق کیفری اطفال و نوجوانان، دانشکده حقوق و علوم سیاسی، دانشگاه تهران  
sharifi1997@ut.ac.ir

### چکیده

گسترش فناوری و استفاده از فضای سایبر، کوچ بزهکاران دنیای واقعی به دنیای مجازی را به دنبال داشته و جرائم نوینی را در بستر اینترنت ایجاد نموده است. منظور از بزه سایبری مجموعه فعالیت‌های مجرمانه‌ای است که در آن‌ها رایانه یا شبکه به عنوان ابزار، هدف یا بستری برای انجام این فعالیت‌ها به کار گرفته می‌شود. نظریه‌ی فعالیت روزمره به عنوان یکی از نظریه‌های مهم جرم‌شناسی در حوزه‌ی جرایم سایبری وجود سه عامل مهم یعنی وجود بزهکار بالقوه، حضور آماج مناسب به عنوان بزه‌دیده‌ی جرم و نیز فقدان نگهدارنده‌ی توانا را در ارتکاب جرم اینترنتی مؤثر می‌داند. این مقاله با تکیه بر مفاهیم مذکور در این نظریه با استفاده از روش توصیفی-تحلیلی و از طریق منابع کتابخانه‌ای به دنبال تبیین مؤلفه‌های مربوط به بزهکاری سایبری بوده و اقدامات لازم از جمله تدابیر مربوط به پیشگیری وضعی را به عنوان راه‌حل کاهش نرخ جرایم سایبری پیشنهاد می‌نماید.

**کلمات کلیدی:** فضای سایبری، بزهکاری سایبری، فعالیت روزمره، جرم‌شناسی، پیشگیری وضعی.

### ۱ مقدمه

در طی دهه‌های اخیر و با پیشرفت و توسعه‌ی فناوری، ابنای بشر به موازات زندگی در دنیای واقعی، تجربه‌ی زیست نوینی را در دنیای سایبر به دست آورده است. این فضا علیرغم منافع بسیاری که برای زندگی انسان فراهم داشته، چالش‌های جدیدی را نیز پیش روی او قرار داده است. یکی از این چالش‌ها، مهاجرت بزهکاران دنیای واقعی به فضای سایبر و نیز شکل‌گیری انواع و اقسام جدیدی از جرایم مخصوص به فضای مجازی است. ویژگی‌هایی همچون ناشناس بودن هویت افراد و فقدان امکانات مناسب جهت شناسایی متهمین، سرعت بسیار زیاد تبادل و تغییر اطلاعات، عدم حضور کنترل‌گران بیرونی و اجتماعی، جهانی بودن و عدم وابستگی به منطقه‌ی جغرافیایی خاص و... فضای مجازی را به محلی ایمن برای ارتکاب جرم بدل ساخته است.

از ابتدای ایجاد اصطلاح جرم سایبری و ارتکاب اولین جرایم در این فضا، جرم شناسان با استفاده از نظریه‌های گوناگون به بررسی ابعاد مختلف این گونه جرایم پرداخته و درصدد تبیین عوامل مؤثر بر ارتکاب این جرایم و نهایتاً کاهش نرخ بزهکاری سایبری برآمدند. هرچند که به واسطه‌ی جدید بودن موضوع، نظریات مترقیانه‌ی جرم‌شناسی آنچنان که باید هنوز شکل نگرفته است لکن نوآوری‌های جرم شناسان در این زمینه قابل توجه می‌باشد. نظریه‌ی «انتقال فضا» یکی از این ابتکاراتی است که با عبور از جرم‌شناسی سنتی، به دنبال بررسی علل و عوامل وقوع جرم در فضای مجازی با تکیه بر ساختارها و ویژگی‌های مرتبط با فضای سایبری است. نظریات نوین جرم‌شناسی، مانع از به‌کارگیری نظریات سنتی جرم‌شناسی برای تبیین علل و عوامل بزهکاری در این حوزه نخواهد بود. چرا که با وجود تفاوت‌های عمده میان دنیای واقعی و مجازی با یکدیگر، بسیاری از مؤلفه‌های مربوط به بزهکاری به‌صورت مشترک میان این دو فضا وجود دارد. مکاتب جرم‌شناسی سنتی، به‌طورکلی عوامل وقوع بزهکاری در سه گروه علل زیستی، علل روانی و علل محیطی - اجتماعی تقسیم‌بندی نموده و نظریات خود را ذیل هر یک از این سه گروه بیان می‌نماید. نظریه‌ی فعالیت روزمره یکی از نظریات سنتی جرم‌شناسی است که ذیل علل محیطی - اجتماعی قرار گرفته و وقوع بزه را از منظرهای گوناگون مورد بررسی قرار می‌دهد. در این نوشتار، ابتدائاً به شناخت انواع جرایم سایبری (بخش اول) پرداخته؛ سپس با تبیین نظریه‌ی فعالیت روزمره در ساحت محیط سایبری (بخش دوم)، راهکارهایی برای کاهش نرخ بزه سایبری (بخش سوم) ارائه خواهد شد.

## ۲ جرایم سایبری

جرایم سایبری، همچون دیگر حوزه‌های مرتبط با فناوری سیر تطور و تکامل خود را از شکل بسیط و مضیق، به اشکال پیچیده و گسترده طی نموده است. تا اواخر دهه‌ی ۱۹۸۰ میلادی، جرایم تنها در حوزه‌ی کامپیوتر و به‌صورت ساده در خصوص داده‌ها و برنامه‌های رایانه‌ای از طریق سرقت و کپی برنامه‌ها انجام می‌گرفت. پس از آن، در دهه‌ی ۱۹۹۰ میلادی، جرایم علیه داده‌ها شکل پیچیده‌تری به خود گرفت و جرایم علیه فناوری اطلاعاتی و ماهواره‌های مخابراتی نیز ارتکاب می‌یافت. در نهایت با گسترش اینترنت و در اختیار عموم قرار گرفتن فناوری مفهوم جرم سایبری نیز ایجاد شد (ابوذری، ۱۳۹۱: ۲۰).

جرم سایبری به صورت‌های گوناگون توسط اندیشمندان تعریف شده است. مارکو گرکی، هرگونه فعالیت که در آن رایانه یا شبکه ابزار، هدف یا مکانی برای فعالیت تبهکاری بکار می‌رود را جرم سایبری تعریف نموده است. (ابوذری، ۱۳۹۱: ۲۱) کنوانسیون جرایم سایبری نیز با احصای مصادیق مرتبط، اقدام به تعریف جرم سایبری نموده است؛ از نگاه این کنوانسیون، ۵ گروه از جرایم سایبری وجود دارد که عبارت است از: الف) جرایم علیه محرمانگی، تمامیت و دسترسی‌پذیری ب) جرایم مرتبط با رایانه ج) محتوای هرزه‌نگاری د) نقض حق نشر ه) محتوای ضد بیگانه و نژادپرستانه. لازم به ذکر است که قانون جرایم رایانه‌ای مصوب ۱۳۸۸ مجلس شورای اسلامی نیز با پیروی از کنوانسیون جرایم رایانه‌ای، تقسیم‌بندی مشابهی را برای این گونه جرایم ذکر نموده است. از میان تعاریف گوناگون در مجموع می‌توان جرم سایبری را معطوف به جرایمی دانست که در یکی از سه حوزه‌ی زیر ارتکاب می‌یابد: الف) جرایمی که رایانه در آن به‌مثابه‌ی موضوع و آماج جرم مورد

استفاده قرار می‌گیرد. برای مثال، در سرقت رایانه‌ای، اطلاعاتی که در یک رایانه ذخیره شده است مورد تجاوز و هتک قرار می‌گیرد و در آن رایانه به‌عنوان موضوع سرقت خواهد بود. ب) جرایمی که در آن رایانه به‌عنوان ابزار جرم بکار گرفته می‌شود. برای نمونه، پورنوگرافی اطفال و نوجوانان امری مستقل از رایانه و سامانه‌های رایانه‌ای می‌باشد لکن استفاده از رایانه و فضای سایبر در تسهیل ارتکاب این جرم بسیار مؤثر می‌باشد. ج) جرایمی که به‌طور خاص مرتبط با رایانه می‌باشد و مشابه آن در محیط واقعی قابل مشاهده نیست. جرم‌ها نمودن رایانه مثال خوبی برای این دسته از جرایم است.

## ۱.۲ بزهکاران سایبری

بزهکاران سایبری در مقایسه با افرادی که در فضای واقعی مرتکب جرم می‌شوند تفاوت‌های مهمی دارند. این تفاوت‌ها به دلیل آن است که ارتکاب بزه در محیط سایبری نیازمند توانمندی‌های خاصی از قبیل آشنایی با فناوری‌ها و فناوری‌های مرتبط با حوزه‌ی سایبر است و بزهکاران در این محیط دارای توانایی‌های فنی و تخصصی بیشتری نسبت به مجرمین عادی هستند. مجرمین این حوزه به دو دسته تقسیم می‌شوند. دسته‌ی اول، اشخاصی هستند که جرم را در محیط‌های واقعی نیز مرتکب می‌شوند و فعالیت‌های مجرمانه‌ی خود را به فضای سایبری انتقال داده‌اند. این افراد عمدتاً به دنبال کسب منفعت مالی از فضای سایبر هستند و با همین انگیزه نیز مرتکب جرم می‌گردند. دسته‌ی دوم، شامل اشخاصی است که در فضای واقعی شهروندان قانون‌مداری بوده و رفتار بهنجاری از آن‌ها انتظار می‌رود، لکن در محیط مجازی و به دلیل ویژگی‌های خاص این محیط مرتکب اعمال مجرمانه می‌شوند.

مطالعات نشان می‌دهد افرادی که محیط برخط را برای سرگرمی انتخاب کرده‌اند گرایش بیشتری به ارتکاب رفتارهای مجرمانه دارند؛ در مقابل، افرادی که فضای مجازی و به‌ویژه شبکه‌های اجتماعی را امری فراتر از سرگرمی‌های ناپایدار و زودگذر تلقی می‌نمایند و علقه‌های اجتماعی و نشانه‌های وفاداری به این محیط را از خود نشان می‌دهند، احتمال کمتری دارد که مرتکب جرایم در فضای مجازی شوند. گردشگران فضای مجازی که این محیط را صرفاً سرگرمی تلقی می‌کنند در جرایم کمتر فنی‌تری همچون توهین و هرزه‌نگاری را دنبال می‌کنند اما مجرمین با مهارت فنی بالا عمدتاً جرایم مهم‌تری از قبیل آزار سایبری، هک و ویرانگری را مرتکب می‌شوند. اساساً افرادی که به دلیل وجود علقه‌های اجتماعی و ساعات طولانی حضور در فضای مجازی و شبکه‌های اجتماعی شهروندان فضای مجازی قلمداد می‌شوند، نسبت به گردشگران این محیط بیشتر مرتکب نقض هنجارهای گروهی و بزه‌های جدی‌تر می‌گردند (ویلیامز، ۱۳۹۰: ۲۴).

در تقسیم‌بندی دیگری، مجرمین سایبری به چهار گروه تقسیم می‌شوند. گروه اول، مجرمین کینه‌جو هستند که دارای شخصیتی بدذات بوده و بیشتر از دیگران اقدام به تهدید و آزار بزه دیدگان می‌نمایند؛ در رفتار این گروه تداوم فعالیت‌های آزاردهنده به‌وفور یافت می‌شود. گروه دوم، مجرمینی هستند که قربانیان را به‌صورت آرام و به دور از هیاهو تعیین کرده و از طریق رفتارهای تهدیدآمیز اقدام به آزار آن‌ها می‌نمایند. گروه سوم، با ایجاد رابطه‌ی صمیمانه با بزه دیده به دنبال عقده‌گشایی و حل مشکلات روحی خود هستند و درنهایت گروه چهارم، مجرمینی هستند که دارای مهارت بالای فنی بوده و به‌صورت جمعی مرتکب جرایم سایبری می‌شوند. این گروه از حیث جرم‌شناسی و عمق خساراتی که وارد می‌نمایند، از اهمیت بالاتری

برخوردار هستند (رستگار صولتی، ۱۳۹۴: ۳۷).

## ۲.۲ بزه‌دیدگی سایبری

قربانیان در فضای سایبری ویژگی‌های متمایزکننده‌ای نسبت به بزهکاران فضای واقعی دارد. بر اساس آمار مراجع رسمی در سال ۱۳۹۶ استفاده‌کنندگان زیر ۱۸ سال از اینترنت در ایران، نزدیک به بیست میلیون نفر بوده است (اقتصاد نیوز، کد خبر: ۱۶۸۵۲۰). این امر نشان‌دهنده‌ی حضور بسیار پررنگ اطفال و نوجوانان در اینترنت و به خصوص شبکه‌های اجتماعی به‌مثابه‌ی افرادی بدون توان حفاظت از خود در میان انبوهی از بزهکاران بالقوه می‌باشد. در یک تقسیم‌بندی کلی از دیدگاه هنتینگ، بزه‌دیدگان فضای سایبری را می‌توان به دو گروه بزه‌دیدگان بی‌گناه یا معصوم و بزه‌دیدگان مقصر یا بی‌احتیاط تقسیم‌بندی نمود. بزه‌دیدگان بی‌گناه افرادی هستند که حضور در این فضا را با اقداماتی از جمله نصب آنتی‌ویروس، عدم مراجعه به لینک‌های نامعتبر و مشکوک و... تأمین نموده و هوشیاری نسبتاً مطلوبی را نسبت به مخاطرات موجود در فضای مجازی از خود نشان می‌دهند. در مقابل این افراد، گروهی از استفاده‌کنندگان از اینترنت و فضای مجازی با خواندن هرزنامه‌ها، دانلود بدافزارها، نصب فیلترشکن، گشت‌وگذار بی‌مورد در سایت‌های غیرقانونی بی‌احتیاطی خود را در استفاده‌ی از این فضا نشان می‌دهند. از نگاه شیندر، بزه‌دیدگان سایبری در شش گروه کلی تقسیم‌بندی می‌شوند: ۱- تازه‌واردان سایبری و افرادی که آشنایی با مخاطرات و ویژگی‌های فضای مجازی ندارند. ۲- افراد ساده‌لوح و زودباور که عمدتاً شامل دو گروه اطفال و افراد مسن و کهن‌سال می‌شوند. ۳- اشخاص ناتوان و آسیب‌پذیر که شرایط ویژه‌ی فردی آن‌ها منجر به بزه‌دیدگی آن‌ها می‌شود. ۴- افرادی که با اعمال و رفتارهای خود از جمله حضور دائم در چت‌روم‌ها، سایت‌های مستهجن و... زمینه‌ی بزه‌دیدگی‌شان را فراهم می‌کنند. ۵- قربانی‌نمایی که با حيله و فریب به مقامات پلیس اعلام بزه‌دیدگی می‌کنند در حالی که واقعاً بزه دیده نشده‌اند. ۶- بزه‌دیدگان بدشانس که به‌صورت اتفاقی مورد بزه‌دیدگی واقع می‌شوند (ابوذری، ۱۳۹۱: ۳۴).

مسئله‌ی دیگری که در خصوص بزه‌دیدگان سایبری باید به آن توجه نمود آن است که این افراد در صورتی که یک‌بار موضوع بزه قرار بگیرند، احتمال بزه‌دیدگی ثانویه در آن‌ها بسیار زیاد است. در سال ۱۹۹۲، ۶۳ درصد بزه‌دیدگان جرایم مالی و ۷۷ درصد جنایات علیه اشخاصی انجام شد که دارای سابقه‌ی بزه‌دیدگی بودند (ابوذری، ۱۳۹۱: ۴۴).

بررسی موارد فوق نشان می‌دهد که در اینگونه جرایم، توجه به بزه‌دیده نیز به‌موازات توجه به بزهکار اهمیت دارد؛ بنابراین دستیابی دقیق‌تر به عوامل و علل وقوع بزه نیازمند آن است که نظریاتی از جرم‌شناسی مورد استفاده قرار گیرد که نگاه خود را بیش از بزهکار به شرایط وقوع جرم و قربانی بالقوه‌ی جرم به‌عنوان یکی از ارکان مداخله‌گر معطوف دارد. نظریه‌ی فعالیت روزمره یکی از این نظریات است که با تکیه بر عناصر سه‌گانه‌ی وقوع جرم اقدام به تحلیل عوامل مداخله‌گر می‌نماید.

### ۳ نظریه‌ی فعالیت روزمره

در تعریفی ساده و کلی، عوامل محیطی مؤثر در وقوع جرایم سایبری علیه اطفال و نوجوانان را مجموعه‌ی عوامل به وجود آورنده‌ی جرم می‌دانند که مستقل از شخص بزهکار تعریف می‌شود. این عوامل، بر اراده‌ی شخصی افراد تأثیرگذار بوده و آن‌ها را به سمت ارتکاب جرایم و تخلفات و سرپیچی از هنجارهای جامعه دعوت می‌نماید. گستردگی مصادیق این تعریف، فراگیر بودن و مهم‌تر از همه در معرض بودن همه‌ی افراد جامعه در برابر این عوامل باعث شده است تا آن‌ها را مهم‌ترین و اصلی‌ترین عامل وقوع جرایم بدانیم. بدیهی است که بسیاری از اختلالات روانی منجر به ارتکاب جرایم در افراد، زاینده‌ی شرایط محیطی و اجتماعی آن‌ها بوده و در مقابل، عوامل زیستی در صورتی به پدیده‌ی مجرمانه منجر می‌گردد که شرایط و عوامل محیطی بستر مناسب ظهور و بروز آن‌ها را مهیا نماید. این امر، خود نمایانگر اهمیت عوامل محیطی و تأثیر بسیار آن‌ها بر سایر عوامل و مؤلفه‌های مؤثر در وقوع جرایم است.

از اوایل دهه ۱۹۷۰ میلادی، جرم‌شناسان تمرکز خود را از مطالعات مربوط به بزهکاران، به مطالعات مربوط تأثیر جرم بر روی بزه دیدگان تغییر دادند. نظریه فعالیت‌های روزمره نیز در زمانی مطرح شد که نظام عدالت کیفری تأکید خود بر روی موضوعات بزه دیدگی را آغاز کرده بود. در این زمان نظریه‌ی سبک زندگی و نظریه‌ی فعالیت‌های روزمره به‌عنوان دیدگاه‌های نظری عقلانی در جامعه‌شناسی ارائه شدند. این دو نظریه برای تحلیل علت وجود احتمال بیشتر بزه دیده شدن افراد با توجه به فعالیت‌ها، تعاملات و ساختار اجتماعی سبک‌های زندگی خویش مورد استفاده قرار گرفتند (Williams & McShane, 1999: 134).

تحقیقات پیشین هیندلینگ و همکارانش به مسئله نقش سبک زندگی روزانه افراد چه در محل کار و چه در منزل بر بزه دیده شدن افراد می‌پرداخت. مسئله‌ی تأثیر نقش موقعیت اجتماعی فرد بر الگوهای سبک زندگی نیز مورد بحث این دو محقق بوده است؛ بنابراین به نظر می‌رسد که سه عامل اصلی در پیش‌بینی بزه دیده شدن یک فرد وجود داشته باشد. اول، ضرورت وجود یک فرد با انگیزه به‌عنوان بزهکار. دوم، ضرورت وجود هدفی مناسب به‌عنوان آماج جرم و بزه دیده‌ی بالقوه. سوم، عدم وجود یک نگهبان توانا برای محافظت از بزه دیده در مقابل رفتار مجرمانه‌ی بزهکار. برای تحقق بزه دیدگی نبود هرکدام از این عوامل احتمال ارتکاب جرم علیه فرد یا افراد را کاهش می‌دهد. بنابراین، ارتکاب یک بزه چه در محیط واقعی و چه در محیط مجازی مستلزم ترکیب این سه عامل با یکدیگر می‌باشد (Cohen & Felson, 1979: 590).

نظریه‌ی فعالیت روزمره به‌نوعی به دنبال گسترده‌تر نمودن یافته‌های نظریه‌ی سبک زندگی است که علاوه بر رفتارهای روزمره‌ی انسان‌ها، به بررسی فعالیت‌های شغلی و تفریحی افراد نیز می‌پردازد. فلسن، برای مناسب بودن یک فرد به‌عنوان آماج جرم، چهار ملاک را ارائه می‌کند: ۱- ارزش هدف جرم ۲- میزان تحرک هدف جرم ۳- مرئی بودن فیزیکی هدف جرم ۴- در دسترس بودن هدف جرم. (جیشانکار، ۱۳۹۵: ۳۳۶) آنچه در مورد جرایم سایبری وجود دارد آن است که هدف به‌صورت فیزیکی در مرئی و منظر بزهکار قرار ندارد.

بزهکار رایانه‌ای با استفاده از فنون ارتکابی جرم در فضای سایبری باعث می‌شود که هدف تحرک خود را از دست بدهد؛ همچنین، در دسترس بودن افراد واجد شرایط بزه دیدگی در محیط سایبر بسیار زیاد است؛

بنابراین باید جهت کنترل بزه دیدگی در این محیط، سطح توان نگرهبانی را افزایش داد. این امر با استفاده از استراتژی سخت کردن هدف صورت می‌گیرد (Yar, 2005: 410) به گفته‌ی هیندلینگ و همکاران، فعالیت‌های کاری و تفریحی مهم‌ترین عوامل در سبک زندگی افراد محسوب می‌شوند که مستقیماً احتمال بزه دیدگی افراد را تحت تأثیر قرار می‌دهند. در مورد نوجوانان حاضر در فضای مجازی باید فعالیت‌های آموزشی و تحصیلی را نیز به حوزه‌های فوق اضافه نمود. از طرف دیگر، افراد درگیر در فعالیت‌های مرتبط با زندگی بزهکارانه با احتمال بیشتری به اهداف مناسب برای بزه دیدگی تبدیل می‌شوند و دلیل بزه دیدگی آن‌ها عدم تمایل به مواجهه با نظامات حقوقی و کیفری است (جیشانکار، ۱۳۹۵: ۳۳۷).

با تحول فناوری جدید، فعالیت‌های روزمره‌ی کودکان از بازی‌هایی همچون دوچرخه‌سواری و بازی با عروسک‌ها به بازی‌های ویدئویی و اینترنت تغییر یافته است. در سال ۲۰۰۶، حدود ۸۷ درصد از جوانان از اینترنت استفاده می‌نمودند که این آمار به طرز شگفت‌انگیزی افزایش داشته است. همگام با ظهور فناوری‌های جدید بزه دیدگی این افراد در فضای مجازی نیز افزایش داشته است. از نگاه سمپسون، کاهش احتمال بزه دیدگی با استفاده از تمهیدات حفاظتی است. این پژوهش بیان می‌دارد که نمی‌توان فعالیت‌های نوجوانان را در اینترنت از جهت زمانی محدود نمود و تمهیدات حفاظتی نیز برای کاهش بزه دیدگی این افراد کافی نیست؛ بنابراین بهتر است آموزش مخاطرات به نوجوانان را هم‌زمان با استفاده از اقدامات حفاظتی افزایش داد (جیشانکار، ۱۳۹۵: ۳۵۸).

در نگاه جرم‌شناسی سنتی می‌توان ۳ نگرهبان توانا را برای کاربران اینترنت مفروض داشت. برنامه‌های ضد ویروس، برنامه‌های ضد جاسوسی و تدابیر پیشگیری‌کننده از ورود (فایروال) (Moore, 2005: 2) در صورتی که برنامه‌های ضد ویروس، بدافزاری را شناسایی نمایند که امنیت کاربر را به مخاطره بیندازد آن را منزوی نموده و یا از بین می‌برد. نرم‌افزارهای ضد جاسوسی نیز در راستای حذف توانمندی‌های بدافزارهای جاسوسی هستند که با استفاده از رهگیری اطلاعات کاربری و رمزهای عبور کاربران، اقدام به ارتکاب جرم سرعت رایانه‌ای می‌نمایند. تدابیر پیشگیری‌کننده از ورود نیز، اجازه‌ی ورود بدافزارها را به درون سامانه‌های کامپیوتری را نمی‌دهد و از این طریق حفاظت و امنیت کاربر را تأمین می‌نماید. به‌طور کلی، احتمال بزه دیدگی سایبری برای افرادی که به شکل منظم و روزآمد نرم‌افزارهای امنیتی خود را بروزرسانی می‌نمایند، استفاده‌ی آن‌ها از اینترنت دائمی و مداوم نبوده و رفتارهای خطرناک آنلاین را نیز انجام نمی‌دهند بسیار کمتر از سایر افراد است. این موضوع نشان می‌دهد که تدابیر حفاظت‌کننده نیز تا حد زیادی تحت تأثیر رفتارها و آموزش‌های قبلی داده‌شده به کاربران فضای مجازی است. در ادامه، راهکارهای مستقل از کاربران اینترنت برای کاهش احتمال بزه دیدگی سایبری بررسی خواهد شد.

## ۴ راهکار کاهش نرخ جرایم سایبری

همانگونه که در مباحث قبلی مطرح گردید، استفاده از تدابیر حفاظت‌کننده‌ی سنتی و وابسته به کاربر نمی‌تواند به اندازه‌ی کافی برای کاهش جرایم سایبری مؤثر واقع شود. چرا که استفاده از این تدابیر نیازمند آموزش کاربران این حوزه می‌باشد در حالی که بسیاری از کاربران این حوزه را اطفال و نوجوانان و یا افراد



فاقد دانش فنی شامل می‌گردد. در مقابل، استفاده از تدابیر حفاظت کننده‌ی هوشمند می‌تواند مستقل از اراده‌ی کاربر از وی حفاظت نموده و به‌عنوان نگهبانی توانا در عرصه‌ی فضای مجازی ظاهر گردد. اساساً از آنجایی که در جرایم فضای مجازی از عنصر فناوری استفاده می‌گردد الزاماً باید برای پیشگیری از آن‌ها نیز از فناوری کمک گرفت.

هوش مصنوعی به‌عنوان یکی از دستاوردهای فناوری که به‌عنوان هنر اندیشیدن ماشین و عمل نمودن آن مانند انسان تعریف می‌شود می‌تواند در پیشگیری از جرایم از طریق کارکردهای گوناگون آن بسیار مؤثر واقع شود. برای مثال، آزار و اذیت سایبری می‌تواند مشکلات زیادی را برای بزه دیدگان علی‌الخصوص افراد دارای ناپایداری عاطفی و اختلالات روانی ایجاد نماید؛ در اینگونه موارد هوش مصنوعی با به‌کارگیری الگوریتم‌های تشخیص خود، این افراد را شناسایی نموده و با تشخیص هوشمند محتوای آزاردهنده از وصول اینگونه محتواها به بزه دیدگان بالقوه جلوگیری نماید (Rakhmator, 2022: 125).

استفاده از این روش تاکنون مورداستفاده‌ی بسیاری از کشورها نیز بوده است. در سال ۲۰۱۲ بانک‌های هلند ۸۰ میلیون یورو خسارت ناشی از جرایم سایبری را متحمل شدند؛ اما پس از آن با استفاده از فناوری نوین هوش مصنوعی و تجزیه و تحلیل داده‌ها و شناسایی رفتار غیرمعمول مشتریان اقدام به شناسایی و پیشگیری از ارتکاب دوباره‌ی جرایم مالی سایبری نمودند (J.Halt, 2019: 220).

## ۵ نتیجه‌گیری

جرایم سایبری امروزه از واقعیت‌های عصر حاضر در دنیای مجازی به شمار می‌آید که روزبه‌روز بر شمار افراد درگیر با این پدیده افزوده می‌شود. با توجه به نظریه‌ی فعالیت روزمره که یکی از نظریات مهم در جرم‌شناسی سنتی است، وجود یک نگهبان توانا در محیط مجازی می‌تواند از بروز بزهکاری جلوگیری و به‌عنوان سدی مستحکم در مقابل بزهکار بالقوه و بزه دیده‌ی بالقوه عمل نماید. تدابیر حفاظت کننده‌ی سنتی که نیازمند اعمال از طریق کاربر و یا افراد مرتبط با حوزه‌ی بزهکاری سایبری هستند نمی‌تواند در مقابل فناوری‌های پیچیده‌ی بکار رفته در اینگونه جرایم مؤثر واقع شود و پیشگیری از آن‌ها نیازمند استفاده از تدابیر فناورانه‌ای است که بتواند مستقل از اراده‌ی انسان عمل نماید. فناوری هوش مصنوعی که خود منبعت از گسترش و توسعه‌ی فناوری به‌ویژه در حوزه‌ی سایبری است می‌تواند به‌مثابه‌ی سدی مستحکم و مستقل از اراده‌ی افراد در مقابل بزهکاران فضای مجازی عمل نماید.

## مراجع

- [۱] ابوذری، مهرنوش، جرم‌شناسی جرایم سایبری، چاپ اول، نشر میزان، ۱۳۹۵.
- [۲] پایگاه خبری تحلیلی اقتصاد نیوز، قابل دسترسی از: [www.eghtesadnews.com](http://www.eghtesadnews.com)
- [۳] جیشانکار، کی، جرم‌شناسی فضای مجازی کشف جرایم اینترنتی و رفتار مجرمانه، ترجمه‌ی دکتر حمیدرضا ملک محمدی، چاپ اول، انتشارات میزان، ۱۳۹۴.
- [۴] رستگار صولتی، محمد سعید، علت‌شناسی بزه دیدگی نوجوانان در فضای سایبر، پایان‌نامه کارشناسی ارشد، دانشکده حقوق دانشکدگان فارابی دانشگاه تهران، ۱۳۹۴.

- [۵] ویلیامز، متیو؛ ترجمه: منفرد، محبوبه؛ جلالی فراهانی، امیرحسین، بزه کاری مجازی: بزه، انحراف و مقررات گذاری بر خط، چاپ اول، انتشارات میزان، ۱۳۹۱.
- [6] Cohen, L.E. & Felson, M, "Special change and crime rate trends: A routine activity approach," American Sociological Review, 1979.
- [7] Dilmurod, Rakhmatov, "Methods and Effectiveness of the Use of Artificial Intelligence in the Fight Against Cyberbullying," Journal of Academic Research and Trends in Educational Sciences. Volume1, Issue4, 2022.
- [8] Moore, R, "Cyber crime: investigating high-technology computer crime," Philadelphia, PA: LexisNexis, 2005.
- [9] Thomas, J. Holt, "Cybercrime Through an Interdisciplinary Lens," Routledge, 2019.
- [10] Williams, F.P. & McShane, M.D, "Criminological theory," Upper Saddle River, NJ: Prentice Hall, 1999.
- [11] Yar, M, "The novelty of cybercrime: An assessment in light of routine activity theory," European Journal of Criminology, 2005.

## وب تاریک و چالش‌های فراروی حقوق کیفری

پریسا حاجی زاده<sup>۱</sup>

<sup>۱</sup> کارشناسی ارشد، حقوق جزا و جرم‌شناسی، دانشگاه شیراز  
pari.hajizadeh@gmail.com

### چکیده

هنگامی که فناوری‌های ارتباطی مدرن همچون اینترنت توسط مجرمان برای تسهیل فعالیت‌هایشان استفاده می‌گردد، مجرمان باهوش به دنبال ابزارهایی هستند که به آنها کمک نمایند فعالیت‌ها و ارتباطات خود را پنهان نمایند. وب تاریک و فناوری زیربنای آن، نحوه‌ی انجام جرم و جنایت را تغییر داده است و از آن جایی که برقراری ارتباط از طریق فناوری وب تاریک به طور پیش فرض شامل رمزگذاری و ناشناس بودن است، مجرمان امروزی بیش از پیش به وب تاریک برای فرار از اجرای قانون در هنگام ریزی و اجرا تکیه می‌کنند و چالش‌های بزرگی را برای مجریان قانون در سراسر جهان ایجاد نموده‌اند. برای دانستن این که چه مشکلاتی پیش روی مجریان قانون در وب تاریک قرار دارد؛ این مقاله نگاهی به تجربه کشور‌های پیشرو و بررسی چالش‌های پررنگ در حقوق کیفری را دارد و پیشنهاداتی در این خصوص ارائه می‌نماید.

**کلمات کلیدی:** وب تاریک، تحقیقات سایبری، نظارت سایبری، حقوق کیفری.

### ۱ مقدمه

وب تاریک یا dark web و فناوری زیربنای آن، اساساً نحوه‌ی انجام جرم و جنایت را تغییر می‌دهد. حجم قابل توجهی از جنایات در این فضا، فرامرزی و بین‌المللی است که هریک از بازیگران اصلی آن، شواهد و عواید حاصل از جرم می‌توانند در حوزه‌های قضایی مختلف باشند. در جامعه امروزی که از نظر فناوری زیرکانه است، شیوه انجام جرم و جنایت با سرعت فزاینده‌ای در حال تغییر است. جرایم در وب تاریک، جدیدترین و تکامل‌یافته‌ترین نوع جرایم سایبری است. وب تاریک «مکانی مخفی و ناشناس است که در آن کاربران سایه به خدمات پنهان، دسترسی دارند» [۱]. به‌ویژه، بازارهایی که در آنجا میزبانی می‌شوند یک چالش حقوقی مهم ایجاد می‌کنند. این بازارها مجرمان را قادر می‌سازند تا بدون زحمت، مجموعه وسیعی از کالاها و خدمات غیرقانونی را از خانه خود خریداری کنند یا بفروشند.

فناوری‌ای که زیربنای وب تاریک است، چالشی منحصر به فرد برای مجریان قانون در سراسر جهان و قوانین کیفری به طور گسترده‌تر فراهم می‌کند. استفاده از یک شبکه خصوصی مجازی (VPN) در ارتباط با

Tor ("The Onion Router") برای اهداف رمزگذاری و امنیتی، این امکان را برای مجرمان فراهم می‌کند تا به طور ناشناس، جنایات فرامرزی را انجام دهند و به‌طور قابل توجهی به مخاطبان، فراتر از حد معمول، دسترسی پیدا کنند. آسایشی همچون خانه خودشان. مهم‌تر از همه، استفاده از ارزهای دیجیتال به‌عنوان وسیله‌ای برای پرداخت کالاها و خدمات خریداری شده در وب تاریک، این امر را تسهیل می‌کند. در نتیجه، وب تاریک، چالش‌های جدیدی به‌وجود آورده و همچنین چالش‌های سنتی قدیمی را بارزتر می‌کند.

قانون و فناوری هرکدام پیچیدگی خود را دارند و وقتی در تعامل با هم قرار بگیرند این پیچیدگی بیشتر نیز می‌شود. اگرچه، دفتر مبارزه با مواد مخدر و جرایم سازمان ملل متحد (UNODC) اعلام کرده است که: «مجریان قانون و سیستم عدالت کیفری در بسیاری از کشورها هنوز در موقعیتی نیستند که بتوانند به‌طور مؤثر با بازار آنلاین ناشناس معروف به وب تاریک مقابله کنند» [۲]. بنابراین در ابتدا وب تاریک به‌عنوان چالش نوظهور تکنولوژی برای حقوق کیفری با رویکرد توسعه دادن به تنظیم این فناوری نوظهور و سپس چالش‌های بارز موضوع را مورد تجزیه و تحلیل قرار می‌دهد که چالش ایجاد شده توسط وب تاریک را برجسته می‌نماید.

## ۲ وب تاریک، چالشی برای حقوق کیفری

اتاق‌های گفتگو و خدمات ارتباطی ناشناس در وب تاریک، آن را به یک محل ایده‌آل برای برنامه‌ریزی و هماهنگی فعالیت‌های خطرناک جنایی و تروریستی تبدیل می‌کند. به‌عنوان مثال، وب تاریک، میزبان هکرها و هکرها برای استخدام است. در آوریل ۲۰۲۱، یک مرد ایتالیایی به اتهام استخدام یک قاتل در وب تاریک برای حمله به دوست دختر سابقش با پرتاب اسید روی او و مجبور کردن او به استفاده از ویلچر، دستگیر شد. یورپل با انتشار بیانیه‌ای اعلام کرد که این شهروند ایتالیایی ۱۰۰۰۰ یورو برای استخدام قاتل از یک «وبسایت ترور اینترنتی» که در شبکه Tor میزبانی شده بود، پرداخت کرده است.

جرم در وب تاریک یک تهدید جدی برای مجریان قانون است؛ چرا که نخست، فناوری پیچیده مورد استفاده وب تاریک، دامنه وسیع آن، عدم احترام به مرزهای ملی و دشواری بار مسئولیت بر شواهد به‌دست آمده را در پی دارد. دوم، نهادهای بین‌المللی و منطقه‌ای که مسئولیت رسیدگی به جرایم وب تاریک را دارند، صلاحیت‌های محدودی دارند و نمی‌توانند تحقیقات را رهبری نمایند. سوم، تلاش حوزه‌های قضایی مختلف برای مقابله با جنایات فراملی و همکاری با یکدیگر در جهت تسهیل همکاری، مدت‌ها ناکارآمد بوده است. چهارم، در اختیار گرفتن نظارت برای دولت محلی به‌ویژه در صورت قدرتمند بودن از لحاظ ملی در جایی که موضوع فراملی نباشد، اجتناب‌ناپذیر است. پنجم، تکنیک‌های تحقیق و رویکرد نظارتی اتخاذ شده همیشه متناسب نیستند و در برخی موارد تکنیک‌های مورد استفاده با غیرقانونی بودن، محدود می‌شوند. ششم، اگرچه استفاده از بخش خصوصی برای تحقیقات در وب تاریک تا حدودی اجتناب‌ناپذیر است، ولی خطراتی را نیز در پی دارد.

## ۱.۲ ضرورت نظارت بر وب تاریک

چشم‌انداز اجرای قانون در نتیجه افزایش روزافزون فعالیت‌های مجرمانه از طریق اینترنت تغییر کرده است. در حالی که پیشرفت‌های گسترده در فناوری ممکن است ردیابی مجرمان را متمایز سازد و امروزه وب تاریک به عنوان پدیده‌ی نوظهور تکنولوژی و روی آوردن مجرمان به این فضا، نیاز ورود نظارتی به این فضا را بیش از پیش واضح نموده است و آن استفاده مجرمان از فضای وب تاریک برای حفظ ناشناس بودن و فرار از تعقیب و اجرای قانون است. برای درک بهتر از چالش مجریان قانون، سه نکته را می‌توان برشمرد. اینترنت به دو بخش دسته‌بندی می‌شود. اول، دنیای قابل رویت یا وب سطحی یا به عبارتی *visible surface web* یا *web* و دیگری، دنیای عمیق یا *deep web*. دنیای قابل رویت، هرچیزی است که می‌تواند توسط یک موتور جستجوی معمولی مانند گوگل یا یاهو نمایه شود [۲]. بنابراین، هرچیزی که از طریق موتورهای جستجو، قابل دسترسی باشد، در حوزه‌ی دنیای قابل رویت است. فراتر از این دنیا، وب عمیق است. این بخش، شامل بخش باقی‌مانده از وب است که وب سطحی آن را پوشش نمی‌دهد [۲]. این بدان معناست که؛ هرچیزی که از طریق موتور جستجو غیر قابل دسترسی باشد، به‌عنوان بخشی از وب عمیق است؛ این یعنی، هم سرورهای خصوصی که دارای مجوز هستند، اینترانت‌هایی که توسط سازمان‌های مختلف استفاده می‌شوند، یا حتی صفحات معمولی رسانه‌های اجتماعی که کاربران می‌خواهند از عموم مردم پنهان نگه دارند، باشد. بخش آخر وب، وب تاریک است.

وب تاریک، بخش کوچکی از وب عمیق است که عمداً پنهان شده است و از طریق مرورگرهای وب استاندارد، غیرقابل دسترسی است [۳]. کاربران اینترنت بدون استفاده از مرورگرهایی که برای آرایه ناشناس بودن مطلق به کاربر، اختصاص داده شده‌اند؛ قادر به دسترسی به این بخش از وب نیستند. مرورگرهایی خاص، این ناشناس بودن را برای کاربران فراهم می‌نمایند و وب تاریک را محلی برای فعالیت‌های مجرمانه و چالشی برای مجریان قانون بدل می‌نمایند.

مرورگر Tor یکی از این مرورگرهاست که کاربران تشویق می‌شوند تا با استفاده از آن، هویت خود را پنهان نموده و اتصال امن و رمزگذاری شده ایجاد نمایند. روش پیچیده رمزگذاری در این مرورگر، کاربر را از طریق رایانه‌های سایر کاربران به‌منظور پنهان کردن اطلاعات، هدایت می‌نماید [۶]. اساساً این فرایند را می‌توان مانند یک پیاز در نظر گرفت، با عبور هرلایه، هویت یک فرد را بیشتر پنهان می‌کند. علاوه بر این، مرورگر Tor چالش دیگری را نیز به وجود می‌آورد و آن، تغییر مکان سایت‌هایی است که در آنجا میزبانی می‌شوند و تغییر هر هفته‌ی آن، چالشی برای مجریان قانون در جمع‌آوری شواهد ایجاد می‌نماید؛ بر خلاف وب سطحی که مکان یا IP آن ثابت است.

مطالعه محققان کالج کینگ لندن در سال ۲۰۱۶ برای نشان دادن دامنه این چالش با استفاده از بررسی وبسایت‌های قابل دسترسی از طریق Tor (The Onion Router) نشان داد که ۱۵۴۷ سایت از ۲۷۲۳ سایت فعال در این فضا به عنوان محتوای غیرقانونی طبقه‌بندی می‌شوند [۷]. رایج‌ترین محتویات این وبسایت‌ها شامل؛ مواد مخدر، امور مالی غیرقانونی و پورنوگرافی شامل خشونت علیه کودکان و حیوانات است. به عبارتی بیش از ۵۰ درصد مواردی که در Tor میزبانی می‌شوند، غیر قانونی و نامشروع است، اگرچه در مطالعات

دیگری این رقم حتی بالاتر نیز می‌رود [۸]. از آن جایی که بازارهای موجود در وب تاریخ در فراسوی مرزها فعالیت می‌کنند و فروش آن محدود به حوزه‌ی قضایی نیست؛ به همین دلیل این بازارها، عامل کلیدی برای جنایات فرامرزی و بین‌المللی هستند. هریک از بازیگران اصلی، شواهد و عواید حاصل از جرم می‌توانند در حوزه‌های قضایی مختلف قرار داشته باشند یا حداقل این طور به نظر می‌رسند.

موارد فوق با استفاده از ارزهای دیجیتال مانند بیت‌کوین به‌عنوان روش پرداخت تشدید می‌شود. آنها جابه‌جایی وجوه را به روشی سریع، ساده و با نام مستعار تسهیل می‌کنند و از سیستم مالی رسمی به شدت اجتناب می‌کنند [۹]. چالش‌هایی که وب تاریخ ایجاد می‌کند به جرمی که در این فضاست محدود نمی‌شود و به مجرمان اجازه می‌دهد جنایات وب سطحی را نیز برنامه‌ریزی یا تسهیل نمایند.

## ۳ چالش‌های مهم حقوق کیفری

اگرچه داشتن دانش و درک مناسب از وب تاریخ و ارزهای دیجیتال توسط مجریان قانون برای بررسی جرایم این فضا آن‌ها را قدرتمند می‌سازد، در حال حاضر حتی کشورهای پیشرو در عرصه فناوری نیز با کمبود تجربه در سازمان‌های مجری قانون در انجام تحقیقات مؤثر و پیگرد قانونی جرایم مربوط به ارزهای دیجیتال روبرو هستند. بنابراین آموزش مداوم افسران در رابطه با خطرات نوظهور، لازم و ضروری است و نکته‌ی مهم تعامل بخش خصوصی برای رفع شکاف دانش اجرای قانون است. اگرچه چالش‌های حقوق کیفری در قبال جرایم وب تاریخ، تقریباً همان چالش‌های سنتی پیشین است، اما موارد تازه‌ای نیز به این چالش‌ها افزوده شده که به مهم‌ترین آنها اشاره می‌نماییم.

### ۱.۳ چالش بین‌المللی

در سطح بین‌المللی، تحقیقات برعهده اینترپل و در اروپا، یورپل و مرکز جرایم سایبری اروپایی و در سطح ملی نیز سازمان‌های مجری قضایی کشورهاست. محدودیت صلاحیت این ارگان‌ها (اینترپل و یورپل) برای مقابله با جرایم وب تاریخ، چالش مهمی است. هر دو ارگان، صلاحیت خود را از عضویت خود می‌گیرند چراکه نهادی قانونگذار نیستند و به‌تنهایی قدرت اجرایی کمی دارند و در درجه اول یک عملکرد هماهنگ کننده دارند.

جنایات بین‌المللی نیازمند پاسخ بین‌المللی هستند. نهادهای بین‌المللی و منطقه‌ای، صلاحیت رهبری تحقیقات در وب تاریخ را ندارند و نقش آنها صرفاً کمک به آژانس‌های مجری قانون ملی در همکاری با یکدیگر برای مقابله با جرایم سازمان‌یافته بین‌المللی از طریق انتشار بهترین شیوه‌ها و هماهنگ کردن واکنش آنهاست. بنابراین، اولویت در این مبارزه با قانون ملی هر کشوری است؛ چرا که هیچ مکانسیم بین‌المللی رسمی برای اطمینان از این که حوزه‌های قضایی اقدامات متقابلی را برای مقابله با جرایم وب تاریخ دارند و در حال اجرای آن هستند، وجود ندارد. بنابراین هر حوزه قضایی اختیار دارد که در این امر مشارکت نماید یا خیر و احتمال این که دولت‌های قدرتمند در این عرصه ابتکار عمل را به دست بگیرند، وجود دارد.



## ۲.۳ چالش صلاحیت

همان‌طور که برشمردیم، یکی از مسائل اساسی در برخورد با جرایم وب تاریک، این است که یک عنصر فرامرزی وجود دارد. در واقع، هریک از عوامل دخیل در ارتکاب جرم و عواید حاصل از آن، همگی می‌توانند در حوزه های قضایی مختلف باشند. در حالی که روش‌ها تغییر کرده‌اند؛ جهانی شدن و جرایم فرامرزی موضوع جدیدی نیست. دفتر مبارزه با مواد مخدر و جرایم سازمان‌یافته سازمان ملل (UNODC) در این خصوص بیان می‌دارد: «جهانی شدن از مراحل رشد حکمرانی جهانی، پیشی گرفته است و این کمبود فقط نوعی خلاء نظارتی ایجاد کرده است که در آن جرایم سازمان‌یافته فراملی می‌تواند رشد کند» [۸].

اگرچه مجریان قانون به دلیل اختلافات قانونی و فرهنگی برای همکاری با یکدیگر تلاش می‌کنند؛ اما کمک حقوقی متقابل حدود ۷۰ درصد از ابزارهای همکاری بین‌المللی در تحقیقات جرایم سایبری را تشکیل می‌دهد و این روند معمولاً کند است. عوامل چندی در این کندی مؤثر هستند، همچون؛ پیگیری‌های متعدد در نتیجه فقدان اطلاعات یا گزارش ناکافی، کمبود منابع در حوزه قضایی دریافت‌کننده و درخواست میان کشورهایی که قوانین متفاوتی دارند و نیازهای داخلی را برای کمک در اولویت قرار می‌دهند. این در حالی است که زمان در تحقیقات جرایم سایبری برای جمع‌آوری شواهد از ضرورت‌ها محسوب می‌شود.

## ۳.۳ چالش دستگیری مجرمان وب تاریک

کشورهای پیشرو همچون ایالات متحده از دو طریق عمل می‌نمایند. اول در همه‌ی دستگیری‌های بزرگ مجرمان، رهبری یا کمک کرده‌اند. یکی از روش‌هایی که سازمان‌های مجری قانون در سراسر جهان معمولاً از آن استفاده می‌کنند، تحقیقات مخفیانه در وب است. برای مثال، FBI با دستگیری Ross Ulbricht، خالق جاده ابریشم، در سال ۲۰۱۳ موفق شد پیچیده‌ترین و گسترده‌ترین بازار جنایی در آن زمان را کشف نماید [۹]. همچنین در تحقیقات مختلف، مانند «عملیات Onymous» مشارکت داشته‌اند<sup>۱</sup>. در حالی که عملیات مخفی از لحاظ تاریخی، موفقیت‌آمیز بوده است، اما به دلیل حضور پلیس مخفی زیادی در اینترنت که باعث مشکوک شدن مجرمان می‌شود، تأثیر این روش نیز کم‌رنگ می‌شود. اگرچه این تحقیقات، ابزار مفیدی در اجرای قانون در وب تاریک است؛ اما چالش دیگری پیش روی مجریان قانون است و آن عمر کوتاه وبسایت‌های این فضا است که به دلیل فرار از شناسایی به ۲۰۰ تا ۳۰۰ روز می‌رسد و روند تحقیق را با مشکل مواجه می‌سازد. دوم، از رویکردی آرام برای تجاوزات سرزمینی حمایت می‌نمایند و موضوع مربوط به زمانی است که تحقیقات وب تاریک شامل دسترسی به دارایی دیجیتالی است. اما در خصوص دسترسی فراسرزمینی برای تحقیقات، کشورها با امضای معاهدات حقوقی، سعی در اجازه تحقیقات بدون اعطای مجوز دارند و این امر در تحقیقات سایبری از ملزومات است.

<sup>۱</sup> عملیات Onymous یک عملیات اجرایی بین‌المللی بود که توسط مرکز جرایم سایبری یورپل FBI، EC3، و تحقیقات امنیتی داخلی اداره مهاجرت و گمرک ایالات متحده رهبری می‌شد. وبسایت‌های تاریک مانند جاده ابریشم 2.0، ابر ۹ و هیدرا را هدف قرار داده است.

## ۴ نتیجه

روشن است که فناوری پیشرفته جهانی، طیف وسیعی از امکانات جدید را برای فعالیت‌های مجرمانه ارائه می‌دهد. وب تاریک و بازارهای آن قهرمانان فعلی هستند که مجریان قانون با آن روبرو هستند. وب تاریک عاملی برای جنایات فرامرزی و بین‌المللی است که در آن بازیگران و عواید حاصل از جرم می‌توانند همچون سایر جرایم در فضای سایبر در حوزه‌های قضایی مختلف باشند و چالش‌های فراروی حقوق کیفری تقریباً همان چالش‌های سنتی در جرایم فضای وب هستند اما موضوعات جدیدی چون روش پرداخت با ارز دیجیتال و فناوری پیچیده‌ی آن، نیاز مجریان قانون را به روزآمد کردن اطلاعات و دانش تخصصی را بیشتر نموده است و این شکاف با تعامل گروه‌های تخصصی و مجریان قانون تا حدودی برطرف می‌شود. از طرفی تعامل بیشتر کشورها برای تحقیقات فرامرزی در این خصوص بیشتر از پیش لازم است.

## مراجع

- [1] Amanda Haasz, Underneath it All: Policing International Child Pornography on the Dark Web, 43 Syracuse J. Int'l. L. & Com. 353 (2016) at 356.
- [2] Cara McGoogan, Dark web browser Tor is overwhelmingly used for crime, says study, The Telegraph (2016) <http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/>.
- [3] Daniel Moore & Thomas Rid, Cryptopolitik and the Darknet, Taylor and Francis Online Vol. 58 (2016). <http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085>.
- [4] Danny Bradbury, 'Unveiling the Dark Web' (2014) 4 Network Security 14, 14.
- [5] For a more technical and in-depth discussion of how this process works, see: Kristin Finklea, 'Dark Web' Congressional Research Service (10 March 2017), <https://fas.org/sgp/crs/misc/R44101.pdf>, accessed 26 April 2019.
- [6] Robert Stokes, 'Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar' (2012) 21(3) I.& C.T.L. 221, 225. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetism Japan, p. 301, 1982].
- [7] United Nations Office on Drugs and Crime, The Globalisation of Crime (Report) (2010) E.10.IV.6, 29, [https://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment\\_html/TOCTA\\_Report\\_2010\\_low\\_res.pdf](https://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment_html/TOCTA_Report_2010_low_res.pdf), accessed 26 April 2019.
- [8] UNODC, 'World Drug Report 2016' (May 2016) UNODC Doc E.16.XI.7.
- [9] Tim Hume, How the FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road, CNN (2013). <http://www.cnn.com/2013/10/04/world/americas/>

[silk-road-ross-ulbricht/index.html](http://silk-road-ross-ulbricht/index.html), J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.



## حوزه علمیه و متاورس، فرصت‌ها و پیامدها

مهدی منصوری خواه<sup>۱</sup>

<sup>۱</sup> طلبه سطح چهار حوزه علمیه، مطالعات تطبیقی اسلام و مسیحیت، موسسه آموزش عالی حوزوی خاتم النبیین (ص)، قم، ایران  
info@aghaedeshie.ir

### چکیده

در این مقاله، به فرصت‌ها و پیامدهایی که پدیده متاورس برای نهاد حوزه علمیه ممکن است ایجاد نماید پرداخته شده است. ابتدا سه ساحت علمی، تبلیغی و تهذیب نفس و انسان‌سازی برای حوزه ترسیم شده و آنگاه با توجه به ویژگی‌های متاورس و با در نظر گرفتن رسالت‌های حوزه، به این سؤال پاسخ داده شده که در آن ساحت خاص چه فرصت‌ها یا پیامدهایی برای حوزه متصور است و در پایان نتیجه‌گیری شده است. با توجه به پژوهش انجام‌شده گرچه متاورس مزایایی در عرصه آموزش، تبلیغ (به خصوص تبلیغ گردشگری) برای نهاد حوزه به ارمغان می‌آورد؛ اما در سایر عرصه‌ها به ویژه اصلاح نفس و تربیت جامعه اسلامی که هدف آن رسیدن انسان به مقام خلیفه الهی است نه تنها مزیتی ندارد؛ بلکه مانع بسیار جدی برای حوزه محسوب می‌شود. لذا با توجه به آسیب‌های جدی متاورس و گسترش روزافزون آن و عدم مطابقت آن با انسان‌سازی متعالی، باید با برنامه‌ریزی دقیق و علمی، بستری مناسب برای آموزش و تربیت مبلغین ایجاد نمود.

**کلمات کلیدی:** متاورس، حوزه علمیه، وظایف حوزه، خلیفه الله.

## ۱ مقدمه

متاورس گرچه یک اصطلاح قدیمی در دنیای دیجیتال است؛ ولی از نوواژگانی است که در سال‌های اخیر به‌شدت بین همگان رواج پیدا کرده است و بنا بر شواهد، ماندگاری زیادی خواهد داشت. متاورس نوعی افزونه برای دنیای واقعیت است؛ دنیای سه‌بعدی که افراد می‌توانند فعالیت نمایند. به نظر می‌رسد این محیط تبدیل به فضایی بسیار محبوب خواهد شد و مطمئناً از همان ابتدا بی‌عیب و نقص نخواهد بود، زیرا تبدیل یک واقعیت مجازی یکپارچه به یک دنیای کاملاً دیجیتال، زمان‌بر خواهد بود. متاورس یک دنیای دیجیتالی است که از ترکیب تکنولوژی‌های گوناگونی همچون واقعیت مجازی، واقعیت افزوده و تصاویر ویدئویی ساخته شده و کاربران در آن فضای مجازی اصطلاحاً قرار است «زندگی» کنند. مطابق پیش‌بینی شرکت‌های فعال در زمینه متاورس، کاربران در آینده خواهند توانست در این دنیای دیجیتالی کار انجام دهند، بازی کنند و با دوستان خود ارتباط برقرار کنند و مثلاً به تماشای نمایش‌های هنری بروند، در سمینارها شرکت کنند یا دور این دنیای

مجازی گشت‌وگذار نمایند. اساساً متاورس یک فناوری «برهم‌زننده» است. متخصصان به فناوری‌هایی که شیوه انجام یک کار را به طور کامل تغییر می‌دهند فناوری‌های برهم‌زننده می‌گویند. در متاورس به جای اینکه کاربر تنها چیزهای مختلف را تماشا کند، خواهد توانست درون آنها غوطه‌ور شود. متاورس اینترنتی است که جسمیت یافته و کاربر درون آن قرار می‌گیرد و در آن تجربه‌های کاملاً نو و نوینی در همه عرصه‌های زندگی فردی و اجتماعی کسب می‌کند. با توجه به قابلیت‌های موجود در متاورس و دنیای متاورسی پیش رو بر آنیم تا به این پرسش پاسخ دهیم که این فناوری جدید چه نسبتی با وظایف و رسالت حوزه‌های علمیه دارد و آیا فضای متاورس می‌تواند به حوزه‌های علمیه برای نیل به اهدافش کمک کند یا خیر؟

لزوم شناخت پدیده‌ها و موضوعات نوپدید و نوین و نسبت‌سنجی آن با رسالت طلبگی و زیست تبلیغی طلاب، نگارنده را بر آن داشت که به پژوهش در این زمینه و نگارش این مقاله اقدام نماید. با توجه به جدید بودن پدیده متاورس، مقاله و کتابی که به صورت مستقیم به موضوع حوزه و متاورس پرداخته باشد، موجود نیست. البته کتبی به فارسی و انگلیسی در موضوع متاورس طی یک سال گذشته در کشور چاپ و منتشر شده از جمله:

- متاورس و انقلاب ان‌اف‌تی، تألیف جواد عباسی و مزگان بهرامی
- راهنمای متاورس برای مبتدی‌ها، تألیف اندرو کلنس با ترجمه مرسته تهرانی
- آموزش متاورس، توسط حسام عزیزوند

• Metaverse for Beginners, by John Russel

• The Metaverse: Prepare Now For the Next Big Thing, by Terry Winters

این کتب و سایر مقالاتی که در این موضوع نگاشته شده صرفاً در موضوع متاورس بوده و اشاره‌ای به حوزه علمیه و مسائل و موضوعات مرتبط با حوزه نداشته است، از این جهت می‌توان مدعی شد عنوان و تمامی مطالب نگاشته شده در این نوشتار نو و جدید است.

در این نوشتار رسالت‌های حوزه شامل وظیفه علمی (آموزشی و پژوهشی)، تبلیغی و تهذیبی را ابتدا ذکر نموده و سپس با قابلیت‌ها و ظرفیت‌هایی که متاورس می‌تواند در اختیار نهاد حوزه بگذارد نسبت‌سنجی نموده‌ایم. در پایان نیز فرصت‌ها و پیامدهای مثبت یا احیاناً منفی در هر یک از این ساحت‌ها را بیان نموده و نتیجه‌گیری کرده‌ایم که آیا استفاده از این پدیده در آن ساحت به نفع حوزه است یا مسکوت است و یا می‌تواند تغایری با منافع و اهداف حوزوی داشته باشد.

## ۲ رسالت‌ها و وظایف حوزه علمیه

مطابق فرمایش بزرگان و علمای حوزه، حوزه به‌عنوان یک مرکز آموزشی علوم دینی، یک هدف کلی، بیشتر ندارد و آن آموزش دین است [۲۵]. هدف از تحصیل در حوزه نیز همان هدفی است که در آیه نفر<sup>۱</sup> توصیف و

<sup>۱</sup>قرآن کریم، سوره توبه، آیه ۱۲۲



ترسیم شده است. در این آیه، سه هدف ذکر شده است:

۱. هدف ابتدایی «لیتفقوها»؛

۲. هدف نهایی «لینذروا قومهم اذا رجعوا الیهم»؛

۳. هدف اعلا «لعلهم یحذرون».

گروهی از هر منطقه‌ای می‌آیند و پس از آنکه تفقه در دین یافتند، باز می‌گردند و فراگرفته‌ها و دانسته‌های خود را ابلاغ می‌کنند. نتیجه نهایی این کار، اصلاح جامعه اسلامی و شکل‌گیری آن در یک قالب کاملاً قرآنی و اسلامی است.

بنابراین، رسالت و وظایف حوزه را ما در سه ساحت و عرصه، دسته‌بندی می‌نماییم. ساحت آموزش و پژوهش که شامل تدریس و تحصیل در حوزه‌های علمیه است. ساحت تبلیغ (تبلیغ سنتی و خطابه، تبلیغ چهره‌به‌چهره، تبلیغ رسانه‌ای - شامل رسانه‌های مکتوب، رسانه‌های صوتی و تصویری مانند رادیو، تلویزیون و ماهواره، تبلیغ از طریق فضای سایبر یا به اصطلاح مرسوم در حوزه تبلیغ مجازی و تبلیغ از طریق گردشگری که چند سالی است به همت طلاب زبان‌دان در کشور نهادینه شده است) و ساحت تهذیب و اصلاح نفوس که تمامی ساحت‌های قبلی مقدمه برای رسیدن به این ذی‌المقدمه است.

با توجه به ساحت‌های بیان شده به‌عنوان وظایف حوزه‌های علمیه باید نسبت این ساحت‌ها را با متاورس سنجد و با توجه به ویژگی‌ها، ظرفیت‌ها و نیازسنجی و امکان‌سنجی فعالیت در فضای متاورس به این نتیجه رسید که آیا متاورس می‌تواند به کمک و معاضدت حوزه در رسیدن به اهدافش بیاید و یا مانعی برای رسیدن به این اهداف است یا علی‌السویه بوده و نمی‌توان از این فضا به نفع حوزه استفاده کرد و نه می‌توان توقع آسیب رساندن متاورس به وظایف و اهداف حوزه را داشت.

در ادامه ابتدا ظرفیت‌ها و امکاناتی که متاورس می‌تواند برای فعالیت‌های حوزوی داشته باشد را بیان می‌کنیم، سپس فرصت‌ها و تهدیدات را بیان کرده و در پایان نتیجه‌گیری می‌شود که در آن ساحت متاورس به نفع حوزه می‌تواند باشد، یا به ضرر و یا علی‌السویه است.

## ۱.۲ ساحت آموزش

پاندمی کرونا و تعطیل شدن دانشگاه‌ها و مدارس تا حد زیادی جهان را با آموزش مجازی و یادگیری از راه دور آشنا کرده است. آموزش از راه دور اگرچه مزیت‌های خاص خودش را داشته و برای مثال باعث صرفه‌جویی در زمان و هزینه‌ها شده است، اما برخی معایب را هم با خود به همراه داشته است. مهم‌ترین معایب آموزش مجازی را می‌توان بی‌روح بودن این نوع آموزش دانست به‌گونه‌ای که باعث افت تحصیلی و کاهش میزان یادگیری بسیاری از دانش‌آموزان و دانشجویان و طلاب حوزه‌های علمیه گردید.

از دیگر چالش‌های آموزش آنلاین و کلاس درس مجازی، عدم تعهد دانش‌آموزان به کلاس بود که این مشکل نیز در متاورس تا حدودی رفع خواهد شد. در کلاس‌های متاورسی به دلیل اینکه دانش‌آموز با بدن

مجازی یا همان آواتار در کلاس درس حضور دارد، همیشه باید هشیار و متعهد به کلاس باشد و در فعالیت‌های کلاسی و گروهی مشارکت نماید.

متاورس می‌تواند تمامی این چالش‌ها و موانع را از بین برده و یک کلاس مجازی و از راه دور با تمام امکانات و شرایط یک کلاس فیزیکی و واقعی را مهیا نماید. علاوه بر این، آموزش متاورسی مزایای دیگری نیز می‌تواند داشته باشد.

وظیفه فقها استنباط احکام از منابع است؛ اما موضوع‌شناسی و مساله‌شناسی و مصداق‌یابی وظیفه مکلف است، گاهی مصداق‌یابی بسیار سخت و پیچیده است به طوری که واگذار کردن تشخیص مصداق به مکلف شاید نوعی تکلیف ما لایطاق محسوب شود. همچنین استنباط دقیق‌تر احکام گاهی نیاز به فراگیری برخی علوم یا مهارت‌های مرتبط با آن موضوع را دارد. برای تقریب به ذهن می‌توان متاورس را مثال زد. یک فقیه ممکن است بدون داشتن تجربه‌ای از متاورس به گونه‌ای حکم دهد؛ اما همان فقیه با حضور، تجربه و یا زیست حتی چندساعته در فضای متاورس، ظرایف و نکاتی را در نظر بگیرد که قبل از آن به دلیل عدم آشنایی با این پدیده به آن واقف نبوده است.

متاورس این امکان را در اختیار فقها می‌گذارد تا بتوانند از طریق متاورس موضوعی را تجربه کنند و با آن بهتر آشنا شوند که این نکته می‌تواند کمک شایانی به فقیه نماید. با این حال متاورس در حوزه آموزش با چالش‌های جدی‌ای می‌تواند مواجه باشد که در ادامه به برخی از آنها اشاره خواهد شد.

- اولین و مهم‌ترین چالش در فضای متاورس حفظ حریم خصوصی داده‌ها و حفاظت از هویت کاربران از جمله طلاب است.
- بسیاری از مطالب و دروس حوزوی مخالفت جدی با سرمایه‌داری و استکبار است و این ممکن است مغایرت جدی با منافع شرک‌های میزبان متاورسی مانند متا و زوم داشته باشد. اینجا است که باید پرسید آیا پلتفرم‌های متاورسی به مبادلات آزاد بدون محدودیت متعهدند حتی زمانی که به قیمت سهام آنها آسیب برسد؟
- حفظ تمرکز دانشجو در یک محیط آنلاین پر از حواس‌پرتی تماشایی، یکی دیگر از مشکلات این فناوری نوین است. ضمن اینکه در این فضا مسئله تبلیغات شخصی‌سازی شده نیز بسیار جدی است. تبلیغات کنونی ممکن است برای بسیاری از مردم آزاردهنده باشد، اما در متاورس دیگر از تبلیغات آزاردهنده خبری نیست، بلکه بالعکس، این تبلیغات می‌تواند بسیار دلچسب و فریبنده نیز باشد.
- توضیح آنکه، شرکت‌های رسانه‌ای و متاورسی قادر هستند با اطلاعاتی که از کاربران جمع‌آوری می‌کنند پیشنهادهای تبلیغی شخصی‌تر شده‌ای را به کاربر ارائه نمایند. گجت‌هایی که به بدن ما در هنگام حضور در دنیای متاورس متصل می‌شوند می‌توانند همه اطلاعات ما حتی میزان ضربان قلب ما را اندازه‌گیری و جمع‌آوری کنند، حتی از طریق این گجت‌ها می‌توانند بفهمند ما چه زمانی گرسنه هستیم. در این هنگام تبلیغ انواع غذاها یا رستوران‌ها نه تنها برای کاربر اذیت‌کننده محسوب

نمی‌شوند؛ بلکه بسیار دلچسب نیز خواهد بود. به این ترتیب میزان حواس‌پرتی یک کلاس متاورسی به مراتب بیشتر از یک کلاس درس واقعی و فیزیکی خواهد بود.

• چالش‌های دیگری نیز می‌توان برای این فضا ترسیم کرد؛ اما آن چالشی که برای حوزه علمیه و تعلیمات حوزوی بسیار مهم است مسئله «نقش و نفس استاد در تعلیم و تهذیب نفس طلبه» است. فضای مدارس علمیه و ساختار و سیستم حاکم بر حوزه‌های علمیه از گذشته تا کنون فضایی عرفانی و جهت تهذیب نفس طلاب طراحی و ساخته شده بودند این چنین فضایی عرفانی جهت معارف دینی قطعاً در فضای متاورس وجود ندارد. طلاب در کلاس متاورسی نمی‌توانند روش و زی‌طلبگی را از استاد بیاموزند. در این فضا آنچه منتقل می‌شود تنها تعلیمات دین است و نه تعلیمات دینی. به عبارت دیگر، طلاب در فضای متاورس تنها چیزهایی در مورد دین یا آموزه‌های دین را از استاد فرامی‌گیرند، اما این فضا استعداد پرورش استعداد و ظرفیت طلاب و نیز انتقال روش زندگی طلبگی از استاد به شاگرد را نخواهد داشت. همچنین فرهنگ حوزوی و زندگی طلبگی که یکی از تفاوت‌های بارز میان حوزه و سایر مراکز علمی است که در این فضا دیگر اثری از آن فرهنگ نخواهد بود و طلبه هیچ‌گاه «یاد» نمی‌گیرد که چگونه مانند اسلاف صالح خویش «طلبگی» نماید، همان‌طور که یک دانشجوی رشته الهیات و معارف نمی‌تواند طلبگی کند.

هیوبرت درایفوس، استاد دانشگاه برکلی آمریکا که از فلاسفه و نظریه‌پردازان حوزه سایبرنتیک است، در مورد اهمیت حضور و نقش استاد می‌گوید: «یادگیری، فرایندی عمیقاً اجتماعی است که به زمان و تماس رودررو نیاز دارد، این بدان معنا است که استاد و دانشجویان باید تعامل داشته باشند [۲۶]». نقش «موضوعیت داشتن» در تعلیم و یادگیری، بی‌بدیل است. شاگرد بودن نیاز به تقلید دارد و بدون دخالت و حضور، نمی‌توان مهارت کسب کرد و شاگرد از راه دور، هیچ‌گاه به درجه استادی نخواهد رسید [۲۶]».۳

نتیجه آنکه متاورس با تمامی مزایایی که می‌تواند در عرصه آموزش داشته باشد؛ اما چالش بزرگی برای طلاب و حوزه‌های علمیه می‌تواند به همراه داشته باشد و آن اینکه در این فضا طلبه پرورش و آموزش نمی‌یابد، بلکه تنها آموزه‌های دینی و حوزوی را فرامی‌گیرد و تبدیل به یک دانشجوی الهیات و عارف می‌شود و فرقی با یک مسیحی، یهودی یا حتی یک بی‌دین که این دروس را خوانده است، ندارد.

## ۲.۲ ساحت تبلیغ

هر مکتب و مذهبی برای بقا و دوام خود، حفظ پیروان و جذب دیگران، نیاز مبرم به شناساندن اصول، مبانی و آموزه‌های خود دارد و بدون عنصر تبلیغ و بیان، نمی‌تواند از آنها پاسداری و حراست نماید و با تبیین و تبلیغ جهان‌بینی و ایدئولوژی هر دین و مذهبی، می‌توان از مشتبه شدن حق و باطل و ارزش‌ها و ضد ارزش‌ها به یکدیگر در عرصه‌های مختلف جلوگیری کرده و زمینه را برای گسترش آموزه‌های آن دین فراهم کرد.

<sup>۲</sup>درباره اینترنت، صفحه ۳۸  
<sup>۳</sup>همان، ص ۵۳

تبلیغ و دعوت، ارشاد و هدایت مردم به ارزش‌های الهی از اصول رسالت پیامبران الهی بوده و خط اصلی برنامه آنان را تشکیل می‌داده است. در همین راستا پیامبر اکرم صلی‌الله‌علیه‌وآله هدایت انسانی را برتر «از آن چه خورشید بر آن طلوع و غروب می‌کند» [۲۴]<sup>۴</sup>، دانسته است و امیرالمؤمنین علی علیه‌السلام در تجلیل از مبلغان به دیدار آنان اظهار اشتیاق می‌کند [۲]<sup>۵</sup>؛ و در مقایسه دعوت و ارشاد مردم با سایر ارزش‌ها آنها را چون دریای پهناور در برابر آب دهان می‌داند [۲]<sup>۶</sup>. امام صادق علیه‌السلام نیز وجود مبلغان راستین را مایه احیای دین و آثار امامت و نبود آنان را سبب نابودی دین دانسته است [۲۱]<sup>۷</sup>.

اکنون روش‌های مختلفی برای تبلیغ دین در حوزه‌های علمیه وجود دارد؛ تبلیغ سنتی و منبر، تبلیغ چهره‌به‌چهره، تبلیغ مکتوب، تبلیغ از طریق گردشگری، تبلیغ از طریق رسانه‌های صوتی و تصویری و تبلیغ از طریق فضای سایبر. با فراگیر شدن متاورس و دنیای مجازی باید دید تکلیف تبلیغ‌های موجود چه می‌شود و تبلیغ متاورسی نیز چگونه خواهد بود؟

همان‌طور که پیش‌ازین ذکر شد، متاورس یک فناوری برهم‌زننده است و تمامی تعاملات انسان را به‌گونه‌ای دگرگون خواهد کرد. در عصر متاورس انسان‌ها کمتر علاقه برای حضور فیزیکی دارند و تقریباً تمامی فعالیت‌های فردی، خانوادگی و اجتماعی در این بستر رقم می‌خورد، بنابراین تصور می‌شود دیگر خبری از **تبلیغ سنتی** و منبر نباشد و می‌رود که این رسانه تبلیغی حوزه‌های علمیه به تاریخ بپیوندد.

در مورد **تبلیغ چهره‌به‌چهره** نیز همین آینده ترسیم می‌شود. اکنون تبلیغ چهره‌به‌چهره در مساجد و هیئات، بقاع متبرکه، مراکز درمانی، مراکز ترک اعتیاد، ورزشگاه‌ها، بیمارستان‌ها، پارک‌ها و بوستان‌ها و سایر مراکز و معابر عمومی به‌صورت فیزیکی و مخاطب واقعی جریان دارد که با فراگیر شدن متاورس برخی از این اماکن مانند بوستان‌ها و پارک‌ها دیگر وجود ندارند و برخی دیگر کمتر مورد اقبال انسان عصر متاورس خواهند بود.

تبلیغ مکتوب هم اکنون نیز کم‌رنگ شده‌اند و کمتر مردم به سراغ کتاب‌های مجلد و چاپ شده می‌روند و به فایل کتاب‌ها یا کتاب‌های صوتی علاقه بیشتری نشان می‌دهند، اما بعید است که به از بین بردن و به سر نوشت دو دسته قبل دچار شود.

**تبلیغ از طریق رادیو و تلویزیون** حتماً دستخوش تغییرات اساسی خواهد شد. در عصری که مخاطب می‌تواند در موقعیت‌های نمایش داده‌شده حضور داشته باشد، اشیای تبلیغ شده را لمس کند، در معروفترین امکان گردشگری جهان قدم بزند و به ورزشگاه و سالن‌های اپرا در آنسوی دنیا برود و شادی و شمع خود را به اشتراک بگذارد، بعید است کسی سراغ رادیو و تلویزیون برود. باین‌حال، در خوش‌بینانه‌ترین حالت ممکن، صنعت تلویزیون در عصر متاورس می‌تواند با بازطراحی خود به صنعت تولید و ارائه چشم‌اندازهای شگرف تبدیل شود و تلاش کند تا با به‌کارگیری هوش مصنوعی، تجربه‌های شخصی‌سازی‌شده‌ای را در اختیار مخاطبان قرار دهد. چشم‌اندازهایی که ریشه در محتوا داشته؛ اما شیوه تولید و ارائه آن با تمامی آنچه که تا

<sup>۴</sup>بحار الانوار، ج ۱۹ ص ۱۶۷  
<sup>۵</sup>اولئک خلفاء الله فی ارضه و الدعاة الی دینه شوقا الی رؤیتهم؛ نهج البلاغه حکمت ۱۴۷، صبحی صالح، فیض الاسلام، حکمت ۱۳۹

<sup>۶</sup>نهج البلاغه، حکمت ۳۷۴، صبحی صالح، فیض الاسلام، حکمت ۳۳۶  
<sup>۷</sup>لولا زراره و نظراته اندرست احادیث ابی علیه السلام، نگاه شود به «بهجة الامال فی شرح زبدة المقال» ج ۴ ص ۱۶۸

امروز به عنوان محتوای شناسیم، متفاوت است. با توجه به خصوصیات و ویژگی‌های عصر متاورس، نهاد حوزه برای تبلیغ از طریق رسانه‌های دیداری و شنیداری از هم‌اکنون باید به فکر برنامه‌ریزی و اقدام باشد تا بتواند در این بستر حضوری و زیست تبلیغی داشته باشد، در غیر این صورت ممکن است این بستر را حداقل برای سالیانی از دست بدهد.

**تبلیغ گردشگری** از شیوه‌هایی است که در سالیان اخیر توسط طلاب زبان‌دان پا به عرصه زیست تبلیغی طلاب گذاشته است. در این روش طلاب زبان‌دان در محیط‌ها و فضاهایی که گردشگران خارجی برای بازدید حضور دارند، حاضر شده و در مورد اسلام، شیعه، انقلاب اسلامی و سایر موضوعات وابسته با گردشگران صحبت می‌کنند و به سؤالات و شبهات آنان پاسخ می‌دهند.

با فراگیر شدن متاورس مردم می‌توانند از این طریق به کاوش در جاذبه‌های گردشگری بپردازند و بدون صرف هزینه‌های بالا و در نظر گرفتن سایر مخاطرات سفرهای واقعی، از سفر مجازی خود لذت ببرند. «گردشگری مجازی» (Virtual Tourism) به افراد در نقاط مختلف جهان اجازه می‌دهد تا به طور مجازی با آواتارهای شخصی به یک شهر سفر کنند و از جاذبه‌های آن بهره‌مند شوند. با این اوصاف، مبلغین می‌توانند با آواتارشان در این اماکن حاضر شده و به تبلیغ بپردازند. البته با در نظر گرفتن ویژگی‌های متاورس می‌توان دو چالش عمده را برای این نوع تبلیغ تصور کرد. اول اینکه بتوانند این اماکن را در سطح گسترده به جهانیان معرفی کنند تا گردشگرانی برای سفر به این اماکن تمایل پیدا کنند. چالش دوم آن است که جاذبه‌های گردشگری در متاورس صرفاً جاذبه‌های توریستی و طبیعی یا تاریخی نیست؛ بلکه برخی حواشی دیگر همچون آزادی‌هایی به سبک غربی و متاورسی نیز باید وجود داشته باشد تا بتواند توریست‌ها را به خود جذب نماید که این مغایر با قوانین جمهوری اسلامی و نیز دین‌شان طلاب فاضل حوزه علمیه و نقض غرض تبلیغی خواهد بود.

**تبلیغ از طریق فضای سایبر** در حال حاضر منحصر به سایت و بلاگ و حضور در شبکه‌های اجتماعی است. یک رویکرد گسترده در متاورس در بین کاربران رواج پیدا کرده که متاورس جایگزینی برای اینترنت فعلی خواهد بود. شاید این نظر تا حدی درست باشد، چون با وجود متاورس، دیگر نیازی به اینترنت نخواهد بود، بلکه کلیه اطلاعات از طریق متاورس برای کاربر دست‌یافتنی خواهد بود. رویکرد دیگر این است که اینترنت یکی از زیر ساخت‌ها و ابزارهای ایجاد متاورس در نظر گرفت نه صرفاً جایگزین آن [۱۹].

به‌هر حال تبلیغ از این طریق ممکن است باز هم بتواند عمر کند؛ اما قطعاً همان‌طور که الان با چالش‌های جدی مواجه است در آینده این چالش‌ها بیشتر شده و مبلغین کمتر می‌توانند به مخاطب دسترسی داشته باشند. هم‌اکنون برخی کشورها مانند چین دسترسی هرگونه IP خارج از کشور خود را برای کاربران خود محدود کرده است، لذا مبلغین نمی‌توانند از طریق فضای سایبر به تبلیغ به زبان چینی بپردازند. همچنین در سال‌های گذشته فیس‌بوک و اینستاگرام بارها اقدام به حذف حساب‌های کاربری مربوط به ایران یا حذف پست‌هایی همچون پست‌های مرتبط با شهید قاسم سلیمانی نموده است؛ بنابراین ما در رساندن پیام به مخاطب در این فضا هم‌اکنون نیز با چالش‌های جدی مواجه هستیم. در دنیای متاورس این چالش‌ها نه تنها برطرف نمی‌شود؛ بلکه به مراتب بیشتر و دقیق‌تر نیز ادامه پیدا خواهد کرد.

متاورس صرفاً پلتفرمی برای محتوای کاربر ساخته همچون یوتیوب و فیس‌بوک نیست که در آن بی‌شمار



انسان بتوانند محتوایی را خلق کنند، اشتراک بگذارند و از آن پول در آورند، جایی که محبوب‌ترین محتواها در آن فقط سهم ناچیزی از کل مصرف را داشته باشند. متاورس مکانی خواهد بود که در آن تعدادی امپراتوری رسانه‌ای در آن سرمایه‌گذاری کرده و می‌خواهند «به طور کامل یک مشتری را مال خود کنند» و داده‌ها، رابطه‌های برنامه‌نویسی، و داده‌های اقتصادی و غیره را کنترل کنند [۲۷].

زاکبرگ به عنوان یکی از مدعیان بزرگ دنیای متاورس بارها ثابت کرده که اعتقادی به آزادی بیان ندارند و هر چه که با امپراتوری رسانه‌ای وی یا با جریان ضد استکبار و ضد صهیونیستی مغایر باشد را حذف می‌کند؛ بنابراین تنها کاری که مبلغین در دنیای متاورس می‌توانند انجام دهند تولید محتوای تبلیغی است؛ اما انتشار و دیده‌شدن آن محتوا توسط کاربر در دنیای متاورس قطعاً با چالش‌های جدی مواجه خواهد بود. حتی اگر برای انتشار و دیده‌شدن محتوا نیز مانعی نباشد باز هم مبلغین با چالش مواجه هستند، زیرا خوش‌گذرانی و تفریح اولین چیزی است که مردم از متاورس می‌خواهند [۱۸] و دین شاید جزو آخرین انتظارات و توقعات بشر از این فضا باشد. در فضای متاورس هر لحظه باید طبق قوانین متاورسی مردم بتوانند کسب یا خلق پول کنند تا بتوانند به حیات خود ادامه دهند و قطعاً در این فضا توقع تبلیغ دین، توقع بی‌جایی است.

اگر یک مبلغ بتواند بر همه این مشکلات فائق آید و پیام را به همان شکلی که می‌خواهد به کاربر برساند، باز تنها توانسته به کاربر تعلیمات دین بدهد و نه تعلیمات دینی (همان چیزی که در مبحث آموزش مطرح شد). ما در دوران متاورس نهایتاً تشیع اینترنتی و متاورسی داریم و نه چیزی فراتر از آن. بنابر آن چه گذشت، پرواضح است، حوزه علمیه در ساحت تبلیغ نمی‌تواند انتظار چندانی برای موفقیت در این عرصه داشته باشد. در فضای حکمرانی متاورس و هوش مصنوعی، اسب سرکش امیال و لذات نفسانی به‌تندی می‌تازد و نهادهای حوزوی نمی‌توانند مواجهه و کنش‌گری فعالی در این فضا داشته باشند.

## ۳.۲ ساحت تهذیب و انسان‌سازی

در فرهنگ و معارف اسلامی، تهذیب و تزکیه نفس از منزلت و جایگاهی بس رفیع برخوردار است. تمامی ساحت‌های گذشته مقدمه است برای این ذی‌المقدمه. طلاب حوزه‌های علمیه هم‌زمان با تحصیل علوم عقلی و نقلی و درس‌های رایج حوزوی باید به اصلاح نفس خود بپردازند و سپس وارد جامعه شده و به در راه اصلاح جامعه قدم بردارند.<sup>۸</sup>

<sup>۸</sup> حضرت امام خمینی (ره) در این باره می‌فرماید «کسب فضایل و مکارم انسانی و موازین آدمیت از تکالیف بسیار مشکل و بزرگی است که بر دوش شماست. گمان نکنید اکنون که مشغول تحصیل علوم شرعی می‌باشید، و فقه که اشرف علوم است می‌آموزید، دیگر راحتید، و به وظایف و تکالیف خود عمل کرده اید؛ اگر اخلاص و قصد قربت نباشد، این علوم هیچ فایده ای ندارد. اگر تحصیلات شما - العیاذبالله - برای خدا نباشد و برای هواهای نفسانیه، کسب مقام و مسند، عنوان و شخصیت در این راه قدم گذاشته باشید، برای خود وزر و وبال اندوخته اید. این اصطلاحات اگر برای غیر خدا باشد، وزر و وبال است. این اصطلاحات هر چه زیاده‌تر شود، اگر با تهذیب و تقوا همراه نباشد، به ضرر دنیا و آخرت جامعه مسلمان تمام می‌شود. تنها دانستن این اصطلاحات اثری ندارد. علم توحید هم اگر با صفای نفس توأم نباشد، وبال خواهد بود. چه بسا افرادی که عالم به علم توحید بودند و طوایفی را منحرف کردند. چه بسا افرادی که همین اطلاعات شما را به نحو بهتری دارا بودند؛ لیکن چون انحراف داشتند و اصلاح نشده بودند، وقتی وارد جامعه گردیدند بسیاری را گمراه و منحرف ساختند. این اصطلاحات خشک اگر بدون تقوا و تهذیب نفس باشد، هر چه بیشتر در ذهن انباشته گردد، کبر و نخوت در دایره نفس بیشتر توسعه می‌یابد؛ و عالم تیره بختی که باد نخوت بر او چیره شده، نمی‌تواند خود و جامعه را اصلاح نماید و جز زیان برای اسلام و مسلمان نتیجه ای به بار نمی‌آورد؛ و پس از سالها تحصیل علوم و صرف وجوه شرعی، برخوردار از حقوق و مزایای اسلامی، سد راه پیشرفت اسلام و مسلمان می‌گردد و ملت‌ها را



رسالت اصلی حوزه‌های علمیه دو چیز است: اول انسان‌ها را به قسمت «خلیفه الله» شدن راهنمایی و مقدمات سیروسلوک آن را فراهم کردن. دوم: جامعه را «جامعه توحیدی» ساختن، مبادی تمدن راستین را مهیا نمودن و اصول حاکم بر روابط داخلی و خارجی را تبیین کردن. نصوص دینی اعم از آیات قرآن و متون احادیث و نیز سیره‌ی معصومان و پیشوایان الهی گرچه حاوی معارف فراوان و نکات آموزنده زیادی است لیکن عصاره‌ی همه آن‌ها همانا دو رکن یادشده است. همان‌طوری که نظام داخلی انسان را روح و جسم او می‌سازد، لکن اصالت از آن روح است و بدن پیرو روح بوده و سلامت و رعایت اصول طبی وی برای تأمین سلامت روح از گزند عقاید سوء و آسیب اخلاقی ناروا و حفظ از زیان رفتار ناپسند است، تشکیل جامعه توحیدی نیز برای پرورش انسان‌هایی است که در جهت «خلیفه الله» قرارگرفتن گام برمی‌دارند و اصالت در بین دو رکن یادشده همانا از آن خلافت الهی است؛ زیرا بدن هرچند سالم باشد، بعد از مدتی می‌میرد و می‌پوسد؛ ولی روح، همچنان زنده و پاینده است. همچنین مدینه فاضله هرچند از تمدن والا برخوردار باشد، بعد از مدتی ویران می‌گردد، لیکن خلیفه الله که همان انسان کامل است از گزند هرگونه زوال مصون است؛ بنابراین مدینه فاضله و جامعه توحیدی به منزله بدن است و خلیفه الله به مثابه روح آن، و همان‌طوری که بر اساس اصالت روح، بدن را روح، سالم می‌سازد، بنا بر اصالت خلیفه الله، مدینه فاضله و جامعه توحیدی را انسان کامل تأسیس و تأمین می‌نماید.

با توجه به آنچه گفته شد، معلوم گردید هدف نهایی حوزه‌های علمیه از تحصیل، تهذیب و تبلیغ، هدایت انسان‌ها جهت تشکیل نظام توحیدی و خلیفه الله شدن است، حال باید دید اساساً خلیفه الهی شدن چه نسبتی با متاورس دارد و پیش از آن آیا حصول به این مرتبه از طریق فضای سایبر با مختصات و ویژگی‌های فعلی مقدور هست یا خیر.

همان‌گونه که پیش از این نیز بیان شد متاورس گرچه ممکن است تجربه‌ای مانند حضور فیزیکی را برای کاربران به ارمغان آورد؛ اما در این فضا تعلیم و تربیت و نفس استاد، نقش ندارد و تنها آموزه‌ها از استاد به شاگرد منتقل می‌شود، در حالی که در سیروسلوک و تهذیب نفس، متعلم و متربی حتماً باید با استاد زیست واقعی و فیزیکی داشته باشد تا از نفس استاد بهره‌مند گردد، به قول جناب حافظ:

طی این مرحله، بی‌همره‌ی خضر مکن      ظلمات است، بترس از خطر گمراهی

شیخ نجم‌الدین رازی در کتاب مرصادالعباد ۱۰ دلیل اقامه کرده است که سالک در سفر الی الله به راهنما و استاد نیاز دارد [۲۳]<sup>۹</sup> و علامه بحرالعلوم در مورد شناخت استاد کاملی که بتوان او را به‌عنوان خضر راه

گمراه و منحرف می‌سازد؛ و ثمره این درسها و بحثها و بودن در حوزه‌ها این می‌شود که نگذارد اسلام معرفی، گردد حقیقت قرآن به دنیا عرضه شود، بلکه وجود او ممکن است مانع معرفت جامعه نسبت به اسلام و روحانیت گردد. من نمی‌گویم درس نخوانید، تحصیل نکنید؛ باید توجه داشته باشید که اگر بخواهید عضو مفید و مؤثری برای اسلام و جامعه، باشید ملتی را رهبری کرده به اسلام متوجه سازید، از اساس اسلام دفاع کنید، لازم است پایه فقاقت را تحکیم کرده، صاحب‌نظر باشید؛ اگر خدای نخواستہ درس نخوانید حرام است در مدرسه بمانید؛ نمی‌توانید از حقوق شرعی محصلین علوم اسلامی استفاده کنید؛ البته تحصیل علم لازم است؛ منتها همان‌طور که در مسائل فقهی و اصولی زحمت می‌کشید، در راه اصلاح خود نیز کوشش کنید. هر قدمی که برای تحصیل علم برمی‌دارید، قدمی هم برای کوبیدن خواسته‌های نفسانی، تقویت قوای روحانی، کسب مکارم اخلاق، تحصیل معنویات و تقوا بردارید. ر. ک. تهذیب نفس و سیر و سلوک از دیدگاه امام خمینی (س)، صص ۶۶ و ۶۷.

<sup>۹</sup> مرصاد العباد، ص ۱۲۸

پذیرفت می‌گوید: «و اما استاد عام شناخته نمی‌شود، مگر به مصاحبت او در خلأ و ملأ و معاشرت باطنیه و ملاحظه تمامیت ایمان جوارح و نفس او و زینهار به ظهور خوارق عادات و بیان دقائق و نکات و اظهار خفایای آفاقیه و خبایای انفسیه و تبدل بعضی از حالات خود به متابعت او فریفته نباید شد، چه اشراف بر خواطر و اطلاع بر دقائق و عبور بر ماء و نار و طی زمین و هوا و استحضار از آینده و امثال اینها در مرتبه مکاشفه روحیه حاصل می‌شود و از این مرحله تا سرمنزل مقصود راه بی‌نهایت است» [۲۰]؛ بنابراین هم سالک برای سیر الی الله به استاد نیاز دارد و هم برای شناخت استاد کامل نیاز به مصاحبت دائم با وی دارد تا نکند به جای استاد گرفتار رهنمان راه گردد و از سیر بازماند. استاد نیز لازم است سلوک و مشی سالک را ببیند تا بتواند به نحو احسن وی را هدایت و راهنمایی نماید.

آنچه گفته شد از ضروریات سیروسلوک و تهذیب نفس است که بین تمامی علمای اخلاق و عارفان الهی یک اصل پذیرفته شده است و کسی مخالف آن نیست. بدیهی است که متاورس با تمام قابلیت‌هایی که دارد هیچ‌گاه نمی‌تواند این چنین رابطه‌ای را بین استاد و شاگرد برقرار نماید و آنچه که غرض از تحصیلات حوزوی است، حاصل نمی‌شود.

اگر طلاب به دلیل حضور در متاورس از استاد دور بمانند و نتوانند تهذیب نفس کنند نه تنها خود را به ورطه عذاب الهی خواهند انداخت، بلکه سبب فساد دیگران نیز می‌شوند. به فرمایش امیرالمؤمنین «زَلَّةُ الْعَالِمِ كَأَنَّكَ سَارِ الْأَسْفِينَةَ تَغْرُقُ وَ يَغْرُقُ مَعَهَا غَيْرُهَا»<sup>۱۱</sup> [۲۲]. حضرت امام خمینی (ره) نیز در این باره می‌فرماید: «روحانی اگر درست شد همه چیز درست می‌شود و اگر - خدای نخواست - فاسد شد، فَسَدَ الْعَالِمُ. این مسئله، واقعیتی است» [۱۷].<sup>۱۳</sup>

علاوه بر اینکه متاورس اقتضای نیل به تهذیب نفس را ندارد، مانع جدی بر سر این راه نیز هست و به قول طلاب مقتضی مفقود و مانع موجود هست. این مانع خود سایبر (به‌عنوان بستر متاورس) است. مقام معظم رهبری در این باره در جمع طلاب و روحانیون شیعه و اهل سنت کرمانشاه می‌فرماید: «شیطان امروز که از راه اینترنت و ماهواره و روش‌های ارتباطی مدرن و فوق مدرن سراغ شما می‌آید، ... شبهه‌آفرینی دارد، اخلال در عقیده دارد، ایجاد تشویش در ذهن دارد، تزریق ناامیدی دارد، ایجاد اختلاف دارد [۱۲].»

اغواگری [۱۶]، شبهه‌افکنی در جامعه [۴]، انحراف جوانان از حیا و ایمان [۱۴]، تجهیز معاندان [۹]، حذف ایمان جوانان و سلب عقیده [۵]، تسلط بر فرهنگ کشور [۷]، تعارض با ادب و حیا [۶]، لغزشگاه بودن فضای سایبر [۶]، بستر حمله شیطان [۱۲]، تبدیل معروف به منکر و منکر به معروف [۳]، انتشار محتوای منفی، وارونه‌سازی واقعیت [۱۰]، ترویج سکولاریسم [۱۵]، بمباران اطلاعاتی مخاطب با تحلیل‌های ممزوج از حق و باطل [۱۱]، نشر افکار باطل [۸]، هجمه به تفکرات شیعی [۱۳] از سایر موانعی است که در فرمایشات رهبری به‌عنوان موانع فضای سایبر بیان شده است.

البته دلایل دیگری نیز وجود دارد که به دلیل جلوگیری از اطاله مطلب از بیان آنها پرهیز شده و تنها به

<sup>۱۰</sup> رساله سیر و سلوک منسوب به بحر العلوم، ص ۱۵۹

<sup>۱۱</sup> لغزش عالم همانند شکسته شدن کشتی در دریا است هم خود غرق می‌شود و هم موجب غرق شدن سرنشینانش می‌گردد

<sup>۱۲</sup> عیون الحکم و المواعظ، ج ۱، ص ۲۷۶

<sup>۱۳</sup> صحیفه امام خمینی، ج ۱۵، ص ۴۸۳

همین مقدار کفایت می‌شود؛ بنابراین، حوزه علمیه اگر می‌خواهد همچون گذشته بتواند به وظایف و رسالت‌های خود پایبند بماند و بتواند موفق باشد باید از این فضا برحذر باشد. البته ممکن است متولیان و مسئولین نهاد حوزه برای معرفی اسلام، پاسخ به شبهات و تبلیغ دین اسلام بخواهند از این فضای جدید بهره‌مند شوند که فی‌الجملة اشکالی ندارد، ولی باید به سه نکته توجه داشته باشند: الف) نباید طلاب و دروس حوزوی را به این فضا سوق دهند، بلکه حتماً باید همچون گذشته به‌صورت فیزیکی و سنتی درس‌ها و مباحثات برگزار شوند؛ ب) استفاده از متاورس برای تبلیغ اسلام به جهانیان همچون استفاده از موسیقی هست و باید با دقت بسیار بالایی از آن بهره‌مند شد و مراقب بود به حرام آلوده نشود؛ ج) حتماً تخاطب واقعی و حضور فیزیکی در سرلوحه فعالیت‌های خویش قرار دهند. نهادهای دینی و تبلیغی هرچقدر هم که در فضای متاورس خوب و موفق عمل کنند بازهم به هدف غایی که «تربیت نفوس در راستای خلیفه الله» شدن است، نخواهند رسید، چون همان‌طور که گذشت، ذات این فضا مسموم است؛ بنابراین باید به این فضا به‌عنوان مکمل فضای فیزیکی نگریست. اصل فضای فیزیکی و حقیقی است نه فضای سایبر و متاورس. اگر اصالت را به فضای سایبر بدهیم ناخواسته و نادانسته بازی را به دشمن واگذار کرده‌ایم و اوست که بازی‌گردان خواهد بود.

فراموش نشود تکنولوژی و فضای سایبر قرار است تسهیل‌کننده روابط و تقویت‌کننده آن باشد نه اینکه با ایجاد گسست و فاصله روابط را کمرنگ و مجازی کند. مراقب باشیم تا فضای سایبر مانند ویروس اکستاکس نت در جامعه عمل نکند؛ ویروسی که ظاهراً همه چیز را عادی و طبیعی نشان می‌دهد؛ اما زمانی خود را نمایان می‌کند که دیگر هیچ کاری نمی‌توان انجام داد.

تمام آنچه در فضای متاورس است بر اساس تقویت قوه واهمه جهت نفوذ و سلطه شیطان بر انسان است. این تکنولوژی ملزوماتی دارد که یکی از آن‌ها ادبیات و استفاده از استعاره‌های ذهنی و لغوی مخصوص به خود آن است. این ادبیات و فرهنگ، برگرفته از فرهنگ شیطان و در ذات فضای متاورس است و «ذاتی الشیء لا یسلب منه».

### ۳ نتیجه‌گیری

متاورس یک پدیده برهم‌زننده و فراگیر است که می‌تواند برای حوزه به‌ویژه در ساحت تبلیغ، دستاوردهایی داشته باشد؛ اما مخاطرات و چالش‌های بسیار جدی نیز دارد. مهم‌ترین وظیفه حوزه از نظر بزرگان حوزوی انسان‌سازی و جامعه‌سازی بر اساس آموزه‌های اسلامی و آرمان‌های والای الهی است که متاورس دقیقاً در جهت مخالف آن در حرکت است و به همین دلیل بهره‌گیری از این فناوری برای حوزه، نقض غرض محسوب می‌شود.

البته نهاد حوزه و حوزویان می‌توانند برای معرفی اسلام به جهانیان و تبلیغ اسلام از این فضا بهره‌مند شوند؛ ولی سه نکته اساسی را هرگز نباید فراموش نمایند:

- استفاده از متاورس از باب اکل میته است و باید تنها به مقدار ضرورت باشد. نباید درس‌ها و مباحثات حوزوی را به این فضا منتقل کرد، بلکه باید تنها برای استفاده‌های خاص همچون تبلیغ بین‌المللی اسلام به آن دست یازید.

- استفاده از متاورس مانند استفاده از موسیقی است. مرز بین موسیقی حرام و حلال بسیار باریک است و باید مراقب بود تا به ورطه گناه کشیده نشویم. متاورس نیز دقیقاً همین حکم را دارد.
- نباید از فضای فیزیکی و مخاطب واقعی غفلت نمود. اصل بر مخاطب واقعی است و فضای متاورس باید به معاضدت و یاری فضای فیزیکی و واقعی بیاید.

## مراجع

- [۱] قرآن کریم.
- [۲] نهج البلاغه.
- [۳] بیانات در دیدار قهرمانان و ورزشکاران مسابقات آسیایی و پارا آسیایی، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۱ بهمن ۱۳۹۳.
- [۴] بیانات در دیدار جمعی از مدیران و اساتید مؤسسه امام صادق با رهبر انقلاب، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۱ خرداد ۱۳۹۶.
- [۵] بیانات در حرم مطهر رضوی، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۱ فروردین ۱۳۹۴.
- [۶] بیانات در دیدار معلمان و فرهنگیان، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۱۳ اردیبهشت ۱۳۹۵.
- [۷] بیانات در مراسم بیست و هفتمین سالگرد رحلت امام خمینی (رحمه الله)، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۱۴ خرداد ۱۳۹۵.
- [۸] بیانات در دیدار جمعی از روحانیون استان همدان، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۱۵ تیر ۱۳۸۳.
- [۹] بیانات در دیدار مردم قم، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۱۹ دی ۱۳۹۵.
- [۱۰] بیانات در دیدار بسیجیان استان قم، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۲ آبان ۱۳۸۹.
- [۱۱] بیانات در دیدار جمعی از اساتید دانشگاهها، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۲ شهریور ۱۳۹۰.
- [۱۲] بیانات در جمع روحانیون شیعه و اهل سنت کرمانشاه، ۲۰ مهر ۱۳۹۰، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۲۰ مهر ۱۳۹۰.
- [۱۳] بیانات در دیدار اعضای مجلس خبرگان رهبری، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۲۷ بهمن ۱۳۷۹.
- [۱۴] بیانات در دیدار مردم آذربایجان شرقی، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۲۷ بهمن ۱۳۹۵.
- [۱۵] بیانات در اجتماع بزرگ مردم قم، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۲۷ مهر ۱۳۸۹.
- [۱۶] گزیده ای از بیانات در دیدار جمعی از مسئولان و فعالان فرهنگی استان های یزد و همدان، پایگاه اطلاع رسانی دفتر حفظ و نشر آثار حضرت آیت الله العظمی سیدعلی خامنه ای (مدظله العالی)، ۳۰ مرداد ۱۳۹۶.

- [۱۷] خمینی، سید روح‌الله. صحیفه امام. مؤسسه تنظیم و نشر آثار امام خمینی (س).
- [۱۸] کلمنس، اندرو. راهنمای متاورس برای مبتدی‌ها. (مترجم: مرسته تهرانی). ۱۴۰۱.
- [۱۹] عزیزوند، حسام. آموزش متاورس. نشر عطران، تهران، ۱۴۰۰.
- [۲۰] حسینی‌طهرانی، سیدمحمدحسین. رساله سیر و سلوک منسوب به بحر العلوم. نشر علامه طباطبایی، ۱۳۹۵.
- [۲۱] علیاری تبریزی، علی‌بن‌عبدالله. بهجة الامال فی شرح زیدة المقال. نشر کوشان‌پور، ۱۳۷۹.
- [۲۲] لیثی واسطی، علی بن محمد. عیون الحکم و المواعظ. مؤسسه علمی فرهنگی دارالحدیث، سازمان چاپ و نشر، قم.
- [۲۳] نجم‌رازی، محمدامین؛ ریاحی، عبدالله بن محمد. مرصاد العباد. شرکت انتشارات علمی و فرهنگی، ۱۳۹۲.
- [۲۴] مجلسی، محمد بن باقر بن محمدتقی. بحار الأنوار الجامعة لدرر أخبار الأئمة الأطهار علیهم السلام. دار احیاء التراث العربی، بیروت لبنان.
- [۲۵] مصباح یزدی، محمدتقی. نشریه پیام حوزه. زمستان ۱۳۷۵.
- [۲۶] دریفوس، هیوبرت. درباره اینترنت. (مترجم: علی فارسی‌نژاد). نشر ساقی، ۱۳۸۹.
- [27] Ball, Matthew. The metaverse: What it is, where to find it, and who will build it, [www.matthewball.vc/all/themetaverse](http://www.matthewball.vc/all/themetaverse), accessed: 20 September 2022.





## پیوند نظام کیفری و جاسوسی صنعتی در فضای سایبر: رویاری یا هم کنشی؟

مرضیه جعفرخانی<sup>۱</sup>، حسن عالی پور<sup>۲</sup>

<sup>۱</sup> کارشناسی ارشد حقوق جزا و جرم شناسی، دانشکده حقوق دانشکدگان فارابی، دانشگاه تهران  
majafarkhani2@gmail.com

<sup>۲</sup> دکتری حقوق جزا و جرم شناسی، عضو هیئت علمی دانشگاه تهران  
hassan.alipour@ut.ac.ir

### چکیده

پدیده‌ی جاسوسی صنعتی در چهارراه حقوق کیفری، حقوق مالکیت فکری، اقتصاد و علوم مرتبط با سیاست دانسته می‌شود و چالش این نوشتار از همین جا آغاز می‌گردد که: نظام کیفری چگونه باید با پدیده‌ی جاسوسی صنعتی روبه‌رو شود؟ در رویکرد رویارویی، جاسوسی صنعتی به عنوان یک رفتار مجرمانه در سه حوزه سنتی، نظامی و سایبری مطرح می‌شود. با این حال عدم تصریح به جاسوسی صنعتی و اقتصادی در قوانین ایران، به استثنای مقررات مرتبط با جرایم نیروهای مسلح، جایگاه قانونی این پدیده را همانند خود جاسوسی مبهم کرده و چهره‌های دوگانه به این جرم بخشیده است. از سوی دیگر، رویکرد هم‌کنشی انگاره‌ی دیگری را مطرح می‌کند که: چون در جاسوسی صنعتی، نقش دولت بیگانه یا عنصر وابسته به آن، تعیین‌کننده و وجه تمایز این پدیده با رفتارهای مشابه است، جاسوسی صنعتی، چیزی جز سیاست دولت‌ها در قبال یکدیگر نیست. از این منظر، جاسوسی صنعتی از جامه‌ی یک بزه به جامه‌ی یک پدیده‌ی تأثیرگذار در روابط کشورها در می‌آید. حاصل پژوهش در موضوع حاضر چنین نمایان می‌شود که رویکرد نظام حقوقی داخلی در رویارویی در سایه‌ی بزه جاسوسی و با رنگ‌مایه‌ی جرائم علیه امنیت بوده و در عرصه بین‌المللی رویکرد سیاسی کشورها در برابر یکدیگر، حاکم است.

**کلمات کلیدی:** اسرار صنعتی، جاسوسی صنعتی، فضای سایبر.

### ۱ مقدمه

با پایان جنگ سرد و اهمیت یافتن تجارت در عرصه داخلی و بین‌المللی، تلاش کشورها از رقابت در زمینه نظامی، به رقابت در زمینه اقتصادی تغییر یافت و تجارت به یکی از زمینه‌های کسب قدرت تبدیل شد. از سال ۱۸۷۵ رقابت بین جاسوسی صنعتی و نظامی آغاز گردید و پس از گونه نظامی و سیاسی آن، موج سوم از جاسوسی را در پیشینه روابط کشورها پدید آورد. به گواه تاریخ «در اواخر قرن ۱۹ مبارزه جدیدی در صحنه

مبارزات جاسوسی پیدا شد و آن ژاپن بود که با توجه به عقب ماندگی اش در صنعت، مصمم بود به هر ترتیب، این نقیصه را جبران نماید و خود را به کشورهای پیشرفته برساند. فعالیت ژاپن در این زمینه به اندازه‌ای بود که مجله آنترپریز ارگان صنایع و بازرگانی فرانسه در مورخ ۲۸ اکتبر ۱۹۶۷ نوشت: بیشتر متجاوزین و جاسوسان صنعتی، ژاپنی‌ها هستند» (عالی‌پور، ۱۳۸۹: ۱۷۲).

در جهان کنونی، در یک سو کشورهایی وجود دارند که توان مالی و نیروی انسانی متخصص و مبتکر به قدر کافی در اختیار داشته، مدام در حال تولید علم و صنعت می‌باشند و در عرصه رقابت تجاری نیز، گوی سبقت را از دیگران می‌ربایند. در دنیای مدرن که صنعت و فناوری حرف اول را می‌زند، کشور تولید کننده اسرار صنعتی به جهت نوین و انحصاری بودن این اطلاعات به منافع مالی فراوانی می‌رسد. بر همین اساس، سعی در جهت کنترل آنها دارد برای مثال «دولت ایالات متحده از پروژه‌های فن‌آورانه شرکت‌های آمریکایی حمایت کرده یا به بهانه حفظ امنیت ملی در معاملات تجاری دخالت می‌کند» (صدیق، ۱۳۹۵: ۸۷).

اما در سوی دیگر جامعه جهانی، کشورهای جهان چندم هستند که توان تولید فن‌آوری ندارند و در اصطلاح مصرف کننده و مشتری فناوری کشورهای جهان اولند. از همین روست که در عرصه بین‌المللی شاهد این هستیم که کشورهایی که توانایی تولید صنعت را ندارند، دست به هرگونه عملی می‌زنند تا از چرخه رقابت عقب نمانند؛ که مهمترین و کارآمدترین آن، ربودن اطلاعات اقتصادی و صنعتی سایر کشورها، علی‌الخصوص از کشورهای پیشرو، می‌باشد. برای مثال، «بر اساس مطالعه انجام شده، به طور متوسط دوازده سال کار مداوم و ۲۳۱ میلیون دلار سرمایه لازم است تا داروی جدیدی وارد بازار آمریکا شود. این در حالی است که آزمایشگاه‌های تایلند، هند و برزیل، پس از عرضه آن دارو در آمریکا، در عرض چند ماه با سرقت فرمول آن، اقدام به تجاری سازی همان محصول می‌کنند. این مسئله سالانه چهار میلیارد دلار برای شرکت‌های آمریکایی هزینه دربرداشته است» (میرمحمدی و سالارکيا، ۱۳۹۱: ۱۲۸). البته تنها کشورهای ضعیف نیستند که به دنبال اسرار صنعتی رقبا می‌باشند بلکه کشورهای پیشرو نیز پیوسته در حال رصد سایر کشورها می‌باشند؛ معرفی آمریکا به عنوان بزرگ‌ترین جاسوسی صنعتی در سال ۲۰۱۳، گواه بر این مدعا است. حالی در پژوهش حاضر تلاش شده تا با بهره‌گیری از روش تحلیلی توصیفی در قالب مطالعات نظری، در چند بخش به پیوند جاسوسی صنعتی و فضای سایبر، شاخص‌های جاسوسی صنعتی، رویارویی با جاسوسی صنعتی در عرصه داخلی و بین‌المللی به این سوال پاسخ داده شود که نظام کیفری چگونه باید با پدیده جاسوسی صنعتی روبه‌رو شود و به واقع رویکرد حال حاضر در برابر این پدیده چیست؟

## ۲ پیوند جاسوسی صنعتی و فضای سایبر

فضای سایبر به عنوان فناوری جدیدی که وارد زندگی بشر شد، تاثیرات فراوانی بر جنبه‌های مختلف زندگی وی گذاشت. یکی از بسترهای ورود و تاثیر آن، بخش اقتصاد و صنعت بود. به دلیل ویژگی‌های منحصر به فردی که دارد، سرعت و سهولت ایجاد و نگهداری اطلاعات در این فضا بالاست. از همین رو کمک بسیاری به بخش صنعت کرده و پیوند تنگاتنگی پیدا کرده است به گونه‌ای که بسیاری از اطلاعات صنعتی در این فضا صورت می‌گیرد. از همین رو شکل اطلاعات، نحوه نگهداری و حفاظت از آنها نسبت به گذشته تغییرات

فراوان کرده است.

همچنین با ورود فضای سایبر به زندگی بشر، فضای ارتکاب جرم نیز تغییر کرده و از محیط فیزیکی و ملموس به دنیای ناملموس تبدیل شده است همین تغییرات و ایجاد اطلاعات در بستر فضای سایبر، شیوه ارتکاب جرائم را متغیر ساخته است. به عقیده برخی، جرم جاسوسی در محیط سایبر، تحول انقلابی در ساختار سنتی این جرم ایجاد کرده و ماهیت، گستره عمل و حوزه آن را تغییر داده است (Sterken, 2013). اکنون ارتکاب جاسوسی صنعتی نیاز به ورود در فضای نگهداری اطلاعات ندارد با هزینه بسیار اندک و در فضایی هرچه مخفی‌تر، امکان دسترسی به اطلاعات صنعتی به سهولت امکان‌پذیر شده است. جاسوسی اقتصادی و صنعتی در پایان سده بیستم، با پدید آمدن فضای سایبر و همنشینی با مفهوم‌هایی مانند جنگ اطلاعات، جنگ نرم و رزم سایبری، برجسته‌ترین و شایع‌ترین گونه از جاسوسی به شمار می‌رود. فن‌آوری سایبر در تمام ابعاد زندگی بشر رسوخ کرده است و با گسترش اینترنت و ارتباطات سایبری، تاثیر این فضا ملموس‌تر و همه جانبه شده است. تاثیر این فن‌آوری در جرم جاسوسی تا اندازه‌ای است که به عقیده برخی در این جرم «انقلاب ایجاد کرده، که این انقلاب ناشی از تحولی است که در مورد اطلاعات و دسترسی به آنها رخ داده» (Benner, 2015). در حال حاضر جاسوسی سایبری اصطلاحی جدید در حوزه امنیت می‌باشد و تهدیدات سایبری، گونه جدیدی از رفتارها برضد امنیت را در بین کشورها ایجاد کرده است. حملات مخرب و مهم و در عین حال سریع و مبهم، امنیت ملی کشورها را به چالش کشیده است و یکی از بدترین تهدیدات علیه منافع ملی به شمار می‌رود؛ چراکه در حال حاضر حجم زیادی از اطلاعات در این فضا شکل گرفته است، اطلاعاتی مهم که چه بسا سندی فیزیکی از آنها وجود ندارد.

از بعد سیاسی، جنگ سایبری گزاره‌ای است که پیرو تحولات فوق‌الذکر، پا به عرصه سیاست گذاشت چراکه امروزه، رفتارهایی متفاوت از رفتارهای جنگی سنتی به وجود آمده است که البته در مورد تشخیص آنها معیار صریحی وجود ندارد لیکن این دلیل بر نادیده گرفتن سرشت خطر آفرین آنها نیست. به همین دلیل است که در کشوری مانند آمریکا می‌بینیم که در سیاست خود، جاسوسی سایبری را نمونه رفتار جنگی می‌داند و پس از کشمکشی طولانی با کشوری مانند چین، به پیمان بر سر خاتمه جنگ سایبری توافق می‌کند.

### ۳ شاخص‌های جاسوسی صنعتی

جاسوسی صنعتی به عنوان پیوندگاه چندین حوزه، در سنجش با دیگر پدیده‌های مجرمانه، ویژگی‌های متمایزی دارد که در ادامه به آنها پرداخته می‌شود:

#### ۱.۳ جاسوسی صنعتی در چهره بزه امنیتی

علی‌رغم اینکه هنوز هم برخی از حکومت‌ها امنیت را در گرو حفظ امنیت نظامی می‌دانند و ارتکاب بزه جاسوسی علیه اطلاعات نظامی را تهدید علیه امنیت خود برمی‌شمرند، اما با پایان جنگ سرد و تغییر در منابع قدرت، جاسوسی صنعتی نیز رفتاری ضد امنیت تلقی می‌شود. به عبارت دیگر «برای کشورهایی که اسرار تجاری معنایی برابر با منافع ملی و پیرو آن امنیت ملی دارد، جاسوسی صنعتی در شمار بزه‌های ضد امنیت

ملی است و حتی در ایران با تصریح بیشتر به عنوان گونه‌ای از جرائم نظامی آمده است» (عالی پور، ۱۳۹۶: ۲۲۶). بر این اساس، جاسوسی صنعتی از جرائم علیه امنیت است و مشمول سخت‌گیری‌ها و حساسیت‌های قانونگذار در مورد این دسته از جرائم می‌باشد.

این نگاه از این نظر تقویت می‌شود که جاسوسی صنعتی، همان رفتار جاسوسی نسبت به اطلاعات و اسرار صنعتی می‌باشد و به نوعی صورت تخصصی جرم جاسوسی است و جاسوسی، تهدیدی علیه امنیت کشور می‌باشد، بنابراین جاسوسی صنعتی نیز به تبع عنوان عام خود، بزهی امنیتی محسوب می‌گردد. همچنین به دلیل اینکه جاسوسی صنعتی همواره پشتوانه خارجی دارد، کشورها این رفتارها را علیه خود، منافی حاکمیتشان می‌دانند و سعی می‌کنند که از کنار آن به آسانی گذر نکنند و برای برخورد شدیدتر با مرتکبین، آنها را در زمره مجرمین امنیتی قرار دهند، چراکه همواره شدیدترین واکنش‌ها در مقابل بزهدی امنیتی صورت می‌گیرد.

### ۲.۳ جاسوسی صنعتی در چهره بزهد اقتصادی

چالش هویت حقوقی بزهد اقتصادی، سبب می‌شود تا مصادق‌هایی که در ذیل آن جای می‌گیرند، گمان‌آور باشند. بیشتر نویسندگان و اندیشمندان نسبت به ارائه تعریف جرم اقتصادی به دشواری آن اذعان نموده‌اند و «اغلب دلیل این دشواری را، گستردگی موضوعات و مصادیق این جرم می‌دانند» (آقای جنت‌مکان، ۱۳۹۶: ۲۸) و برخی دیگر «علت را در مبهم بودن تعریف اقتصاد می‌دانند» (نورزاد، ۱۳۸۹: ۱۷۴).

بطور کلی، «جرم اقتصادی هر رفتاری است که تهدیدی علیه امنیت اقتصادی کشور باشد» (نورزاد، ۱۳۸۹: ۱۷۴)؛ لیکن نهادن مصادیق پدیده‌های زیانبار اقتصادی در دسته بزهدی اقتصادی، بستگی به نوع نظام حقوقی دارد که به شدت از منابع عمده اقتصادی هر جامعه، متاثر است؛ برای مثال جرایم رایانه‌ای یا سایبری در برخی کشورها به عنوان جرم اقتصادی معرفی شده اند چراکه؛ در مواردی حملات رایانه‌ای یا انتشار برنامه‌های مخرب و موجد اختلال چون ویروس‌های رایانه‌ای ضربه جبران‌ناپذیر و خسارت‌هنگفتی را به اقتصاد آنها وارد می‌کند. حال آنکه در کشورهایی که اساساً استفاده چندانی از شبکه‌های رایانه‌ای نمی‌شود و یا اینکه این استفاده به صورت کاملاً محدود می‌باشد، اطلاق جرایم اقتصادی به این طیف از جرائم چندان مورد قبول نمی‌باشد.

در یک جمع‌بندی می‌توان گفت، در نظام حقوقی ایران که اقتصاد هم بخشی از امنیت ملی است، سخن از بزهد اقتصادی بدون آنکه این پدیده را در جرگه بزهد امنیتی دانست، شدنی نیست. بنابراین هرچند از دید قانون، نشانه‌هایی از قرار داشتن جاسوسی صنعتی در دسته بزهد اقتصادی نیست؛ به ویژه آنکه تبصره ماده ۳۶ قانون مجازات اسلامی ۱۳۹۲ که بر پایه بند ب ماده ۱۰۹ این قانون، در مقام شمارش بزهدی اقتصادی است، به جاسوسی اقتصادی و صنعتی اشاره نمی‌شود؛ اما بخش بزرگی از بزهد اقتصادی در ایران همچنان دارای چهره امنیتی است؛ لیکن در این میان پروایی نیست که در یک نظام حقوقی بدون مرز روشن در شناخت طبقه‌بندی بزهدی، جاسوسی صنعتی را در جرگه بزهد اقتصادی یا بزهد امنیتی یا هر دو دانست.

## ۴ رویارویی با جاسوسی صنعتی

در برابر ارتکاب رفتار جاسوسی صنعتی، چگونگی رویارویی با این پدیده نیز به عنوان جزئی از این پدیده بایستی مورد بررسی قرار گیرد که در زیر بیان می‌گردد:

### ۱.۴ رویارویی کیفی

با وجود عدم تصریح قانونی در مورد جرم انگاری جاسوسی صنعتی، نمی‌توان این جرم را رفتاری بدون سرزنش تلقی کرد، بلکه با توجه به عموم عنوان جاسوسی می‌توان این رفتار در زیر عنوان جاسوسی جای داد. البته پیش‌بینی قانونی رفتار جاسوسی رایانه‌ای این مشکل وجود ندارد اما تشخیص موضوع این جرم وابسته به تصویب آیین‌نامه‌ای گردیده است که در تبصره ۲ ماده ۷۳۱ قانون مجازات اسلامی به آن اشاره شده است که تاکنون این تبصره به تصویب نرسیده است و همین کوتاهی از سوی مرجع مذکور در قانون موجب شده تا اجرای این مواد به حالت تعلیق درآید و در حال حاضر امکان اجرای این مواد وجود ندارد.

به‌طور کلی، ضمانت اجرای جاسوسی صنعتی در ایران بر حسب جایگاه مرتکب و نوع اطلاعات و چگونگی ارتکاب، متفاوت است؛ بطورکلی، بر اساس نقش فضای سایبر و رایانه در ارتکاب بزه، به سراغ قوانین مربوط به جاسوسی سنتی و رایانه‌ای می‌رویم و با توجه به جایگاه مرتکب به قواعد مربوط به جرم‌انگاری نظامیان و موارد تشدید مجازات در ارتکاب جرائم رایانه‌ای توجه می‌نماییم. با این حال ضمانت اجرای اصلی، زندان است. هرچند جاسوسی اقتصادی با انگیزه مالی انجام می‌شود ولی جزای نقدی در اینجا تناسبی با این انگیزه ندارد؛ زیرا جاسوس به ویژه اگر برای دولت بیگانه می‌کوشد، سودش را نه از بزه بلکه از دولت بیگانه می‌گیرد، از این رو جزای نقدی کیفر شایسته‌ای برای این پدیده نیست. جاسوسی اقتصادی برای بیگانه به ویژه برای نظامیان با عنوان دیگری یعنی محاربه مطرح می‌شود و نیز گاه جاسوسی بر پایه گستردگی انجام رفتار و پیامدهای آن با عنوان حدی افساد فی الارض تفهیم می‌شود.

### ۲.۴ اقدامات پیشگیرانه

بر اساس عبارت معروف که پیشگیری بهتر از درمان است، وفق حکم عقل سلیم قبل از هر تهدیدی، بایستی امنیت را در مقابل آنها افزایش داد، بر همین اساس در مورد اطلاعات نیز باید اقدامات پیشگیرانه صورت گیرد. البته لزوم حفظ امنیت در لفظ «محرمانگی» نهفته است اما منظور از اقدامات پیشگیرانه در اینجا مقصود افزایش و نگهداری امنیت در سطحی مطلوب و متناسب با نوع اطلاعات است و چاره‌اندیشی در این مورد، یک قدم قبل از عرصه اصلی ارتکاب جرم است. به عبارت دیگر با اعمال اینگونه تدابیر می‌توان از آسیب‌پذیری اطلاعات کاست و با سخت‌تر کردن ارتکاب جرم نسبت به آنها، به نوعی پیش‌گیری وضعی در مورد آن اعمال کرد. همچنین افزایش نظارت بر این اسرار می‌تواند به نوعی اقدام پیشگیرانه محسوب گردد. در برخی موارد نیز افراد موقعیت‌های خطر را پیش‌بینی می‌کنند و سعی می‌کنند از این موقعیت‌ها بهره‌مند شوند، مانند اینکه دو نفری که در مورد فرمول نوشابه کوکاکولا اطلاع دارند، هم زمان با هم در یک مسافرت هوایی حق شرکت ندارند. مقصود از ارائه این بحث بررسی این نکته است که شناسایی این ضرورت و چاره‌اندیشی قانونگذار

نسبت به این مرحله از تهدید تا چه حد بوده است و این دست از تهدیدات تا چه حد دارای ضمانت اجرا قانونی است. بطور کلی اطلاعات ممکن است داده‌ها<sup>۱</sup>ی رایانه‌ای باشد یا اطلاعات فیزیکی و اسناد کاغذی، از همین رو حفظ امنیت در مورد آنها متفاوت صدق می‌کند.

در مورد پیش‌گیری قانونی از ارتکاب رفتارهایی که می‌تواند به ارتکاب جاسوسی صنعتی در فضای سایبر ختم شود، قانونگذار چاره‌اندیشی کرده و در ماده ۷۵۳ ق.م.ا به جرم‌انگاری رفتارهایی پرداخته است که «گاهی زمینه و مقدمه ارتکاب جرائم رایانه‌ای می‌شوند و گاهی تشکیل‌دهنده رفتار اصلی جرائم ناب رایانه‌ای می‌باشند که با توجه به موارد مذکور در ماده می‌توان آنها را در سه عنوان جای داد:

- تولید یا انتشار یا توزیع یا در دسترس گذاری یا معامله نرم افزارهای مجرمانه: در این جرائم، نرم افزارها موضوع جرم هستند؛ البته نه به این معنی که خود دارای ارزش می‌باشند، بلکه به این دلیل که استفاده از آنها پیش‌سازی برای ارتکاب جرم رایانه‌ای قرار می‌گیرند، به جرم‌انگاری رفتار نسبت به آنها پرداخته است.
- فروش یا پخش یا در دسترس گذاری داده‌های رخنه‌گر: سه عمل مذکور، رفتارهای این جرم هستند که بر روی گذر واژه و داده‌های رخنه‌گر صورت می‌گیرند. البته «این سه رفتار راهی برای انجام دسترسی غیر مجاز هستند و دارای موضوع مستقیم نمی‌باشند و تنها به جهت منتهی شدن به دسترسی غیر مجاز، جرم دانسته شده‌اند
- انتشار یا در دسترس قرار دادن محتویات آموزنده جرائم ناب رایانه‌ای: در اینجا نیز، همانند بند قبلی، در این جرم، محرمانگی داده‌ها و صحت و تمامیت آنها مورد نظر بودن است که، پیش‌بینی این دو رفتار برای بازدارندگی از تهدید آنها بوده است.

اما آنچه ذکر گردید مربوط به حمایت از داده‌های رایانه‌ای است» (عالی‌پور، ۱۳۹۵: ۴۵۲) و در جایی که این اطلاعات در قالب اسرار رایانه‌ای نباشند، فاقد حمایت قانونی هستند و این در حالی است که علی‌رغم گسترش فناوری رایانه هنوز هم بسیاری از اطلاعات در قالب اسناد فیزیکی و کاغذی تهیه و نگهداری می‌شوند که همواره امکان تهدید در مورد آنها وجود دارد که حمایت پیشگیرانه قانونی در مورد آنها صورت نگرفته است.

### ۳.۴ اقدامات بعد از ارتکاب

به این معنی که سیستم کیفی، پس از تکمیل جرم توسط مجرم کار را تمام شده نداند و به نوعی در صدد به حداقل رساندن آسیب جرم و جلوگیری از پیش‌روی جرم و تکرار جرم برآید؛ مثلاً بتوان اطلاعات لو رفته را به نوعی بازبازی امنیتی کرد و اطلاعات هرچند سوخته را از دسترس فرد مجرم خارج کند و مجرم را تا زمان فراموش شدن اطلاعات در بازداشت نگهدارد، در فضای سایبر نیز می‌توان با تغییر رمزهای عبور و سامانه‌ها و حامل‌های ذخیره اطلاعات این عمل را انجام داد و یا تمامی سامانه‌های الکترونیکی وی ضبط شود و پیگیری

<sup>1</sup>Data



سریع صورت گیرد تا اطلاعات در دسترس وی به سرعت امحاء گردد و اطلاعات ارسال شده احتمالی حذف گردد. همچنین سایر اطلاعات حساس شناسایی گردد تا ضریب امنیت آنها افزایش یابد. چرا که ممکن است مجرم تا زمانی که از ناآگاهی بزه دیده مطمئن است به پیشروی خود ادامه می دهد.

با توجه به اینکه بخش اعظمی از آسیب پذیری ناشی از عدم آگاهی است می توان اقداماتی را در جهت آگاه سازی افراد انجام داد، مانند اینکه بخشی از اقدامات پیشگیرانه را در قالب الزامات اداری گنجانده؛ همچون لزوم آگاهی و داشتن دانش مورد نیاز در زمینه راه های حفظ و تامین امنیت فضای سایبر و بایگانی اسناد محرمانه، آگاهی از تهدیدات سایبری و... به افرادی که به هر نحو به اطلاعات دسترسی دارند.

## ۵ همکاری یا رویارویی بین المللی

در زمینه رویارویی با جاسوسی صنعتی، وجود همکاری بین المللی نقشی اساسی دارد؛ چراکه در ارتکاب این جرم، عامل بیگانه، عنصر اصلی رفتار است. در نتیجه کوچکترین پیگیری در مورد این جرم نیاز دارد که با از مرزهای یک کشور فراتر گذاشت، عرصه ای که قلمرو کشوری دیگر است. در نگاه اول چنین به نظر می رسد که جامعه بین الملل از چنان پیشرفتی برخوردار است که کشوری بیگانه عرصه جولان مجرمین سایر کشورها نشود و نهادهای بین المللی تیزبینانه خلاءهای احتمالی موجود را پر خواهند کرد؛ لیکن اندکی تأمل ما را به نتیجه ای عکس می رساند.

### ۱.۵ شورای امنیت سازمان ملل متحد

این شورا، نهادی بین المللی است، که بر اساس بند یکم ماده ۳۶ منشور سازمان ملل متحد، «کشور قربانی یا زیان دیده می تواند یک جرم را به شورای امنیت ارجاع نماید» و در صورتی که شورای امنیت وضعیت را تهدیدی علیه صلح، نقض صلح یا اقدام تجاوزکارانه تلقی کند، می تواند اختیارات خود را بر مبنای فصل هفتم منشور اعمال کند. «هرچند در نظر طراحان منشور ملل متحد تهدید علیه صلح با استفاده از قوای مسلح متعارف محدود بود، اما دامنه آن به تدریج توسعه یافت؛ به نحوی که شورای امنیت می تواند با ارزیابی شرایط خاص هر قضیه، هرگونه اقدامی را تهدیدی علیه صلح تلقی کند؛ مانند یک حمله سایبری» (نقی زاد، ۱۳۹۵: ص ۸۲) لیکن در پذیرش رفتار جاسوسی به عنوان بزه ای علیه کشور دیگر از سوی سازمان، تردید وجود دارد؛ چراکه جاسوسی رفتاری اجتناب ناپذیر و طبیعی در عرصه بین المللی می باشد ضمن اینکه ادله اثبات این جرم، همواره مخفی و تا حد زیادی غیر قابل دسترس است. از همین رو، بسیار بعید به نظر می رسد که شورای امنیت در زمینه جاسوسی صنعتی ورود کرده و این عمل را تهدید علیه صلح بداند، رویه ای که تاکنون در پیش گرفته است.

### ۲.۵ دیوان کیفری بین المللی

گرچه در مورد جرائم ارتكابی در سطح بین المللی نهادی تحت عنوان «دیوان کیفری بین المللی» وجود دارد. طبق ماده ۵ اساسنامه «دیوان نسبت به چهار جرم نسل کشی، جرائم علیه بشریت، جرائم جنگی و تجاوز دارای

صلاحیت است». همچنین «صلاحیت دیوان تکمیلی و در کنار صلاحیت محاکم داخلی می‌باشد و هنگامی که تحقیقات و تعقیبی در سطح ملی انجام می‌شود، صلاحیت نخواهد داشت» (میانی و فردین، ۱۳۹۵: ۵۰). باتوجه به تعریف ارائه شده از تجاوز بند یک ماده هشت مکرر اساسنامه دیوان کیفری بین‌المللی؛ جاسوسی صنعتی را نمی‌توان نمونه‌ای از رفتار تجاوز دانست، چراکه؛ این عمل نه علیه حاکمیت و تمامیت ارضی یک کشور است و نه علیه استقلال سیاسی. به عبارت دیگر، این عبارات کلی مذکور در ماده را نمی‌توان بیش از حد گسترش داد و به حدی وسیع معنا کرد، که هر رفتار خلافی را علیه یک کشور، تجاوز به حساب آورد و تحت صلاحیت دیوان قرار داد. بر همین اساس «بهتر است که جنایت تجاوز فقط به موارد تجاوز توأم با جنگ یا هرگونه حمله و تهاجم به سرزمین یک دولت و یا اشغال و یا الحاق سرزمینی ناشی از حمله و تجاوز محدود گردد. چراکه گسترش بیش از حد این مفهوم به صلاح هیچیک از دولت‌ها نیست» (شایگانفرد، ۱۳۸۷: ۲۶۱).

بطور کلی در زمینه جاسوسی صنعتی، علی‌رغم مبتلابه بودن این جرم، همکاری بین‌المللی صریح و جامعی صورت نگرفته است و پشتیبانی دولت‌ها از جاسوسی صنعتی، همچنان پایه چنین همکاری‌ها را سست می‌کند. اینطور به نظر می‌رسد که کشورها تمایلی ندارند تا در این زمینه خود را ملزم به رعایت قواعد بین‌المللی کنند، چراکه؛ برخی از کشورها این عمل را در قانون داخلی خود جرم‌انگاری نکرده که یا ناشی از نقص قوانین و غفلت قانونگذاران بوده یا واقعاً عمل از دید آنها سرزنش پذیر نیست (مانند کشور فرانسه). «از دید برخی، این یک روند طبیعی است که موجبات رشد اقتصادی و صنعتی کشورهای کم‌توان را فراهم می‌کند و از ایجاد قطب ضعیف و قوی در اقتصاد جهانی جلوگیری می‌نماید» (عالی‌پور، ۱۳۹۶: ص ۲۲۵). به‌راستی در این یک دهه، هیچ پرونده جاسوسی صنعتی باز نشده است چرا که «عنصر سود دولت بیگانه بازدارنده‌ای دیگر در رویه قضایی دانسته می‌شود» (Edelma, 2011: 449) که گاه پیگرد پرونده‌ها را به بن بست می‌کشاند. با آنکه گفته می‌شود از دید «حقوق بین‌الملل راهکارهای چندی هست که برجسته‌ترین آنها مسؤلیت دولت در برابر زیان‌های برخاسته از جاسوسی اقتصادی است» (Lotrionte, 2015: 512) ولی این راهکارها هیچ‌یک چهره کیفری ندارد و در هر حال پیگرد و دادرسی نسبت به جاسوسی اقتصادی به ویژه سایبری که بدون حضور مرتکب در سرزمین کشور دیگر است، بزرگ‌ترین چالش فراروی دولت‌ها است.

## ۶ نتیجه‌گیری

جاسوسی صنعتی در فضای سایبر نسبت به اطلاعات حساس یا اسناد اقتصادی طبقه‌بندی شده متعلق به کشور دیگر است که چهره سیاسی و امنیتی آن کم‌رنگ شده ولی چهره اقتصادی آن پررنگ گردیده است. از این رو تحت سایه اقتصاد که چهره‌ای جهانی داشته و نیز رقابت‌های تجاری و صنعتی که معمولاً در حوزه خود، رفتارهای سرزنش‌پذیر نمی‌شود، قرار گرفته است. نتیجتاً جاسوسی صنعتی در فضای سایبر، پدیده‌ای نیست که بتوان با استفاده از نظام کیفری در سرکوب یا کنترل آن کوشید. از آنجا که دولت‌ها خود در تحقق این پدیده نقش دارند و در این زمینه حتی رقابت می‌کنند، در نتیجه تعامل و همکنشی سیاستی بس موثرتر از سیاست کیفری در قبال این پدیده است.

دستاورد این نوشتار در ترجمان جاسوسی صنعتی به عنوان رویکرد سیاسی و حقوقی در نظام کیفری کشورها است. به همان اندازه که ذکر جاسوسی صنعتی در قانون مجازات جرایم نیروهای مسلح می تواند نقش نهادهای نظامی در تولید صنعت دفاعی را نشان دهد، از سوی دیگر نبود این پدیده در قوانین کیفری دیگر، نشان می دهد چندان پدیده ای جدی برای صنعت نهادهای غیر نظامی نیست. به همین منوال برای کشورهای چون ایالات متحده، جاسوسی صنعتی یک بزه بسیار مهم تلقی می شود، چراکه؛ چنین کشورهای بستر شکل گیری اطلاعات عدیده صنعتی است؛ ولی همین نگرش را ممکن است کشوری دیگر چون چین که گرایش به روگرفت برداری دارد؛ نداشته باشد. بنابراین جاسوسی صنعتی خود می تواند به شاخصی تبدیل شود که نشان دهد حقوق کیفری تا چه اندازه از جایگاه و ماهیت اصلی خود دور شده است و به چه میزان به عنوان دستاویزی برای دولت در راستای سخت گیری یا سهل گیری بدل شده است.

## مراجع

- [۱] آقایی جنت مکان، حسین. «اجرای آرای کیفری بزهکاران اقتصادی». دانشنامه علوم جنایی اقتصادی. گردآورنده: امیرحسن نیازپور. تهران: میزان، ۱۳۹۶.
- [۲] تقی زاد، مهرداد. سازمانهای بین المللی و قاعده مندسازی فضای سایبر. تهران: خرسندی، ۱۳۹۵.
- [۳] شایگان فرد، مجید. «دیوان بین المللی کیفری و صلاحیت رسیدگی به جنایت تجاوز». فصلنامه حقوق دانشکده حقوق و علوم سیاسی، دوره ۳۸، ش ۴، زمستان ۱۳۷۸.
- [۴] صدیق، میر ابراهیم. «انقلاب سایبری و تحول در پدیده جاسوس». فصلنامه مطالعات راهبردی، ش ۷۱، بهار ۱۳۹۵.
- [۵] عالی پور، حسن. «جاسوسی اقتصادی». دانشنامه علوم جنایی اقتصادی. گردآورنده: امیرحسن نیاز پور. تهران: میزان، ۱۳۹۶.
- [۶] عالی پور، حسن. حقوق کیفری فناوری اطلاعات. تهران: خرسندی، ۱۳۹۵.
- [۷] قانون تجارت الکترونیکی، مصوب ۱۳۸۲.
- [۸] قانون جرائم و مجازات های نیروهای مسلح، مصوب ۱۳۸۲.
- [۹] قانون مجازات اسلامی، بخش تعزیرات، مصوب ۱۳۷۵.
- [۱۰] قانون مجازات اسلامی، مصوب ۱۳۹۲.
- [۱۱] میانی، علیرضا و فردین، مینا. «صلاحیت دیوان کیفری بین المللی». فصلنامه مطالعات علوم اجتماعی، دوره ۲، ش ۱، بهار ۱۳۹۵.
- [۱۲] میرمحمدی، مهدی و سالارکیا، غلامرضا. «سازمانهای اطلاعاتی و توسعه اقتصادی». فصلنامه مطالعات راهبردی، سال پانزدهم، ش ۳، پاییز ۱۳۹۱.
- [۱۳] نورزاد، مجتبی. جرائم اقتصادی در حقوق کیفری ایران. تهران: جنگل، ۱۳۸۹.
- [۱۴] نیازپور، امیرحسن. دانشنامه علوم جنایی اقتصادی. تهران: میزان، ۱۳۹۶.
- [15] K. Benner. "Cyber Spying Road Rules," benner-on-tech-cyber-spying-road-rules, Bloomberg, 2020, available at: <https://www.bloomberg.com>.
- [16] W. Edelman. "The Benefit of spying: Defining the boundaries of economic espionage under the Economic Espionage Act 1996," Stanford Law Review, vol.63, 2011.

- [17] C. Lotrionteatherine. "Countering state sponsored cyber economic espionage under international law," N.C.J.I-NT'LL. & COM. REG, vol. XL, 2015.
- [18] Rome Statute of International Criminal Court Done at Rome on, 17 July 1998.
- [19] R. Sterken. "the digital revolution in international relation: Chinese accuse of widespread cyber-espionage," 2018.

## مدل سازی دینامیکی هوشمند صادرات در کشورهای نفت خیز

ارشیا بادی<sup>۱</sup>، حبیب الله آراسته راد<sup>۲</sup>، محمد طالبی<sup>۳</sup>، اسماعیل ناظم شهرضا<sup>۴</sup>

<sup>۱</sup> پژوهشگر پسادکتری، دانشکده اقتصاد و پژوهشکده سامانه‌های هوشمند، دانشگاه تهران  
arshia.badi@guest.ut.ac.ir

<sup>۲</sup> استادیار، پژوهشکده سامانه‌های هوشمند، دانشگاه تهران  
habib.arasteh@ut.ac.ir

<sup>۳</sup> دانشجوی دکتری، دانشکده اقتصاد و پژوهشکده سامانه‌های هوشمند، دانشگاه تهران  
muhammادتalebi@ut.ac.ir

<sup>۴</sup> استادیار، مؤسسه علوم و فنون حکمت‌بنیان، پژوهشکده سامانه‌های هوشمند، دانشگاه تهران  
esmailnazem@ut.ac.ir

### چکیده

در این مقاله با استفاده از مدل دینامیک سیستم هوشمند به طراحی سیستم تجارت خارجی در اقتصاد کلان پرداخته‌ایم، در ابتدا مدل ریاضی مبتنی بر واردات، صادرات و تولید داخل توسعه داده شده است. یکی از روش‌های تنظیم‌گری در کشورهای پیشرفته با حجم صادرات بالا اعمال تعرفه بر صادرات در برخی از محصولات است، اما این موضوع در کشورهای در حال توسعه بسیار متفاوت است. تفاوت نرخ ارز رسمی و بازار سیاه در اقتصادهای مذکور سبب می‌شود صادرکنندگان برای کسب سود بیشتر با استفاده از راه‌های جایگزین تا حد امکان ارز صادراتی را حفظ کنند و یا آن را در بازار سیاه عرضه کنند. لذا دولت‌ها همواره در پی جلوگیری از این موضوع هستند مدل مذکور با در نظر گرفتن میزان تعرفه صادراتی، مالیات بر ارزش افزوده و تاثیر درآمد نفتی در کشورهای نفت‌خیز مورد بررسی قرار گرفته است. نتیجه حاصل شده نشان می‌دهد اهمیت درآمد نفتی در حوزه کشورهای نفت‌خیز امری بسیار مهم است؛ اما در صورت تحریم یا قطع صادرات می‌تواند اثرات جبران‌ناپذیری بر روی اقتصادهای وابسته ایجاد نماید. لذا استفاده از بسترهای اقتصادی با مزیت صادراتی غیرنفتی بسیار مهم ارزیابی می‌شود.

**کلمات کلیدی:** سیستم تجارت خارجی، اقتصاد کلان، صادرات، مدل سازی دینامیکی هوشمند، کشورهای نفت‌خیز.

### ۱ مقدمه

مالیات بر صادرات سیاستی است که معمولاً به جهت تنظیم‌گری در سراسر جهان وضع می‌شود. در سال ۲۰۱۰، سازمان همکاری اقتصادی و توسعه (OECD) نتیجه گرفت که از سال ۲۰۰۳ تا ۲۰۰۹، ۶۵ عضو از ۱۲۸ عضو سازمان تجارت جهانی برخی از انواع محدودیت صادرات را به ویژه برای کالاهای خام اعمال

کرده‌اند [۲]. از آنجا که تأثیر اصلی مالیات‌های صادراتی در کاهش قیمت داخلی کالاها است، این موضوع اغلب به‌عنوان سیاست امنیت غذایی اعمال می‌شود [۳].

توجیه دیگر استفاده از مالیات بر صادرات شامل بهبود شرایط تجارت، افزایش درآمد عمومی و پاسخ به افزایش تعرفه در کشورهای پیشرفته است [۴]. بیشتر تعرفه، به‌عنوان وضعیتی تعریف می‌شود که در آن با پردازش بیشتر یک محصول، حقوق واردات افزایش می‌یابد، که منجر به محافظت مؤثر برای مرحله تولید نهایی یک زنجیره ارزش می‌شود، این سیاست وقتی در کشورهای پیشرفته اعمال می‌شود، به نفع صنایع تولیدی در این کشورها است [۴]. در پاسخ به تشدید تعرفه‌ها، برخی از کشورهای در حال توسعه نرخ‌های مالیاتی صادرات را در طول زنجیره ارزش تولید خود کاهش می‌دهند تا تولید فرآوری شده بیشتری را در کشورهای خود گسترش دهند.

همان‌طور که توسط کوردن (۱۹۷۱) اشاره شده است [۵]، مالیات صادرات کالاها اولین به‌عنوان یارانه غیرمستقیم صنایع تبدیلی عمل می‌کند، اشمیتز و زیلبرمن (۱۹۷۹) نشان می‌دهند که در یک مدل تجارت بین‌الملل با یک بنگاه تجاری بین‌المللی که از قدرت انحصار استفاده می‌کند [۶]، دولت در کشور صادر کننده ممکن است مالیات صادرات را برای به حداکثر رساندن رفاه اعمال کند. ایتون و گروسمن (۱۹۸۶) [۷]، رودریک (۱۹۸۹) [۸]، برنهوفن (۱۹۹۷) [۹] و دنوردورف و راجارامان (۲۰۰۵) بر روی بحث تغییر سود تمرکز دارند [۱۰]، در حالی که پیرمارتینی (۲۰۰۴) [۴]، همچنین میترا و جوزلینگ (۲۰۰۹) [۱۱] و کیم (۲۰۱۰) [۱۲]، مروری بر ادبیات نظری و تجربی مالیات بر صادرات ارائه می‌دهند. بوییت و لایورد (۲۰۱۲) منطق مالیات صادرات را در زمینه بحران غذایی ارزیابی کردند [۱۳]. سرانجام، بوییت، استرادیس و لایورد (۲۰۱۳) تأثیر مالیات‌های صادراتی بر رفاه جهانی را برای همه بخش‌ها ارزیابی کردند و دریافتند که حذف مالیات‌های صادراتی رفاه جهانی را ۰/۲۳٪ افزایش می‌دهد.

دینامیک سیستم یک روش مدل‌سازی رایانه‌ای است که ریشه‌های فکری آن در مهندسی کنترل، علوم مدیریت و محاسبات دیجیتال است [۱۴]. در مدل‌سازی دینامیکی سیستم، رفتار ((واقعی)) سیستم زیربنایی مفهوم یافته و در طول زمان پیوسته آشکار می‌شود. به‌همین ترتیب، از نظر ریاضی، یک مدل دینامیک سیستم یک مدل معادله دیفرانسیل معمولی است. برای تقریب راه حل مدل معادلات دیفرانسیل معمولی زمان پیوسته در رایانه دیجیتال (گسسته)، از معادلات تفاضلی استفاده می‌شود. برخلاف مدل‌سازی معادله تفاضلی سنتی در اقتصاد، که در آن افزایش زمان برای مطابقت با داده‌های اقتصادی انتخاب می‌شود (به‌طور معمول یک چهارم یا یک سال)، افزایش زمان در مدل‌سازی دینامیک سیستم برای ارائه یک راه حل دقیق برای مسئله انتخاب می‌شود در دسترس است [۱۴].

تأثیرات گسترده نرخ ارز بازار سیاه بر صادرات به‌طور گسترده مورد بررسی قرار گرفته است. با این حال، تا زمانی که برابری بینتو در زمینه حق بیمه بازار سیاه و یکسان‌سازی نرخ ارز در جنوب صحرائی آفریقا کار نکرد، اولین مدل کمی را در تلاش برای توضیح پدیده مالیات ضمنی صادرات به‌وجود آورد [۱۵]، در مدل بینتو برای سادگی، فرض بر این است که هزینه‌های دولت فقط شامل کالاهای وارداتی و پرداخت‌های ثابت خارجی است. حال  $t$  و  $g$  به‌ترتیب در واحدهای ارزی خارجی به‌عنوان هزینه دولت و درآمد رسمی مالیات نشان داده می‌شود.  $e$  به‌عنوان نرخ رسمی ارز مشخص می‌شود.



$$\Delta M = e(g - t) \quad (1)$$

یعنی کسری رسمی از نظر واحدهای ارزی محلی برابر با تغییر در عرضه پول است. همچنین می‌تواند به عنوان مالیات تورم ناشی از افزایش حجم پول انتقال قدرت خرید از شهروندان به دولت تعبیر شود. با توزیع  $e$ ، این معادله را می‌توان به صورت (۲) نوشت:

$$\frac{\Delta M}{M} \frac{M}{b} \frac{b}{e} = (g - t) \quad (2)$$

جایی که  $M$  عرضه پول است،  $b$  نرخ بازار سیاه است. جمله‌ی اول در سمت راست،  $\frac{\Delta M}{M}$  را می‌تواند به عنوان درصد تغییر در عرضه پول (یا نرخ مالیات تورم) در نظر گرفت. جمله‌ی دوم،  $\frac{M}{b}$  می‌تواند به عنوان پایه پول برای مالیات تورم از نظر مقدار ارز خارجی حاصل از بازار سیاه در نظر گرفته شود. جمله‌ی سوم،  $\frac{b}{e}$  را می‌توان به عنوان ضریب حق العمل بازار سیاه در نظر گرفت.

مدل پینتو اولین و تنها در نوع خود بود که سعی در توضیح دینامیک نرخ بازارهای سیاه و مالیات صادراتی ضمنی داشت [۱۵]. با این حال، نقاط ضعف بارز بسیاری دارد. از نظر حسابداری، اساساً فرض بر این است که تنها منابع درآمد ارزی دولت مالیات رسمی و تورم است و بسیاری از منابع قابل توجه دیگر که توسط دولت‌های جهان واقعی استفاده می‌شود، نادیده گرفته می‌شود. علیرغم این نقص‌ها، پاشنه آشیل واقعی آن در این واقعیت نهفته است که از دینامیک بین صادرکنندگان، واردکنندگان و دولت صرف نظر می‌کند. این مدل فرض می‌کند که دولت‌ها برای تأمین نیازهای مالی از جمله تأمین مالی واردکنندگان یارانه از طریق نرخ رسمی، به همان اندازه که می‌توانند ارز خارجی را از طریق کانال‌های رسمی تهیه کنند و سپس به سادگی برگردانده و بقیه را به طور ضمنی از صادرکنندگان تأمین کنند. این به معنای دیدگاه بازار سیاه به عنوان یک «بزار ریاضی» ساده است که در آن می‌توان ساده‌لوحانه مالیات صادرات را به عنوان یک تفاوت ساده بین هزینه‌های واقعی و نظری دولت استخراج کرد. با این وجود، این موارد کاملاً نادیده گرفته شده است که این امکان را فراهم کرده است. آنها همچنین به بازار سیاه دسترسی دارند و می‌توانند تصمیم بگیرند که چه میزان از درآمد خود را از طریق کانال‌های رسمی و یا موارد دیگر ثبت کنند. بنابراین، ضروری است که یک مدل صحیح از مالیات صادراتی ضمنی، تلفیق چشم انداز صادر کننده باشد [۱۵].

## ۱.۱ کسری بودجه و مالیات صادرات

مشهورترین روشی که دولتها از طریق آن بودجه کسری را تأمین می‌کنند، از طریق صدور ارز جدید است که به آن سینیورژ<sup>۱</sup> می‌گویند. یک روش ثانویه دیگر، روشی غیرمعمول و کمتر متداول وجود دارد که به عنوان مالیات صادرات ضمنی شناخته می‌شود. دولتها می‌توانند با مجبور کردن صادرکنندگان برای تسلیم ارز

<sup>1</sup>seigniorage

خارجی با نرخ‌های رسمی و کم ارزش ارز محلی، مازاد ارز تولید کنند. با این حال، توانایی مالیات ضمنی صادرکنندگان منوط به وجود یک نرخ ارز موازی «بازار سیاه» است. در این سناریو، یک نرخ ارز «رسمی» تعیین شده توسط دولت وجود دارد و یک نرخ بازار سیاه شناور آزاد است که توسط نیروهای عرضه و تقاضا تعیین می‌شود، دومی به دلیل غیرقانونی بودن با این لقب درگیر شده است. نرخ ارز رسمی که بیش از حد ارزش‌گذاری شده است به طور مؤثر به عنوان یارانه وارداتی ضمنی عمل می‌کند. واردکنندگان ممتاز قادر به مبادله ارز محلی با ارز خارجی با این نرخ هستند و به آنها اجازه می‌دهد کالاهایی با ارزش بیشتر از ارزش واقعی ارز محلی خود را وارد کنند. البته این اختلاف بین ارزش رسمی و واقعی واردات باید از طریق دولت تأمین شود. این امر با هزینه‌ی صادرکنندگان محقق می‌شود. صادرکنندگان قادر نیستند ارزش واقعی صادرات خود را بدست آورند [۱۶].

زیرا دولت آنها را مجبور می‌کند ارز خود را به‌ازای مبلغ ارزان‌تر تحویل دهند و باعث ایجاد دینامیک جالب بین این دو موضوع می‌شود. صادرکنندگان باید تصمیم بگیرند که تا چه حد در بازار سیاه مشارکت داشته باشند که به نوبه‌ی خود بر میزان مالیات صادراتی ضمنی دولت از آنها تأثیر می‌گذارد.

سیاست‌های تجاری مجموعه سیاست‌ها و اقداماتی است که در جهت هدایت تجارت خارجی کشورها اعمال می‌شود. این سیاست‌ها از دو طریق ابزارهای بازاری و غیر بازاری اعمال می‌شوند. وضع تعرفه‌های گمرکی معمول‌ترین ابزار بازاری و اقدامات غیرتعرفه‌ای شامل ممنوعیت‌ها و محدودیت‌های تجاری، الزاماتی چون اخذ انواع مجوز برای واردات و صادرات و اعطای انواع یارانه به ویژه یارانه‌های صادراتی از معمول‌ترین ابزارهای غیربازاری هستند. جهت‌گیری این سیاست‌ها می‌تواند در راستای افزایش صادرات در جهت گسترش بازار برای صنایع داخلی (راهبرد توسعه صادرات) و یا ایجاد محدودیت در واردات در جهت حمایت از تولید داخلی، کنترل تقاضای ارز و بهبود تراز پرداخت‌ها (راهبرد جایگزینی واردات) باشد [۱].

این مقاله در پنج بخش تهیه شده است که در بخش اول شاهد مقدمات اقتصادی در حوزه صادرات بودیم. در بخش دوم به مدل‌سازی ریاضی تولید داخل، واردات و صادرات پرداخته می‌شود. در بخش سوم این مقاله نسبت به توصیف صادرات و شکاف نرخ ارز در بین بخش رسمی و غیررسمی پرداخته شده است. در بخش چهارم شبیه‌سازی سیستم دینامیکی صادرات و سپس در قسمت پایانی نتیجه‌گیری فنی و اقتصادی از مقاله صورت گرفته است.

## ۲ مدل ریاضی

مدل دینامیکی حمایت از تولیدات داخلی با استفاده از مدل ارائه شده توسط آرشم (۲۰۱۳)، رازین و وسگرا (۲۰۱۱) و کاتایاما (۲۰۱۲)، [۱۹]، [۱۸]، [۱۷] با در نظر گرفتن عوامل مؤثر موقت در تجارت بین‌الملل بر اساس معادلات (۳ تا ۷) دینامیک مربوط به بودجه دولت، منحنی تقاضا، سود واردات و سود قاچاق را نشان می‌دهد. با توجه به مقررات معرفی شده، مبلغ بدست آمده از معادلات که شامل عوارض گمرک و مالیات می‌باشد به بودجه کشور تخصیص می‌یابد.

$$S = \tau qy + sxp + \alpha zp + \tau_{exp} \cdot X \cdot e \cdot p_{exp} \quad (3)$$

$$p(x + y + z) = M \quad (4)$$

$$D = y(p - q - \tau q) \quad (5)$$

$$G = z[(1 - \alpha)p - q] \quad (6)$$

$$E = X(p_{exp} \cdot e - p - \tau_{exp} \cdot e \cdot p_{exp}) \quad (7)$$

$\alpha$  مؤثر بودن گمرک،  $p$  قیمت محصول در داخل کشور،  $x$  میزان تولید داخلی،  $y$  میزان واردات کالا،  $q$  قیمت محصول در خارج از کشور،  $y$  حجم واردات و  $z$  حجم قاچاق،  $X$  حجم صادرات،  $p_{exp}$  قیمت کالا در خارج از کشور،  $e$  نرخ ارز در بازار داخلی (جهت سادگی میزان آن را ثابت (۱) در نظر می‌گیریم) است.  $M$  مبلغ ثابتی که مردم برای محصول معین پرداخت می‌کنند و کالای وارداتی جایگزین ندارد،  $D$  سود واردات، هدف چنین مقررات اغلب درآمد از محل مالیات‌ها و پرداخت‌های گمرکی و یا رشد بخش تولید داخلی در حجم فروش است. عوارض گمرکی به‌عنوان تعرفه  $\tau$  نامیده می‌شود، مالیات بر ارزش افزوده به‌عنوان  $s$  و مالیات صادرات  $\tau_{exp}$  تعیین شده است.  $G$  سود حاصل از واردات کالا به‌صورت قاچاق می‌باشد.  $E$  سود صادرات کالا به خارج در نظر گرفته می‌شود. انگیزه‌های تغییر حجم تولیدکننده داخلی می‌تواند متفاوت باشد: ایجاد شغل، تشکیل پتانسیل صادراتی کشور، تقویت تولید مرتبط با امنیت ملی و غیره. در هر حالت، تغییر در میزان تولید داخل و قیمت آن بسته به شرایط بازار عمل خواهد کرد.

با توجه به معادله (۸) میزان قیمت با توجه به تقاضا در بخش واردات داخلی تغییر می‌کند.

$$\frac{dP}{dt} = f \cdot (Y_d - x - y - z) \quad (8)$$

در معادله بالا  $f$  افزایش مقطعی قیمت و  $Y_d$  میزان تقاضای داخلی است که با توجه به سناریو مطلوب در نظر گرفته شده است. همچنین جهت رسیدن به قیمت کالا در بخش خارجی معادله (۹) را خواهیم داشت:

$$\frac{dP_{foreign}}{dt} = f \cdot (Y_{d,exp-foreign} - x_{foreign} - y_{foreign} (= X)) \quad (9)$$

در معادله بالا  $x_{foreign}$  میزان تولید کالا در خارج از کشور،  $Y_{d,exp-foreign}$  میزان تقاضا در خارج و  $y_{foreign}$  میزان واردات کشور خارجی می‌باشد که از منظر ما می‌تواند میزان صادرات به یک کشور در نظر گرفته شود.



شکل ۱: زیرسیستم تجارت خارجی در بخش واردات و صادرات

## ۳ صادرات

استراتژی صادرات به ارسال کالاها به مکان‌ها یا کشورهای دیگر برای فروش یا معاوضه است. در اقتصاد، یک کالای صادره یا هر کالای خوب از یک کشور تا کشور دیگر در یک شیوه مشروع است.

### ۱.۳ مدل مالیات صادرات اصلاح شده

مدل پینتو به عنوان پایه ای برای شهود ریاضی مالیات صادراتی ضمنی خوب عمل می‌کند، اما بر فرضیات ساده ای تکیه می‌کند که تعمیم به دنیای واقعی را دشوار می‌کند. بسیاری از کاستی‌های آن این فرض است که دولت‌ها فقط برای واردات و پرداخت سود خارجی هزینه می‌کنند. این مدل متغیرهای مربوط به صادرات یا عمده هزینه‌های دولت را در نظر نمی‌گیرد. مدل در نظر گرفته شده در این بخش مبتنی بر مدل قبلی، مدل اصلاح شده ارائه می‌دهیم [۱۶].

$$G = (\Delta M = D) + T + OR \quad (10)$$

$$ID = (\Delta M = D) + \Gamma \sim ID = \text{Total Import} \cdot (b - e) \quad (11)$$

در معادلات (۱۰ و ۱۱) هزینه‌های دولت ( $G$ ) را برابر با جمع تغییر در عرضه پول ( $\Delta M$ ) که می‌توان آن را به عنوان مالیات تورم تفسیر کرد، مالیات ( $T$ ) و سایر منابع درآمد ( $OR$ ) تعیین می‌کنیم. توجه به این نکته مهم است که در این زمینه، می‌توان تغییر در عرضه پول را کسری دولت ( $D$ ) نیز تصور کرد. سپس، تفاوت بین استفاده از ارز بازار سیاه و نرخ ارز رسمی برای محاسبه ارزش کل واردات در واحدهای ارزی محلی ( $ID$ ) برابر با جمع کسری دولت ( $\Delta M = D$ ) و مالیات صادراتی ضمنی را تعیین کردیم. به طور یقین، این موضوع بیان می‌کند که کسری دولت (همان‌طور که از گزارش‌های مخارج رسمی و منابع درآمد محاسبه شده است) برای پرداخت بخشی از هزینه‌های وارداتی یارانه ضمنی استفاده می‌شود. بقیه از مالیات ضمنی

دریافت شده از صادرکنندگان است. همچنین می‌توانیم مالیات صادرات ضمنی را به شکل تابع (۱۲) تشریح کنیم:

$$\Gamma = (1 - \phi) \cdot X \cdot (b - e) \quad (12)$$

جایی که  $(\phi)$  سهم صادراتی است که از طریق بازار سیاه محاسبه می‌شود (بین ۰ تا ۱)،  $X$  ارزش کل صادرات (در واحدهای ارزی)،  $b$  نرخ ارز بازار سیاه است و  $e$  نرخ ارز رسمی است. منطق این است که صادرکنندگان، که معمولاً ارزهای خارجی را دریافت می‌کنند، باید در مورد نسبتی که از طریق نرخ ارز بازار سیاه مبادله می‌کنند تصمیم بگیرند (در نتیجه ارز محلی بیشتری نسبت به نرخ رسمی دریافت کنند). پس از آن دولت فقط می‌تواند از مبلغ  $(1 - \phi) \cdot X$  فاکتور شده از طریق نرخ رسمی سود ببرد. این سود را می‌توان به عنوان تفاوت بین فاکتور دادن این مقدار از طریق نرخ بازار سیاه در مقابل نرخ رسمی الگوی خود قرار داد [۱۶].

در نگاه اول، می‌توان فرض کرد  $X$  با تبدیل آمار صادرات به واحدهای ارزی با استفاده از نرخ بازار رسمی یا بازار سیاه به راحتی می‌توان به دست آورده شود. با این حال، همان‌طور که قبلاً نشان داده شد، در کشورهایی که بازارهای سیاه پررونقی دارند، خیلی ساده نیست. در حقیقت، هیچ منبع معتبری برای چنین داده‌هایی وجود ندارد. در عوض،  $X$  را می‌توان از طریق موارد زیر به دست آورد:

$$E = (1 - \phi) \cdot X \cdot e \quad (13)$$

در اینجا، صادرات  $E$  به طور رسمی از نظر واحد پول محلی مشخص می‌شود تنها چیزی که در نهایت باقی مانده است استخراج  $(\phi)$  می‌باشد.

## ۴ شبیه‌سازی بخش صادرات

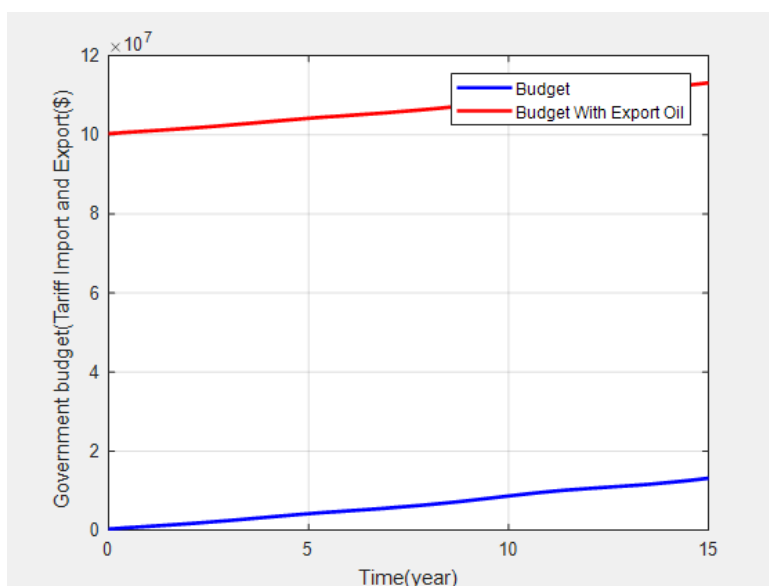
در این بخش از شبیه‌سازی سیستم تجارت خارجی را با در نظر گرفتن صادرات در حوزه نفتی نسبت به تاثیر این درآمد در بودجه کلی کشور می‌پردازیم. باید توجه داشت در اکثر کشورهای در حال توسعه درآمد حاصل از نفت و صادرات آن در اختیار دولت می‌باشد، لذا می‌توان در نظر گرفت که مالیات (تعرفه صادراتی) بر این کالا حاکم نخواهد بود، به این علت که کل درآمد مستقیم به خزانه واریز می‌گردد. در جدول ۱ لیستی از پارامترها و مقادیر مورد استفاده در این بخش را مشاهده می‌کنید.

به منظور شبیه‌سازی بازار تقاضای داخلی در کشور از تابع سینوسی و غیر خطی استفاده می‌کنیم. مدت زمان شبیه‌سازی را ۱۵ سال در نظر می‌گیریم. بازار با رشد و کاهش شدید تقاضا مواجه است. حداکثر میزان تقاضا که در پیک سیگنال سینوسی به وجود می‌آید در حدود ۶۰۰۰ تقاضا می‌باشد. همچنین مقدار اولیه آن ۵۰۰ می‌باشد (شکل ۲).

همان‌طور که در شکل ۲ مشاهده می‌شود وجود عامل صادرات نفت درآمد دولت را تا حدود ۶ الی ۷ برابر افزایش می‌دهد. لذا این موضوع نشان‌دهنده اهمیت صادرات نفت جهت توسعه کشور می‌باشد. همچنین

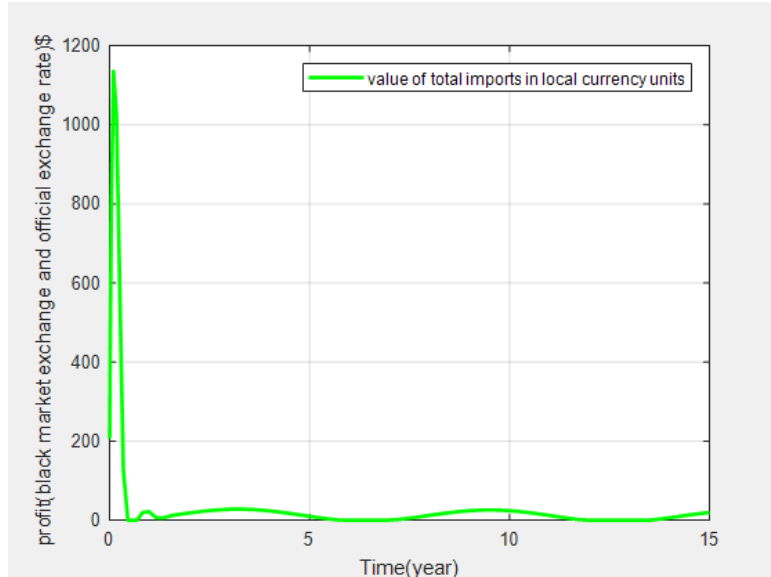
جدول ۱: پارامترهای مدل تجارت خارجی در بخش صادرات

۵۰	میزان تولید اولیه	$x_1$
۱۵۰۰	میزان تولید در سال پانزدهم	$x_n$
۵۰۰	تقاضا اولیه	$Y_{d0}$
ورودی سینوسی با دامنه ۵۵۰۰	تقاضا نهایی	$Y_{dn}$
۰/۰۹	مالیات بر ارزش افزوده	$s$
۳۰۰۰۰	قیمت محصول وارداتی نوع ۱ در خارج از کشور	$q$
۷۰۰۰۰	قیمت اولیه محصول وارداتی نوع ۱ در داخل کشور	$p_0$
۵	حجم قاچاق	$z$
۱۰	بهره کنترل کننده تناسبی	$P$
۱۰۰	بهره کنترل کننده انتگرالی	$I$
متغیر بر اساس کسش قیمتی تقاضا	میزان واردات هدف	$y_r$
۲۰۰۰	حجم صادرات نفت	$x_e$
۵۰۰۰۰	قیمت داخلی نفت	$p_e$



شکل ۲: بررسی میزان بودجه کشور با اضافه کردن درآمد صادراتی





شکل ۳: میزان سود واردات حاصل از تفاوت قیمت ارز داخلی و بازار سیاه

جهت جلوگیری از ورود بدون ضابطه این از حجم از پول به سیستم مالی کشور در نظر گرفتن صندوق ارزی جهت ذخیره امری مهم است.

همچنین جهت دستیابی به میزان سود واردکنندگان در خلال بازار سیاه نرخ ارزی همان طور که در شکل ۳ مشاهده می کنید، با توجه به اینکه سیاست کشور مفروض عدم واردات است کاهش زیادی خواهد داشت. البته بایستی در نظر داشت که این تنها فرضی جهت اثبات منطق معادلات به کار رفته می باشد، به این علت که در صورت نبودن کالا در بازار تشنه کالای مصرفی شاهد افزایش قیمت بسیار زیاد خواهیم بود. یکی از راه های تکمیل مدل سازی استخراج میزان کمبود کالا است. در زمانی که شاهد کمبود به علت فقدان تولید باشیم و هدف دولت سیاست عدم واردات باشد ناخودآگاه به علت شکاف بازار و نرخ ارز داخلی، جریان قاچاق به دلیل سود زیاد شکل خواهد گرفت، در شکل ۳ با توجه به مطالب بیان شده در بخش های قبلی شاهد میزان سود عایدی برای واردکنندگان به دلیل اختلاف نرخ ارز بازار داخلی و بازار سیاه بر اساس معادله (۱۲) هستیم. نرخ ارز در بازار داخلی ( $e = 11000$ ) و نرخ آن در بازار سیاه ( $b = 30000$ ) در نظر گرفته شده است.

## ۵ نتیجه گیری

در این مقاله مدل ریاضی از تجارت خارجی در بخش صادرات توسعه یافته است. اهمیت صادرات برای اقتصادهای شکوفا بسیار پر اهمیت است، اما در صورتی که صادرات اصلی ترین تکیه گاه اقتصادی باشد، موضوع متفاوت خواهد شد. این موضوع به خصوص در کشورهای نفت خیز و در حال توسعه نمود بیشتری خواهد داشت.

در صورت قطع یا کاهش درآمد صادراتی در کنار وابستگی ارزی سبب خواهد شد که شکافی بین قیمت ارز در داخل ایجاد شود که همواره نرخ غیر رسمی نسبت به قیمت رسمی بالاتر خواهد بود. در این شرایط اعمال مالیات یکی از راه‌های جبران این اختلاف و جلوگیری از احتکار و فاکتورسازی است.

## مراجع

- [۱] مظاهری، مرتضی (۱۳۹۶). بررسی آثار سیاست‌های تعرفه‌ای بر اقتصاد ایران، گروه پژوهشی مطالعه کمی سیاست‌گذاری اقتصادی.
- [2] Organization for Economic Cooperation and Development. 2010. The Economic Impact of Export Restrictions on Raw Materials. OECD Trade Policy Studies, Paris, OECD, Trade and Agriculture Division.
- [3] Bouët, A., and D. Laborde. 2010. Assessing the Potential Cost of a Failed Doha. World Trade Review 9: 319–351.
- [4] Piermartini, R. 2004. The Role of Export Taxes in the Field of Primary Commodities. WTO Discussion Paper, World Trade Organization, Geneva.
- [5] Corden, W.M. 1971. The Theory of Protection. Oxford: Clarendon Press.
- [6] Just, R.E., A. Schmitz, and D. Zilberman. 1979. Price Controls and Optimal Export Policies under Alternative Market Structures. American Economic Review 69: 706–714.
- [7] Eaton, J., and G.M. Grossman. 1986. Optimal Trade and Industrial Policy under Oligopoly. Quarterly Journal of Economics CI: 383–406.
- [8] Pinto, B. 1989. Black Market Premia, Exchange Rate Unification, and Inflation in Sub Saharan Africa. The World Bank Economic Review, 3(3), 321–338. doi: 10.1093/wber/3.3.321.
- [9] Bernhofen, D. 1997. Strategic Trade Policy in a Vertically Related Industry. Review of International Economics 5(3): 429–433.
- [10] Deardorff, A.V., and I. Rajaraman. 2005. Can Export Taxation Counter Monopsony Power? Research Seminar in International Economics Discussion Paper. Ann Arbor, MI: Research Seminar in International Economics, University of Michigan.
- [11] Mitra, S., and T. Josling. 2009. Agricultural Export Restrictions: Welfare Implications and Trade Disciplines. IPC Position Paper, Agricultural and Rural Development Series, Washington DC: International Food and Agricultural Trade Policy Council.
- [12] Kim, J. 2010. Recent Trends in Export Restrictions. Organization for Economic Cooperation and Development Trade Policy Working Papers, No. 101, OECD, Paris.
- [13] Bouët, A., C. Estrades, and D. Laborde. 2013. A Global Assessment of the Economic, Effects of Export Taxes. The World Economy 36(10): 1333–1354.
- [14] MICHAEL J. R. 2008. System Dynamics and Its Contribution to Economics and Economic Modeling, Worcester Polytechnic Institute, Encyclopedia of Complexity and Systems Science Worcester, USA.

- [15] Pinto, B. 1989. Black Market Premia, Exchange Rate Unification, and Inflation in Sub Saharan Africa. *The World Bank Economic Review*, 3(3), 321–338. doi: 10.1093/wber/3.3.321.
- [16] J.Chen, S.Choi, 2020. A PRACTICAL MATHEMATICAL MODEL FOR IMPLICIT EXPORT TAXES, No.156, Johns Hopkins Institute for Applied Economics, Global Health, and the Study of Business Enterprise.
- [17] Arsham, H. 2013. MODELING TARIFF TO ANALYZE PROTECTIONISM, *International Journal of Pure and Applied Mathematics*, Volume 84, No. 4, <http://dx.doi.org/10.12732/ijpam.v84i4.9> (ON ONE PUBLICATION in IJPAM Alexander V. Prasolov, St. Petersburg State University St. Petersburg, Russia).
- [18] A. Razin, H-J. Vosgerau, 2011. *Trade and Tax Policy, Inflation and Exchange Rates: A Modern View*, Springer, New York, N.Y.
- [19] S. Seiichi Katayama, (Editor), H. Ursprung, 2012. *International Economic Policies in a Globalized World*, Springer, New York, N.Y.



## روند تکوین جنبش‌های اجتماعی در تطبیق محیط مجازی با محیط واقعی

عباس چگینی<sup>۱</sup>

<sup>۱</sup> پژوهشگر و مسئول مرکز زبان‌شناسی و مدیریت دانش دانشگاه جامع امام حسین (ع)  
ababbas848@gmail.com

### چکیده

شکل‌گیری جنبش‌های اجتماعی، امروزه در دو محیط واقعی و محیط مجازی از سوی تحلیل‌گران اجتماعی، سیاسی، فرهنگی و به ویژه امنیتی مورد بررسی و تدقیق قرار می‌گیرد. جنبش‌های اجتماعی در فضای واقعی در روندی سه مرحله‌ای به سمت و سوی جنبش مقاومت پیش می‌روند، اما جنبش‌های اجتماعی در فضای مجازی که امروزه با عنوان شبکه‌های اجتماعی شناخته می‌شوند نیز در روندی سه مرحله‌ای با بسیج توده‌های کاربر، آن‌ها را به صحنه‌ی واقعی می‌کشاندند. جنبش‌های اجتماعی به منظور یکپارچه نمودن مردم و به جهت پاسخ‌گویی به نیازهای فرهنگی، سیاسی، اقتصادی و... صورت می‌پذیرند. رشد تکنولوژی ارتباطات و اطلاعات یکی از دلایل اساسی گسترش جنبش‌های اجتماعی در فضای مجازی است. تکنولوژی اطلاعات فرصت‌های فراوانی در اختیار گروه‌های اجتماعی قرار داده است. عدم شناخت آن و پی‌آمدهایش به عنوان یک معضل اجتماعی ضرورت بررسی روند تکوین جنبش‌های اجتماعی در فضای مجازی را گوشزد می‌نماید. از این جهت روند رشد و تکوین جنبش‌های اجتماعی در محیط مجازی را در نسبتش با محیط واقعی مورد بررسی قرار داده‌ایم.

**کلمات کلیدی:** شبکه‌مندی‌سازی، بسیج‌سازی، یک‌پارچه‌سازی، جنبش‌های اجتماعی، محیط واقعی و محیط مجازی.

### ۱ مقدمه

فرآیند یک‌پارچه‌سازی<sup>۱</sup>، گام مقدماتی در شکل‌گیری جنبش‌ها و حرکت‌های اجتماعی است. پس از شکل‌گیری و تحقق این گام در محیط واقعی، بسیج<sup>۲</sup> صورت می‌پذیرد. چنان‌چه در واقعیت اجتماعی جامعه با درگیری‌های داخلی و یا تحت اشغال خارجی و ... مواجه باشد، به سمت تسلیح<sup>۳</sup> پیش می‌روند. این در

<sup>۱</sup>Integration

<sup>۲</sup>Mobilization

<sup>۳</sup>Armament

حالی است که در فضای مجازی<sup>۴</sup> نیز به منظور ایجاد اندراج و پیوستگی میان اعضاء از سوی کسانی که تلاش دارند بر این فضا حاکم شوند و از فرصت‌های ایجاد شده‌ی آن استفاده نمایند، یکپارچه‌سازی صورت می‌پذیرد. این در حالی است که در گام دوم و با ایجاد شبکه‌ی مجازی که در بستر شبکه‌های مجازی صورت می‌گیرد، تلاش‌هایی برای شبیه‌سازی فضای واقعی جامعه در این محیط صورت می‌پذیرد، که می‌توان از آن با عنوان شبکه‌سازی مجازی یاد نمود، و در نهایت این شبکه‌سازی‌ها در فضای مجازی با هدف تحقق بسیج در فضای موجود، و به جهت متأثر ساختن فضا و محیط واقعی صورت می‌پذیرد.

آنچه در این میان مجهول است این است که، میان جنبش اجتماعی در فضای مجازی، با فضای واقعی چه نسبتی برقرار است؟ چه گروه‌های در محیط مجازی امکان تأثیرگذاری در محیط و فضای واقعی را دارند؟ و روش‌های تأثیرگذاری آن‌ها چگونه است؟

به نظر می‌رسد شبکه‌سازی اجتماعی در فضای مجازی با جهت تأثیر در فضای واقعی صورت می‌پذیرد. در این پژوهش تلاش می‌شود تا با هدف قرار دادن امکان و استعداد جنبش‌ها و شبکه‌های اجتماعی در فضای مجازی و واقعی به چالش‌هایی که متأثر از هر دو فضا وجود دارد، پرداخته شود.

جنبش اجتماعی هم در فضای واقعی و هم در فضای مجازی دارای روندی ۲ وجهی است، از یک سو خیزش، شکل‌گیری و گسترش آن، و از سوی دیگر فروکاهش و تقلیل‌اش به شکل اختیاری یا اجباری شناخته شود.

**پرسش اصلی.** شکل‌گیری جنبش‌های اجتماعی در چه فرآیندی صورت می‌پذیرد؟

**فرضیه.** جنبش‌های و شبکه‌های اجتماعی در فضای واقعی و مجازی از جهت روند شکل‌گیری، بسط، و گسترش با یکدیگر متفاوت هستند.

**روش‌شناسی.** روش‌شناسی در جنبش‌های اجتماعی شامل دو بخش کلی سلبی و ایجابی است. در بخش ایجابی، مسأله‌ی روند پیدایش، تکوین و گسترش جنبش‌ها و شبکه‌های اجتماعی مورد بحث و بررسی قرار می‌گیرد، و در بخش سلبی، ساز و کار خنثی‌سازی، و بی‌اثر نمودن و محو آن جنبش‌ها و شبکه‌های اجتماعی مدنظر است.

## ۱.۱ خیزش جنبش‌ها و شبکه‌های اجتماعی

خیزش جنبش‌های اجتماعی معلول شرایط و زمینه‌هایی است، که با شناخت این عوامل است که می‌توان این جنبش‌ها را درک کرد، و سپس حدود و ثغورش را تعیین نمود.

### ۱.۱.۱ زمینه‌های محیطی و عوامل بیرونی خیزش

پیدایش جنبش‌های اجتماعی در سطح جهان، معلول عوامل بیرونی و زمینه‌های محیطی متعددی است. اگر بازه‌ی زمانی عوامل و زمینه‌های پیدایش جنبش‌های اجتماعی در سطح جهان اسلام، در یک‌صد سال اخیر

<sup>4</sup>Cyber



در نظر گرفته شود، برخی از مهم‌ترین عوامل و زمینه‌های آن عبارتند از:

- (۱) دخالت قدرت‌های خارجی در امور ملت‌ها
- (۲) استبدادهای داخلی در کشورهایی که از حمایت قدرت‌های استکباری برخوردارند.
- (۳) تسلط رسانه‌ای قدرت‌های استعماری
- (۴) رشد تکنولوژی‌های ارتباطاتی
- (۵) گسترش تکنولوژی اطلاعات
- (۶) امکان دسترسی عمومی به فضای مجازی
- (۷) بالا رفتن سطح آگاهی عمومی و افزایش میزان سواد
- (۸) بالا رفتن میزان وابستگی‌های عمومی به اطلاعات موجود در فضای سایبر

### ۲.۱.۱ جنبش و شبکه‌های اجتماعی در محیط واقعی و محیط مجازی

جنبش‌های اجتماعی، زمینه‌های ماهوی خیزش توده‌ها در نیل به «جنبش‌های مقاومت» محسوب می‌شوند، و البته هر جنبش اجتماعی را نمی‌توان یک جنبش مقاومت دانست، اما هر جنبش مقاومت، خود یک جنبش اجتماعی است. این در حالی است که بسیاری از گروه‌های اجتماعی در فضای مجازی به منظور مقاومت در برابر دستگاه یا نظام سیاسی صورت می‌پذیرد، و بیشتر کارکردشان اعمال فشار می‌باشد.

### ۲.۱ روش خیزش جنبش‌ها و شبکه‌های اجتماعی

خیزش جنبش‌ها و شبکه‌های اجتماعی در محیط واقعی از شرایط زندگی عادی اعضای گروه‌ها، تا وضعیت آماده‌باش عملیاتی آنها برای اجرای مأموریت، سه مرحله‌ی اساسی دارد. این سه مرحله را می‌توان روند آمایش توان انسانی جنبش‌های و شبکه‌های اجتماعی در محیط واقعی دانست:

- (۱) یک‌پارچه نمودن سلول‌های اجتماعی جنبش‌های و شبکه‌های اجتماعی، Integration.
- (۲) بسیج نمودن سلول‌های داوطلب جنبش‌های و شبکه‌های اجتماعی، Mobilization.
- (۳) مسلح نمودن سلول‌های بسیج شده جنبش‌های و شبکه‌های اجتماعی، Armament.

این در حالی است که در جنبش‌ها و شبکه‌های اجتماعی مجازی، خیزش از شرایط عادی ارتباطاتی کاربران آغاز می‌شود و تا وضعیت بسیج در فضای واقعی، سه مرحله‌ی کلی را دنبال می‌نماید. این سه مرحله را می‌توان روند آمایش توان ارتباطاتی جنبش اجتماعی در شبکه‌ی مجازی دانست.

جدول ۱: روند یک‌پارچه‌سازی جنبش‌ها و شبکه‌های اجتماعی

در محیط واقعی	در محیط مجازی
۱ واجد رهبری است.	۱ فقدان رهبری در آن مشهود است.
۲ هدف و آرمان جنبش مشخص است.	۲ هدف و آرمان جنبش مشخص نمی‌باشد.
۳ جنبش دارای ایدئولوژی مشخصی است.	۳ بیشتر خواست و اراده‌ی مشخص را نمی‌توان برای آن‌ها یافت.
۴ جنبش واجد دکترین و استراتژی است.	۴ فاقد دکترین و استراتژی هستند.
۵ انگیزه‌ی ایجاد، در انسجام جنبش، عامل اصلی است.	۵ انگیزه در آن، ارتباط برای ارتباط است.
۶ تبلیغ به شکل آشکار و عینی صورت می‌پذیرد	۶ تبلیغ در جنبش سطحی به نظر می‌رسد.

- (۱) یک‌پارچه نمودن کاربران فضای سایبر با برقراری ارتباط تا شکل‌گیری خوشه‌ها، Integration.
- (۲) شبکه‌مند نمودن سلول‌ها و بلوک‌های ایجاد شده و استمرار ارتباط میان آن‌ها، Networking.
- (۳) به صحنه‌ی واقعی آوردن شبکه‌ی یک‌پارچه شده در فضای مجازی به منظور ایجاد تحرک اجتماعی و به دست آوردن مطالباتی که جنبش اجتماعی مجازی به آن جهت شکل گرفته است Mobilization.

## ۲ روش‌شناسی خیزش

### ۱.۲ یک‌پارچه نمودن در محیط واقعی

در یک جامعه‌ی اسیر استبداد یا تحت اشغال قدرت‌های بیگانه، رخوت و یأس و ناامیدی، به سکوت و سکون و ایستایی آحاد آن جامعه انجامیده، و روزمرگی به شیوه‌ی رایج گذران دوران تبدیل می‌شود. در جوامعی که ارتباطات چهره به چهره و واقعی فاقد کیفیت بوده و چندان قابل قبول نمی‌باشد، و مردم، درگیر زندگی تکنولوژی زده‌ای هستند که ناچار نیاز تعاملی‌شان را با بهره‌گیری از فرصت شبکه‌ی مجازی مرتفع می‌نمایند. در این جامعه جنبش و شبکه‌ی اجتماعی در واقع متشکل از هزاران کاربر شبکه‌ی اینترنتی است که با وحدت نظر در خصوص مجموعه‌ای از خواست‌ها و نیازها با یکدیگر ارتباط برقرار می‌نمایند. روند یک‌پارچه‌سازی گروه‌های اجتماعی به صورت جدی در راستای ایجاد انسجام صورت می‌پذیرد. اندراج و پیوستگی اجتماعی به عنوان عامل ثبات‌بخش اجتماع مورد نظر صاحب نظران جامعه‌سازی قرار می‌گیرد. یک‌پارچه‌سازی جنبش اجتماعی در فضای مجازی با فضای واقعی دارای نسبتی مطابق جدول ۱ است. آن‌گاه که پیکره‌ی جنبش، از وجود این سلول‌های انسانی ساخت یافت و شکل گرفت، جنبش اجتماعی در فضای واقعی به مرحله‌ی «یک‌پارچه»سازی «سلول»های برانگیخته شده دست یافته است. آن‌گاه که پیکره‌ی جنبش، از وجود این سلول‌های انسانی، ساخت یافت و شکل گرفت، جنبش اجتماعی به مرحله‌ی «یکپارچه»سازی «سلول»های برانگیخته شده، دست یافته است. این مرحله را یکپارچه نمودن

یا Integration می‌نامند.

این در حالی است که روند یک‌پارچه‌سازی در فضای مجازی هنگامی صورت می‌پذیرد که ارتباط میان کاربران اینترنتی و استفاده‌کنندگان از اطلاعات برقرار شده و با تشریک مساعی و سهیم شدن در اطلاعات، ضمن تعریف مسأله‌ی مشترک و فهم مشترک خوشه‌سازی<sup>۵</sup> صورت می‌پذیرد.

## ۲.۲ بسیج نمودن در محیط واقعی

آنگاه که افرادی از متن جامعه، به عنوان سلول‌های اجتماعی، داوطلب شدند، و به صورت یکپارچه، پیکره‌ی جنبش را شکل دادند، مرحله‌ی دوم یا وضعیت «بسیج» شدن آنان آغاز می‌شود. هر فرد برخاسته و داوطلبی که رهبری فرهمند جنبش، هدف والا، ایدئولوژی و دکترین آن را پذیرفته باشد، لزوماً «بسیج» شده به حساب نمی‌آید، زیرا توان‌مندی انجام تعهدات اجتماعی و انقلابی، که سلامت جسم و تعادل ذهن و ثبات شخصیت و موارد دیگری از ویژگی‌های یک مصلح را در بر می‌گیرد، در هر فرد داوطلبی نیست؛ چه بسا یک شخص برخاسته و داوطلب حضور در جنبش، اسیر احساسات آنی، و جو زده‌ی تبلیغات جنبش مقاومت، یا تحت تأثیر شرایط استبداد و اشغال و ... به صحنه آمده است، اما از عهده‌ی انجام فعالیت‌هایی که باید انجام دهد برنمی‌آید. لذا در این مرحله باید ضمن انجام آموزش‌های مورد نیاز، مهارت، زندگی در شرایط دشوار را کسب نماید، و سپس به شکل مناسبی سازمان‌دهی گردد. عدم سازمان‌دهی اعضای جنبش موجب ناکارآمدی و از بین رفتن آن می‌شود.

روند بسیج سلول‌ها در جنبش‌ها و شبکه‌های اجتماعی در فضای واقعی به‌صورت زیر است:

۱. گزینش و عضوگیری.

۲. آموزش.

۳. سازمان‌دهی.

۱.۳. سازمان‌دهی به عنوان عضو ثابت یا سمپات (هوادار).

۲.۳. سازمان‌دهی به عنوان عضو ستادی یا صفی.

۳.۳. سازمان‌دهی موضوعی: عضو فرهنگی، عضو سیاسی، عضو عملیاتی، عضو اطلاعاتی، و ... ..

۴.۳. سازمان‌دهی در واحدهای رزمی، در سلسله مراتب، در قالب گروه‌ها، تیم‌ها، دسته‌ها، گروهان‌ها، گردان‌ها، (و حتی رده‌های بالاتر)، در قالب رشته‌های گوناگون و رشته‌های مختلف و شغل‌های متنوع.

<sup>۵</sup>هدف از خوشه‌سازی در شبکه‌های مجازی و واقعی تفکیک جنبش شبکه‌ی اجتماعی به گروه‌های مرتبطی است که بتوان آن‌ها را به صورت مجزا مورد بررسی قرار داد.

اکنون با سازمان‌دهی نیروها، مرحله‌ی «بسیج» نمودن جنبش یا Mobilization به انجام رسیده است و این نیروها، برای انجام عملیات و بر عهده گرفتن مأموریت، آماده‌اند. هر چه یک جنبش بتواند کیفیت نیروهای جذب شده را افزایش دهد و به میزان بیشتری به مسایل و معضلات اجتماعی پاسخ دهد، قدرت بسیج‌کنندگی‌اش بیشتر خواهد بود. و از سوی دیگر ماندگاری بیشتری در جامعه و جذب نیروهای خنثی و بی‌طرف اجتماعی خواهد داشت.

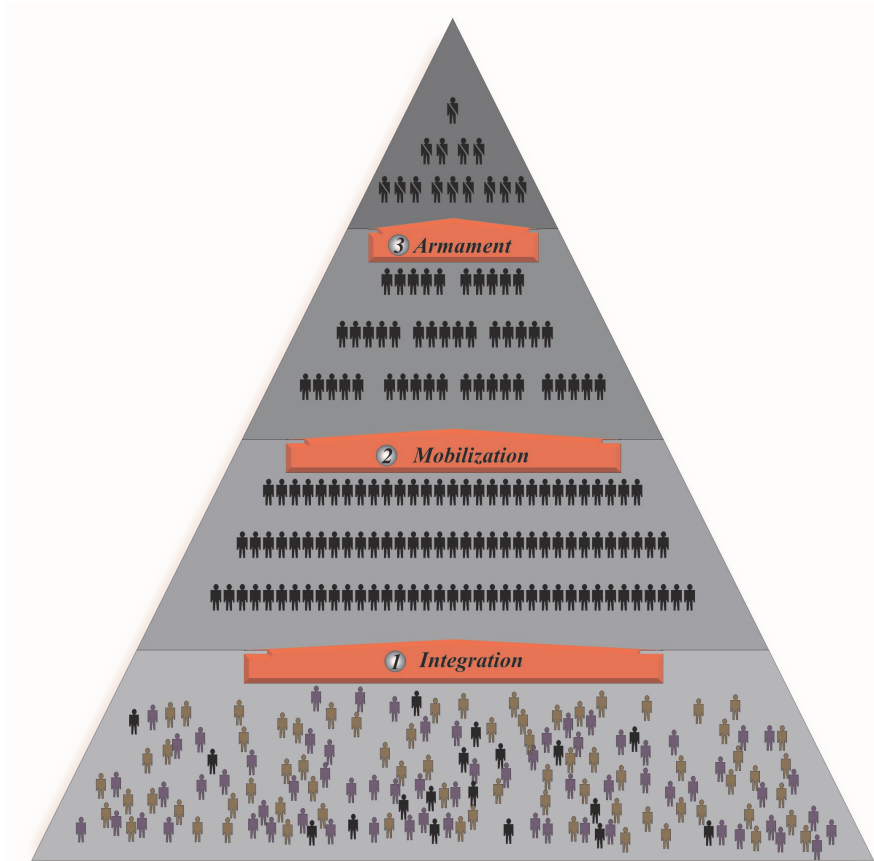
## ۳.۲ شبکه‌مند نمودن در محیط مجازی

جنبش اجتماعی در فضای مجازی، پس از این که سلول‌های اینترنتی به شکل متصل با یکدیگر یک‌پارچه گردیدند، به صورت شبکه‌ای مرتبط با یکدیگر به تبادل اطلاعات می‌پردازند. شبکه‌مند شدن کاربران به عنوان سلول‌های مجزا پس از برقرار شدن ارتباط و تبادل اطلاعات صورت می‌پذیرد. مؤلفه‌هایی که برای شبکه‌مند شدن این سلول‌ها نیاز است عبارتند از:

۱. وجود شبکه‌ی سخت
۲. شکل‌گیری شبکه‌ی نرم‌افزاری
۳. وجود زیرساخت ارتباطاتی و برقرار شدن اتصال و ارتباط
۴. ضریب نفوذ اینترنت با توجه به اعتبار این فضا کاهش یا افزایش می‌یابد.

برای شبکه‌سازی در فضای مجازی به صورت‌های زیر عمل می‌شود:

۱. سهیم شدن در اطلاعات اعضاء دیگر و شبکه فهمیم نمودن دیگر اعضاء از اطلاعات موجود، این مرحله را مرحله‌ی اشتراک در اطلاعات می‌گوییم. یعنی اعضاء شبکه مدارک‌شان را با یکدیگر تقسیم می‌نمایند.
  ۲. انتقال پیام‌های کسب شده توسط اعضاء به دیگر اعضاء از طریق به اشتراک‌گذاری آن‌ها.
- امکان دستیابی به شبکه‌ی مجازی، معلول برقرار شدن ارتباط اینترنتی، حفظ و گسترش این ارتباط می‌باشد. چنان‌چه این ارتباط قطع گردد، عملاً هیچ شبکه‌ای شکل نخواهد گرفت و یا این که شبکه ناکارآمد گردیده و نابود می‌شود. آماده بودن زیرساخت‌های فنی و تکنولوژیک در کنار وجود قابلیت‌های نرم‌افزاری به عنوان مقدمه‌ی شبکه‌مندسازی در فضا و محیط مجازی می‌باشد.
- وجود نیازهای مشترک در میان کاربران و دستیابی به درک مشترک برای شکل‌گیری شبکه امری ضروری است. زیرا امکان تفاهم و گفت‌وگو در فضای موجود منوط به وجود نیازهای مشترک است و تنها تشریح و تسهیم اطلاعات نمی‌تواند قوام‌بخش یک جنبش اجتماعی باشد.



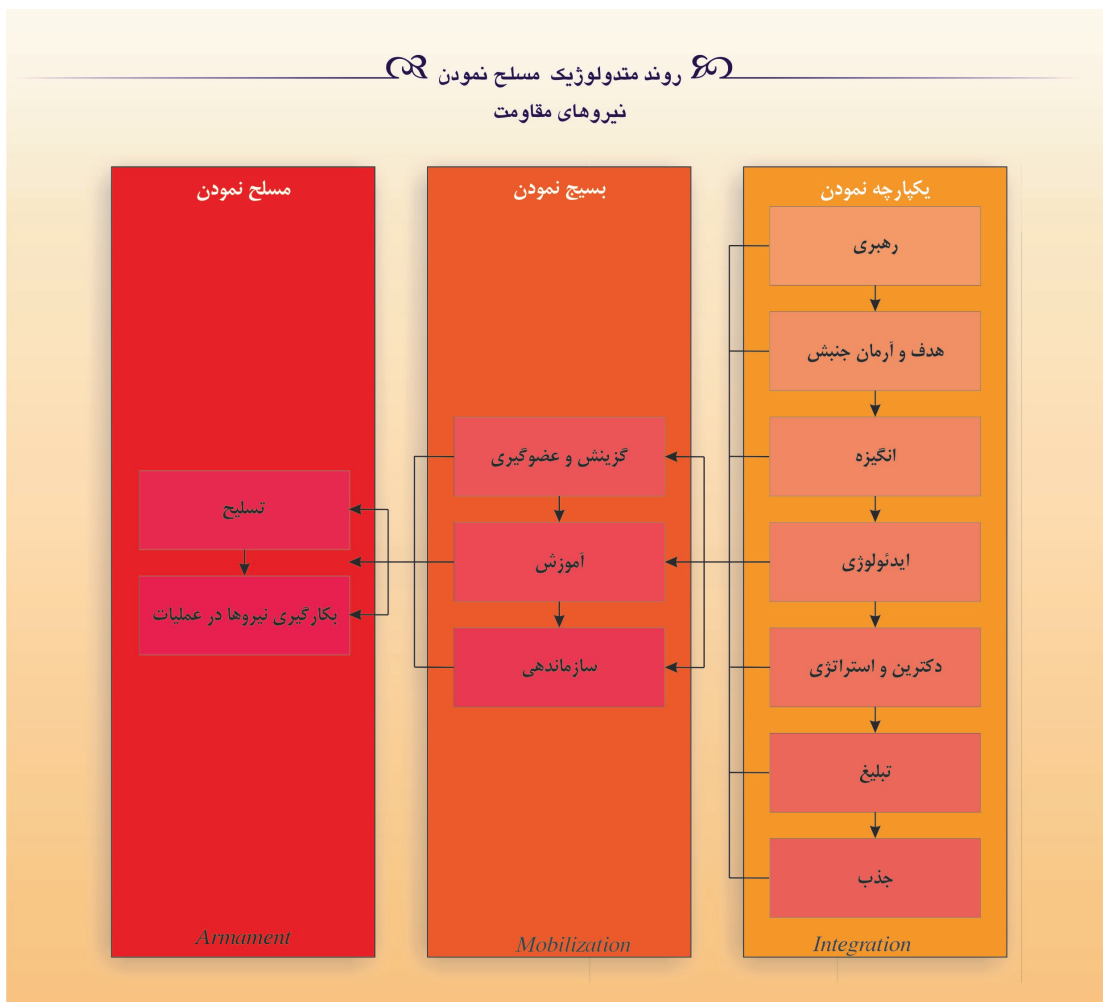
شکل ۱: مراحل سه‌گانه

## ۴.۲ مسلح نمودن جنبش اجتماعی در فضای واقعی

جنبش‌های اجتماعی هنگامی که به منظور مقابله با قدرت‌های خارجی اشغال‌گر و یا استبداد داخلی یک‌پارچه و بسیج شوند، در گام سوم و در روند تبدیل شدن به جنبش مقاومت اقدام به تسلیح اعضا خود منطبق با مأموریت و هدف‌شان می‌نمایند.

### ۱.۴.۲ تسلیح

حال که جنبش اجتماعی با سازمان‌دهی نیروهای آموزش دیده‌ی خود به جنبشی با شکل مقاومت تبدیل شده است، اعضا جنبش را برای اجرای وظایف و مأموریت‌ها، «مسلح» می‌کند. واگذاری اسلحه‌ها و تجهیزات مورد نیاز اجرای عملیات آینده، در قالب «سازمان برای رزم» جنبش مقاومت، با تکیه بر تعریف دقیق نقش‌ها در سازمان، و رعایت سلسله مراتب، صورت می‌گیرد. در این مرحله، مسلح‌سازی یا Armament محقق می‌شود.

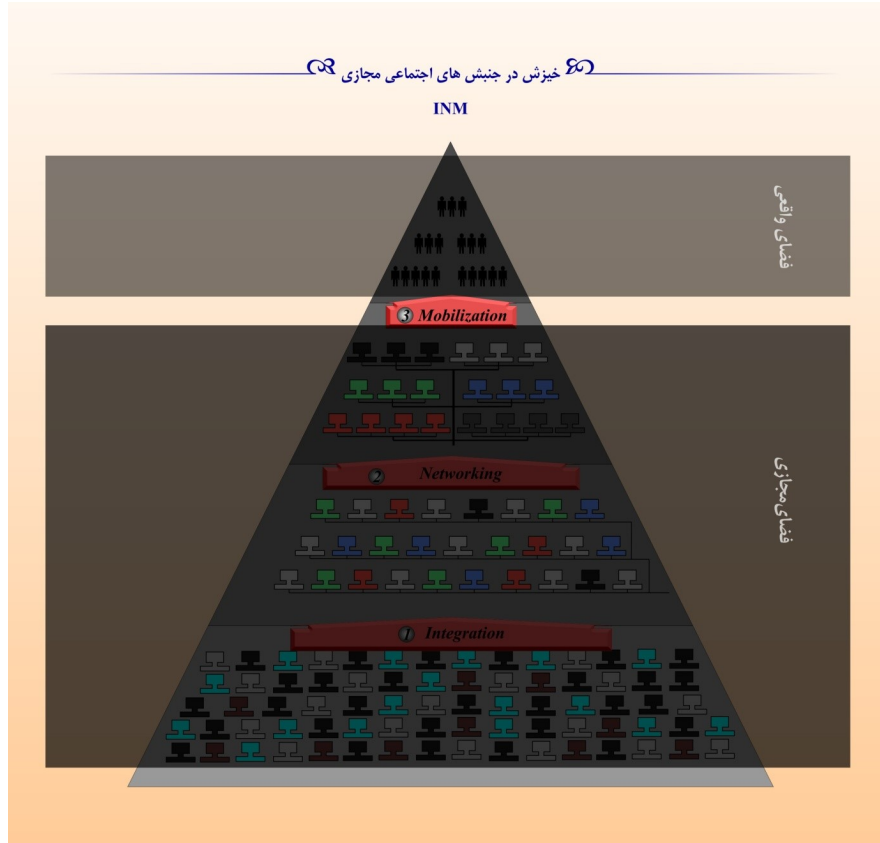


شکل ۲: روند متدولوژیک مسلح نمودن در محیط واقعی

## ۲.۴.۲ بکارگیری نیروها در عملیات

پس از سازماندهی جنبش مقاومت و مسلح‌سازی آن، اکنون جنبش‌ها و شبکه‌های اجتماعی برای انجام وظیفه و مأموریت آماده هستند. طرح عملیاتی برای اجرا آماده شده و «سازمان برای رزم» نسبت به طرح مزبور پدید می‌آید. روند خیزش جنبش مقاومت یا IMA در مورد جنبش‌های مردمی موضوعیت دارد و سازمان‌های نخبه‌گرا یا گروه‌های تروریستی، مافیایی و گانگستری از دو شیوه‌ی متفاوت دیگر، یعنی روش نخبه‌گرای مزدوری برای گروه‌های مافیایی، و روش نخبه‌گرای وفادار در گروه‌های گانگستری بهره می‌برند که از موضوع بحث این تحقیق بیرون است.





شکل ۳: خیزش جنبش اجتماعی در محیط مجازی با بسیج سازی در محیط واقعی INM

## ۵.۲ بسیج نمودن جنبش اجتماعی مجازی در فضای واقعی

اکنون که جنبش اجتماعی مجازی در قالب شبکه‌ی مجازی، سازمان یافته است، به دنبال کسب موقعیت جنبش است، لذا ضمن بالا بردن بهره‌وری فضای مجازی تلاش می‌نماید تا با افزایش ضریب نفوذ اینترنت، درجه‌ی هم‌گرایی<sup>۶</sup> در محیط مجازی را افزایش داده و از این طریق واگرایی اجتماعی در فضای واقعی را کاهش دهد. پس در این مرحله، همت جنبش اجتماعی در وارد نمودن اعضا به صحنه‌ی واقعی است. هر چه جنبش اجتماعی مجازی در صحنه‌ی واقعی حضور پررنگ‌تری داشته باشد، میزان گستردگی و عمق آن افزایش خواهد یافت. و این که افزایش ضریب نفوذ اینترنت و میزان وابستگی کاربران به اطلاعات و پیام‌هایی است که از سوی عوامل محرک و با بهره‌گیری از محیط مجازی صورت می‌پذیرد.

ورود جنبش اجتماعی مجازی به فضای واقعی بسته به میزان اقناعی که در کاربران به وجود می‌آورد، ممکن می‌شود. تلاش دستگاه‌های امنیتی بیگانه‌ای که کشورهای آن‌ها از رابطه‌ی سیاسی با جمهوری اسلامی

<sup>۶</sup> درجه‌ی هم‌گرایی In degree میزان ارتباط هر کاربر در محیط مجازی و یا سلول‌های اجتماعی در محیط واقعی می‌باشد. درجه‌ی هم‌گرایی شمارش تعداد ارتباطات و کیفیت آن سنجیده می‌شود.



شکل ۴: روند متدولوژیک بسیج‌سازی جنبش اجتماعی مجازی در محیط واقعی

برخوردار نیستند، مهندسی پیام‌هایی است که در فضای مجازی منتشر می‌شود. یعنی آن‌ها تلاش دارند تا با دادن پیام‌هایی که بر شایعه استوار است و با غفلت مسئولین از مکان پاسخ‌گویی به خواست مردم، آن‌ها را به صحنه‌ی واقعی، بکشانند، و بر این اساس به نظام سیاسی به صورت جدی اعمال فشار نمایند. مسأله‌ی اصلی در شیفت کردن جنبش اجتماعی از شبکه‌ی اجتماعی در محیط مجازی به محیط واقعی امنیتی شدن آن‌ها می‌باشد. مسأله‌ای که پس از انتخابات دهمین دوره‌ی ریاست جمهوری در کشور جمهوری اسلامی ایران و شکل‌گیری جنبش اشغال وال استریت در آمریکا که به جنبش ضدکاپیتالیستی در بیش از ۱۱۴ کشور در مدت کوتاهی گسترش یافت، به عنوان موردهای مطالعاتی در این روند می‌باشند.

### ۳ نتیجه‌گیری و پیشنهاد

روند جنبش‌های اجتماعی با توجه به محیطی که در بستر آن شکل می‌گیرند، رقم می‌خورد. در فضای واقعی با توجه به این که افراد به صورت چهره به چهره با یکدیگر ارتباط برقرار می‌کنند، و مبتنی بر نیازهای واقعی‌شان در کنار یکدیگر قرار می‌گیرند، انسجام و یکپارچگی‌شان عینی و ملموس‌تر می‌باشد. در حالی که روند جنبش‌های اجتماعی در محیط مجازی مبتنی بر برقراری ارتباط ایجاد شده توسط شبکه‌ی اینترنتی، و حفظ و تداوم این ارتباط است.

شبکه‌ی اجتماعی در فضای واقعی برای مواجهه‌ای که با معضلات و مفاسد اجتماعی و یا در برابر قدرت‌های خارجی اشغال‌گر و یا قدرت‌های داخلی مستبد، به شبکه‌ی مقاومت تبدیل می‌شود. اما شبکه‌ی اجتماعی در فضای مجازی بیشتر در جوامعی که شبکه‌ی ارتباطاتی اطلاعاتی مجازی از کیفیت برخوردار باشد، و از حیث وجود زیرساخت‌های شبکه‌ای امکان برقراری ارتباط مهیا باشد ممکن و مقدور خواهد بود. یعنی در جوامعی که از رفاه نسبی برخوردارند و ارتباطات رو در رو در آن‌ها به سبب رشد تکنولوژی کاهش یافته است صورت می‌پذیرد.

آن‌چه در نهایت جنبش اجتماعی در محیط واقعی و یا مجازی دنبال می‌نمایند، حضور مردم در صحنه‌ی واقعی برای به دست آوردن خواست‌های عمومی شده‌ای می‌باشد که جنبش اجتماعی به واسطه‌ی آن شکل گرفته است. مواجهه‌ی حکومت‌های مرکزی با شبکه‌های اجتماعی مجازی و واقعی با یکدیگر متفاوت است. هر چند شبکه‌های اجتماعی در دو سطح مطالبات عمومی از یک سو و مطالبات گروهی را از سوی دیگر دنبال می‌نمایند، اما بسته به این که به چه میزان می‌توانند خواست‌های عمومی را پوشش دهند، امکان فراگیری بیشتری خواهند داشت.

شیوه‌ها و روش‌های مهار و کنترل نیز در دو حوزه متفاوت است، تا جایی که جنبش‌های اجتماعی واقعی که در روند تکوین‌شان به جنبش مقاومت مسلحانه تبدیل شده‌اند به روش غیرمسلح‌سازی، بسیج‌زدایی و بازیک‌پارچه‌سازی در فرآیندی سه مرحله‌ای و با مهندسی معکوس صورت می‌پذیرد. اساسی‌ترین بخش در این روند شامل غیرمسلح‌سازی اعضاء جنبش، و متلاشی کردن وضعیت بسیج‌شدگی و بازگرداندن به زندگی عادی است. از سوی دیگر جنبش‌های اجتماعی مجازی که در روند تکوین‌شان موفق به وارد نمودن مردم در صحنه‌ی عمومی شده باشند، در فرآیندی سه مرحله‌ای که شامل کاهش ضریب نفوذ اینترنت با شفاف‌سازی مطالبات و از صحنه خارج نمودن مردم سپس با قطع شبکه‌ی ارتباطی و کنترل آن می‌توان نسبت به کنترل و حذف شبکه‌ی اجتماعی مجازی واقعی شده اقدام نمود. لذا به صورت مختصر پیشنهاد می‌شود که:

۱. در حوزه‌ی سیاسی؛ می‌توان با درک مطالبات عمومی از فراگیر شدن اعتراضات مختل‌کننده‌ی جنبش‌های اجتماعی جلوگیری کرد. در این راستا شفافیت در بخش‌های حاکمیتی می‌تواند مفید فایده باشد، که در کنار آن می‌بایست به مطالبات به حق آن‌ها پاسخ مناسب داده شود.
۲. در حوزه‌ی اجتماعی؛ باید از انسجام اجتماعی که در اثر تهدیدات و فشارهای خارجی صورت می‌پذیرد، در راستای هم‌کاری‌های عمومی جهت بالا بردن کیفیت زندگی و افزایش روحیه‌ی مسئولیت‌پذیری

عمومی استفاده کرد.

۳. در حوزه‌ی تکنولوژیک؛ فضای مجازی دارای دو وجه فرصت و تهدید می‌باشد. لذا می‌بایست به شکل مناسب در شرایط مواجهه‌ی با شبکه‌های مجازی که از سوی قدرت‌های خارجی تجهیز می‌شوند، عمل گردد، تا نظام اجتماعی و سیاسی با مشکلات عدیده‌ای مواجه نگردد. لذا کنترل و در اختیار داشتن شبکه‌ی مجازی و اینترنت ضرورتی غیرقابل انکار است.

۴. در حوزه‌ی امنیت؛ ادراک و ارزیابی‌های درست دستگاه‌های امنیتی و مسئولین از شبکه‌های اجتماعی و روند رشد آن‌ها در محیط واقعی و مجازی ضروری است، زیرا عدم شناخت مناسب و درک درست جنبش‌های اجتماعی ناشناخته موجب غافل‌گیری امنیتی خواهد شد این مسأله در رخدادهایی که شهریور و مهر ۱۴۰۱ در کشور صورت گرفت، به خوبی مشهود بود.

## مراجع

- [۱] بشیریه، حسین. انقلاب و بسیج اجتماعی، تهران، انتشارات دانشگاه تهران، ۱۳۷۲.
- [۲] بکویت، چارلی، ناکس، دونالد. نیروی دلتا، ترجمه‌ی رضا فاضل زرنندی، تهران، انتشارات امیر کبیر، چاپ چهارم، ۱۳۷۸.
- [۳] پرحلم، مجید. جنگ فرهنگی، اتحادیه انجمن‌های اسلامی دانش‌آموزی، ۱۳۸۵.
- [۴] تورس، پابلو. ضد شورش و جنگ انقلابی، انتشارات منصور.
- [۵] انسون، چالمرز. تحول انقلابی، ترجمه‌ی حمید الیاسی، تهران، انتشارات امیرکبیر، ۱۳۶۴.
- [۶] چگینی، عباس. ابعاد پروژه‌ی DDR در جهان اسلام، اندیشکده یقین، ۱۳۸۷.
- [7] Berdal. Mast. R, Disarmament and Demobilization after civil wars, published IISS, NewYork, 1996.
- [8] The Covenant Of The Islamic Resistance Movement (Hamas). Media Analysis Center, Oct. 1988.
- [9] Eric V. Larson, Bogdan Savych, American Public Support for U.S. Military Operations, Published by the RAND Corporation, 2005.

## فضای سایبری به مثابه ذهن - جهان

احمد امامی<sup>۱</sup>

دکتری فلسفه اسلامی از انجمن حکمت و فلسفه ایران و دانش آموخته‌ی دانشگاه مفید  
ahmademami@yahoo.com

### چکیده

ایده‌ی محوری نوشته‌ی پیش رو، بیان «چیستی فضای سایبری» است. نویسنده، نخست نگاهی به ریشه‌های تاریخی و چگونگی طرح اصطلاح «سایبری» می‌اندازد و سپس به بیان چیستی «امر سایبری» و انواع آن می‌پردازد و از آن میان، چیستی «فضای سایبری» و تعاریف و نظریات مطرح شده راجع به آن را با اشاره به تاریخ طرح این اصطلاح، برجسته می‌سازد. در ادامه با بیان این نکته که فضای سایبر اساساً هویتی کارکردی است، سه کارکرد اصلی آن را اطلاعات، ارتباطات، و کنترل یا تمشیت امور دانسته، تعریفی کارکردگرایانه از آن به دست می‌دهد. سپس پیشنهاد تفکیک دو مفهوم «فضای سایبر» و «فضای سایبری» را طرح می‌کند و وجه آن را بیان می‌دارد؛ و در نهایت، با توجه دادن به بُعد شناختی ایجاد شده از فضای سایبر که از لوازم وجودی آن است، تعریف یا نظریه «فضای سایبری به مثابه جهانی بین‌الذهانی یا ذهن-جهان» را طرح و شرح می‌نماید و آن را به عنوان مبنای مفهومی مطالعات فلسفی، و علوم انسانی راجع به فضای سایبر پیشنهاد می‌دهد.

**کلمات کلیدی:** سایبرنتیک، فضای سایبر، ذهن-جهان سایبری، فلسفه‌ی فضای سایبر.

### ۱ مقدمه

شناخت چیستی «فضای سایبر»، تفکیک لایه‌های مختلف، و تحلیل مفاهیم مرتبط با آن، و به دست دادن تعریفی دقیق از هر کدام، گام نخست و پایه‌ی نظری برای هرگونه مطالعات دیگر راجع به این جهان نوپدید و لوازم و توابع مختلف آن است. در این زمینه، پژوهش‌ها و آثار اندکی به زبان فارسی خلق و نشر شده است. در حالی که زندگی شخصی و اجتماعی، ابعاد فرهنگی تمدنی و سیاسی، و تقدیر حال و آینده‌ی ما و مردم ما نوردگاه تندبادهای شدید و دگرگون‌ساز این پدیده‌ی بی‌نظیر است، ناگزیر از شناخت همه‌جانبه و دقیق این موضوع، برای تعریف موضع مناسب و بایسته در برابر آن هستیم، و جبران خلأ معرفتی و فقدان نظریه‌پردازی در این زمینه، ضرورتی اجتناب‌ناپذیر و فوری است. نوشته‌ی حاضر تلاشی است در همین راه.

## ۲ اصطلاح‌شناسی فضای سایبر

معنای لغوی «فضا» روشن است؛ اما اینکه مقصود از آن در تعبیر «فضای سایبر» چیست، در گرو فهم دقیق مفهوم «سایبر» و معنای اراده شده از آن است که در جای خود به آن خواهیم پرداخت.

### ۱.۲ سایبرنتیک و سایبر

«سایبر»<sup>۱</sup> برگرفته از «سایبرنتیکس»<sup>۲</sup> است.<sup>۳</sup> این اصطلاح نخستین بار در سال ۱۹۴۸ توسط ریاضیدانی به نام نوربرت وینر<sup>۴</sup> در کتابی با عنوان سایبرنتیکس<sup>۵</sup> به کار گرفته شد. این کتاب، سایبرنتیکس را علم «کنترل» و «ارتباط» انسان-ماشین (کامپیوترها) می‌داند. وینر در این کتاب تاریخ‌ساز و الهام‌بخش، نخستین بار اصطلاح سایبرنتیک را که در اصل یونانی<sup>۶</sup> خود، دلالت بر معنای سکانداری، راهبری، هدایت، راندن، مدیریت و اداره، و فرمان یا دستور دارد، و روح معنای آن «اعمال کنترل» است، درباره‌ی دستگاه‌های خودتنظیم‌شونده<sup>۷</sup> و به‌عنوان وصف «ماشین‌های محاسباتی»<sup>۸</sup> به کار برد. این ماشین‌ها امتداد ایده‌ی چارلز بابیج<sup>۹</sup> برای ساخت ماشین‌های محاسبه‌گر برنامه‌پذیر، و ماشین آلن تورینگ<sup>۱۰</sup> است که دو ویژگی اصلی آنها، برخورداری از چرخه‌ی ورودی-پردازش-خروجی، و خودکار یا اتوماتیک بودن آنهاست، و کارکرد اصلی‌شان: محاسبات و پردازش است-شبه آنچه که ذهن انسان انجام می‌دهد- که امروزه شکل پیشرفته‌ی آن را در رایانه‌ها و هسته‌های پردازشگر می‌بینیم.

بنابراین، اصطلاح «سایبرنتیک» در اصل، درباره‌ی ماشین‌های محاسباتی اتوماتیک و رایانه‌ها<sup>۱۱</sup>، و برای دلالت بر معنای مکانیزم‌های «کنترل» و مدیریت فرایندهای پردازشی، در ارتباط انسان‌ها با آن ماشین‌ها، به کار برده شده است. به عبارت دیگر، هسته‌ی مفهومی سایبرنتیک، بر مکانیزم‌های کنترل انسانی بر کامپیوترها اشاره می‌کند<sup>۱۲</sup> (چنان که آن را در فارسی به علم فرمانش، یا فرمان‌شناسی نیز ترجمه کرده‌اند که می‌تواند معادل خوبی باشد) و «سایبرنتیکس» معادل دانش «شناخت روابط انسان-ماشین و نحوه‌ی کنترل انسان بر ماشین‌های محاسبه‌گر» است.

<sup>1</sup> Cyber

<sup>2</sup> Cybernetics

<sup>3</sup> Longman Dictionary of Contemporary English/Cyber

<sup>4</sup> Norbert Wiener

<sup>5</sup> Cybernetics: Or Control and Communication in the Animal and the Machine

<sup>6</sup> κυβερνάω

<sup>7</sup> Self-regulating mechanisms

<sup>8</sup> Computing machines

<sup>9</sup> Charles Babbage (1791-1871)

<sup>10</sup> Alan Mathison Turing (1912-1954)

<sup>۱۱</sup> در حقیقت، ماشین‌های محاسباتی یا حسابگر، نام نخستین کامپیوتر به معنای امروزی بود؛ چون در آن زمان، کلمه‌ی Computer به افرادی که برای انجام محاسبات عادی استخدام می‌شدند، اطلاق می‌گشت (Random House Webster's Unabridged Dictionary/Computer).

<sup>۱۲</sup> هر چند بعدها این اصطلاح از باب توسعه‌ی مفهوم، درباره‌ی کنترل اجتماعی یا سیاسی و به‌مثابه ابزار حکمرانی نیز به کار رفت، لکن مفهوم «کنترل» قصد شده از اصطلاح سایبرنتیک به‌لحاظ ریشه‌ی کاربرد تاریخی خود، مفهومی فنی و تکنولوژیکال است.



بعدها که با گسترش فناوری‌های دیجیتالی، همه‌ی این ماشین‌ها به صورت دیجیتالی تحقق<sup>۱۳</sup> و توسعه یافتند، «سایبرنتیک» در مقام وصف دستگاه‌های محاسبه‌گر «دیجیتال» غلبه‌ی کاربرد یافت، و سپس این وصف، بر خود موصوف یعنی دستگاه‌های محاسبه‌گر دیجیتالی (کامپیوترها) اطلاق شد، و تعبیر «سایبری» در کاربرد، با «دیجیتالی بودن» ملازم شد و پسوند‌های «سایبری»<sup>۱۴</sup> و «دیجیتالی» هم‌ارز گشت و بر مصادیق یکسان اطلاق شد؛ گرچه به لحاظ مفهومی میان آنها تفاوت وجود دارد. در حقیقت، دیجیتالی بودن در معنا، به نحوی خاص تحقق و شیوه‌ی کار این دستگاه‌ها اشاره می‌کند و اصطلاحی فنی‌تر و فناوریک است؛ و سایبری بودن، به قابلیت مدیریت فرایندهای پردازشی ماشین‌های پردازشگر کنترل‌پذیر (= سیستم‌های سایبرنتیکی) توسط انسان دلالت می‌کند، و مفهومی عام‌تر و انتزاعی‌تر است.<sup>۱۵</sup>

بدین‌سان، پسوند «سایبری» به وجوه مختلف، وصف ساختارها، سخت‌افزارها، اشیاء، انسان‌ها، پدیده‌های عینی یا مفهومی انتزاعی قرار گرفت که به نوعی، ارتباطی با رایانه‌ها یا همان سیستم‌های سایبرنتیکی داشتند. به تدریج و با اتصال کامپیوترها به یکدیگر، و به وجود آمدن شبکه‌های دیجیتالی، و به ویژه با فراگیر شدن اینترنت، این پسوند، بیشتر به شبکه‌ای از رایانه‌ها و به طور مشخص، اینترنت ارجاع می‌یافت؛ و بدین گونه، اصطلاحاتی ترکیبی چون شهروند سایبری<sup>۱۶</sup>، تجارت سایبری<sup>۱۷</sup>، پول سایبری<sup>۱۸</sup>، امنیت سایبری<sup>۱۹</sup> پدید آمد؛ تا حدی که هر امر مربوط به کامپیوتر و خصوصاً اینترنت، یا مبتنی بر آن، با عنوان «سایبری» وصف شد و اصطلاح «سایبری» تقریباً معادل «اینترنتی» شد.<sup>۲۰</sup>

بنابر این اصطلاح، امر سایبری چیزی است که بر بستر شبکه‌های دیجیتال تحقق می‌یابد، و به مثابه صورت برای ماشین‌های دیجیتال - به عنوان ماده‌ی آنها - فرض می‌گردد. برخی امور هم گرچه بر بستر سیستم‌های سایبرنتیکی تحقق نمی‌یابند، به نوعی نسبتی با آن دارند، و از همین روی منتسب به آن می‌شوند، مانند سبک زندگی سایبری یا دیجیتالی<sup>۲۱</sup> اخلاق سایبری<sup>۲۲</sup>، فرهنگ سایبری<sup>۲۳</sup> و حقوق سایبری<sup>۲۴</sup>.

<sup>۱۳</sup> نمونه‌هایی از ماشین‌های محاسباتی مکانیکی قبلاً ایجاد شده بود که تلاش برای ساخت ماشین چارلز بابیج، از جمله‌ی آنها بود.

<sup>۱۴</sup> در انگلیسی به صورت پیشنهاد Cyber

<sup>۱۵</sup> علت برجسته شدن مفهوم مرکزی «کنترل» در رابطه با دستگاه‌های محاسباتی یا کامپیوترها نیز، ویژگی خاص و تفاوت آنها با ماشین‌های غیر محاسباتی، یعنی پذیرش حالات چندوجهی، و امکان اتوماتیزه شدن و برنامه‌پذیری آنهاست که طبعاً نحوه‌ی کنترل و مدیریت آنها را از دستگاه‌های تک‌وجهی و غیر محاسباتی، متمایز و بسیار پیچیده‌تر می‌سازد.

<sup>۱۶</sup> Cybercitizen

<sup>۱۷</sup> Cyber Business

<sup>۱۸</sup> CyberCash

<sup>۱۹</sup> Cyber Security

<sup>۲۰</sup> Vanderbilt University, "Postmodernism and the Culture of Cyberspace" Archived 2007-01-07 at the Wayback Machine, Fall 1996 course syllabus (<https://www.vanderbilt.edu/AnS/english/Clayton/sch295.htm>).

<sup>۲۱</sup> Digital Lifestyle

<sup>۲۲</sup> Cyber Ethics

<sup>۲۳</sup> Cyber Culture

<sup>۲۴</sup> Cyber Rights

## ۲.۲ فضای سایبر

از این میان، اصطلاح «فضای سایبر»<sup>۲۵</sup> نیز نخستین بار در سال ۱۹۸۲ توسط ویلیام گیبسون، نویسنده داستان علمی تخیلی، و با الهام از مفهوم سایبرنتیکس وینر در مجموعه‌ی داستان کوتاهش با عنوان نابودی کروم<sup>۲۶</sup> به کار رفت و دو سال بعد در کتاب نورومنس<sup>۲۷</sup> توسعه داده شد. کتاب اخیر، داستان هکری است که جهت به دست آوردن اطلاعات هویتی فردی، اجیر می‌شود، و در این راه با افراد، ابزارها و فضاهایی غیر واقعی، و شخصیت‌هایی که هویت آنها ربات یا نیمه‌ربات است درگیر می‌شود، و این ارتباطات، فضایی را به وجود می‌آورد که وی آن را **فضای سایبر** یا ماتریکس<sup>۲۸</sup> می‌نامد. فضایی که در آن، انسان‌ها و ماشین‌ها با خطوط و امواج نامرئی و ارتباطات غیر فیزیکی با هم پیوند می‌یابند و در یک جهان وهمی برساخته از واقعیت‌های مجازی قرار می‌گیرند که درون آن، مجموعه‌ای از رخدادها، نسبت‌ها و روابط میان انسان‌ها و هوش‌های مصنوعی و ماشین‌ها برقرار می‌گردد که قواعد و ویژگی‌های خاصی بر آنها حاکم است.

مقصود نویسنده‌ی این داستان علمی تخیلی آن بود که در آینده، در اثر گسترش ابزارهای ارتباطاتی دیجیتال، موقعیت، امکان، و فضایی - به موازات جهان زندگی واقعی و روزمره - پدید خواهد آمد که انسان از طریق آن خواهد توانست از طریق دستورات از راه دور و کنترل‌هایی که بر ماشین‌ها اعمال خواهد کرد، بسیاری از امور خود را تمثیت کند بی‌آنکه نیازی به حضور فیزیکی باشد، نظیر آنچه که امروز از طریق شبکه‌های اینترنتی انجام می‌گیرد؛ و از طریق برقراری رابطه و نسبت با واقعیت‌های مجازی اعم از اشخاص، محیط‌ها، هویت‌ها، اشیاء و دیگر موجودیت‌ها و ویژگی‌های آنها جهانی خاص ساخته خواهد شد. این جهان، ویژگی‌ها و قواعد متفاوتی از جهان واقعی که می‌شناسیم خواهد داشت، تا جایی که شاید انسان بتواند حیاتی دیگر، و متفاوت در آن جهان داشته باشد. وی این فضا را به گونه‌ای ترسیم می‌کند که بر اساس آن، حتی هویت انسان‌ها از جهان واقعی قابل انتقال به فضای سایبر است و امکان ادامه‌ی حیات در آن فضا، پس از مرگ بدن مادی و بازسازی هویت او در ماتریکس یا فضای سایبر وجود دارد و اساساً کاراکتر محور داستان، رومنس، هم خود موجودی سایبری و هوشی مصنوعی است که می‌تواند کپی هویت واقعی افراد را برداشته، پس از خروج آنها از جسد، در این فضای وهمی و خیالی بازآفرینی کرده، حیاتی متفاوت به آن ببخشد، تا جایی که هکر داستان، می‌فهمد یکی از افرادی که مدت‌ها با او سروکار داشته، در حقیقت مرده بوده، و فقط در فضای موهوم سایبر حضور و حیات داشته است.

این فضای خیالی چند سال بعد با غلظتی بیشتر در فیلم سینمایی ماتریکس<sup>۲۹</sup> تصویرسازی و درباره‌ی وجه تخیلی آن داستان‌پردازی بیشتری شد. در بخشی از این فیلم، نویسندگان، ماتریکس را فضای درون یک برنامه‌ی کامپیوتری، و جهان رؤیاگون ساخته شده توسط کامپیوتر معرفی می‌کنند. در عین حال، تردد میان ماتریکس و جهان واقعی (که البته گاهی واقعی بودن آن به جای ماتریکس، موضوع پرسش و تشکیک

<sup>25</sup>Cyberspace

<sup>26</sup>Burning Chrome (Gibson, William (1982))

<sup>27</sup>Neuromancer (Gibson, William (1984))

<sup>28</sup>Matrix

<sup>29</sup>Wachowski, Lana and Wachowski, Lilly (Directors) (1999). The Matrix [Film]. Warner Bros and Village Roadshow Pictures.

می شود) از طریق کانال‌های زیرساختی سخت‌افزاری، نظیر سیم تلفن و با عبور از دنیایی از اطلاعات صفر و یک صورت می‌گیرد.

### ۳ فضای سایبر به مثابه محیطی دیجیتال

فارغ از این تصور وهمی درباره‌ی فضای سایبر، آنچه در واقعیت رخ داد، این بود که با گسترش ابعاد گوناگون فناوری‌های دیجیتال - سخت‌افزاری و نرم‌افزاری - و ایجاد شبکه‌های ارتباطات و انتقال اطلاعات، مجموعه‌ای از ارتباطات میان انسان‌ها و ماشین‌ها بر بستر شبکه‌های به هم پیوسته‌ای از رایانه‌ها شکل گرفت؛ جهانی صورت یافته از الگوریتم‌ها، بر بنیاد سخت‌افزارهای دیجیتال و الکترونیکی، حاوی و حامل اطلاعات و داده‌های متکثر که میان انسان‌ها و ماشین‌ها ساخته، پرداخته، داده و گرفته یا حذف می‌شد. فعلیت و صورتی از عالم که از پیوندهای انسان‌ها و رایانه‌ها، بر بسترهای طیف گسترده‌ای از سخت‌افزارها و با وساطت الگوریتم‌ها و قواعد سایبرنتیکی تحقق یافته بود.

با توجه به اینکه فعالیت‌ها، عملیات‌ها، ارتباطات و انتقال اطلاعاتی که گفته شد، وابستگی تامی بر بستر سخت‌افزاری و زیرساختی شبکه‌های کامپیوتری داشت، در همه‌ی تعریف‌هایی که از فضای سایبر صورت می‌گرفت بُعد سخت‌افزاری و الکترونیکی آن به‌عنوان مؤلفه‌ی اصلی یا حتی تنها مؤلفه‌ی آن در نظر گرفته می‌شد. در اوایل قرن حاضر، فضای سایبر به محیطی الکترونیکی تعریف شد که در آن، اطلاعات گوناگون ایجاد، ارسال، دریافت، ذخیره، پردازش و حذف می‌شوند. این تعریف که در آن، عنصر «سخت‌افزارها» و بُعد الکترونیکی یا دیجیتال داشتند، و نیز «اطلاعات» که بر مجرای آن سخت‌افزارها منتقل و پردازش و مورد استفاده قرار می‌گیرند، برجسته است، و اساساً فضای سایبر را محیطی الکترونیکی معرفی می‌کند، از جمله توسط کارشناسان امنیت سایبری آمریکایی - روسی به‌دست داده شد.<sup>۳۰</sup>

این تعریف با معنای لفظی سایبرنتیک، مطابقت داشت. همچنین با کارکردهای خاصی مانند نگاه امنیتی، و زاویه‌ی نگاه فنی - مهندسی به موضوع (خصوصاً بررسی‌های سخت‌افزار محور و عموماً در علوم کامپیوتر) مناسب و تناسب داشت؛ و امروزه هم به‌عنوان یکی از تعاریف پذیرفته شده و رایج در این عرصه‌ها، به کار گرفته می‌شود. لکن برخی مؤلفه‌های مهم و مؤثر مرتبط با آن را نادیده می‌گیرد یا آنها را جزو مؤلفه‌های اصلی فضای سایبر به حساب نمی‌آورد. بنابراین، حداقل برای مقاصد غیرفنی، و خصوصاً بررسی‌های علوم انسانی تعریفی جامع و کافی نبود (چنان‌که همان‌طور که در ادامه مشخص خواهد شد، مانع هم نبود) به‌همین خاطر، تعریف‌های دیگری حاوی سایر عناصر ذاتی فضای سایبر، به دست داده شد.

<sup>30</sup>“Russia-U.S. Bilateral On Cybersecurity,” April 2011, p17

## ۴ فضای سایبر به مثابه امری چند لایه

به عنوان یکی از کامل ترین تحلیل ها، دیوید کلارک<sup>۳۱</sup> و نازلی شوکری<sup>۳۲</sup> در مقاله ای چارچوب فضای سایبر را در چهار لایه ی کلی تحلیل کردند:

۱. **لایه ی فیزیکی** که بر سازه های زیر ساخت و بنیان اینترنت است و لایه ی منطقی را پشتیبانی می کند؛ از کابل های فیبر نوری تا دکل های مخابراتی و کامپیوترهای شخصی و سرورها.

۲. **لایه ی منطقی** که بر بنیادهای الکترونیکی و دیجیتالی تحقق می یابد، و متشکل از ساختارهای نحوی است و ماهیت پلتفرمی فضای سایبر را پشتیبانی می کند؛ شامل نظام های اینترنتی، شبکه ی جهانی وب، مرورگرها، نظام نام دهی دامنه یا DNS، وبسایتها و نرم افزارهای که امکان تفاهم و ترابط با سخت افزار را میسر می سازد و نیز سرویسها و اپلیکیشنها.

۳. **لایه ی اطلاعات** شامل متون رمزدهی شده، تصاویر، ویدئوها، و اطلاعات دیگر که در فضای سایبر اندوخته، پرداخته و رسانده می شوند.

۴. **لایه ی کاربران** که از طریق برقراری ارتباطات، کار بر روی اطلاعات، اعمال مدیریت، و اجرای برنامه ها، تجربه ی سایبری و خود فضای سایبر را شکل می دهند.<sup>۳۳</sup>

تحلیل فوق، قدمی رو به جلو در روشن ساختن مفهوم و تفکیک ابعاد و لایه های گوناگون شکل دهنده ی فضای سایبر بود، و کارکردهای مفیدی هم داشت و دارد، لکن اشکالاتی دارد:

- چنان که گفته شد، اطلاق فضا بر لایه ی سخت افزاری سلسله ی مزبور، فقط با نگاه های مهندسی و فنی مانند آن تناسب دارد. اشکال دیگر این تحلیل این است که در آن، یک اصطلاح (فضای سایبر) بر طیف گسترده ای از هویت، از سخت افزارها گرفته تا الگوریتمها و اطلاعات و انسانها اطلاق می شود؛ در حالی که اطلاق اصطلاح «فضا» به طور مشترک، به سخت افزار و الگوریتم و اطلاعات و انسان چندان تناسب ندارد.
- از سوی دیگر، اگر کاربران را جزئی از فضای سایبر و تشکیل دهنده ی آن بدانیم، دیگر حضور کاربران در فضای سایبر یا تعامل با آن بی معنا خواهد بود. نیز اطلاعات، در درون فضای سایبر منتقل می شود، و نمی تواند خودش بخشی از این فضا بوده باشد.
- افزون بر آن، اشکال مشترک این تحلیل، با تعریف نخست، در این نکته است که دخالت دادن شالوده های سخت افزاری و نحوه ی تحقق یک پدیده - که امکان تحقق دیگرگونه ی آن هم وجود دارد - در تعریف

<sup>31</sup>David Dana Clark

<sup>32</sup>Nazli Choucri

<sup>33</sup>Choucri, N., and Clark, D. D. (2013). Who controls cyberspace? Bulletin of the Atomic Scientists, 69(5), 21-31

چیستی آن، و معرفی آن پایه‌های سخت‌افزاری و حتی لایه‌های منطقی، به‌عنوان یکی از عناصر و مؤلفه‌های هویتی آن، منطقاً کاری نادرست است.

## ۵ فضای سایبر به‌مثابه کارکرد

بنابر ایده‌ی تحقق‌پذیری چندگانه<sup>۳۴</sup> - که فارغ از ادعاهای فلسفه‌ی ذهنی مرتبط با آن بی‌گمان درباره‌ی رایانه‌ها صادق است - فضای سایبر می‌تواند دیجیتال‌بنیاد نباشد، و در آینده (یا در یک جهان ممکن) به‌نحو دیگری تحقق یابد؛ چنان‌که نمونه‌های ساده‌ای از ماشین‌های محاسباتی، پیش‌تر به اشکال مکانیکی (یا الکترومکانیکی) و غیردیجیتال هم تحقق یافته بود و در آینده هم ممکن است همین ماشین‌ها مثلاً به‌صورت فیزیولوژیکال یعنی درون یک موجود زنده و داخل سیستم زیستی آن (یا به‌نحو دیگر) طراحی و تحقق یابد. بنابراین، الکترونیک یا دیجیتال بودن<sup>۳۵</sup> نمی‌تواند مؤلفه‌ی ذاتی فضای سایبر در نظر گرفته شود. حتی نحوه‌های حصول نرم‌افزاری کارکردهای فضای سایبر نیز دخلی در تعیین یا تغییر ماهیت آن ندارند، و فقط خود آن کارکردهاست که می‌تواند عناصر ثابت و ذاتی فضای سایبر در نظر گرفته شود. بنابراین، فضای سایبر اساساً هویتی کارکردی است، و تعریف آن نیز باید صرفاً بر اساس کارکردهایش به دست داده شود.

هویات کارکردی اساساً به چیزهایی گفته می‌شود که صرفاً بر اساس کارکردهایشان تعریف می‌شوند؛ و بنابراین با تغییر صورت‌ها و نحوه‌های تحقق، ماهیت آنها یکسان و همان باقی می‌ماند. ساعت، کاربراتور و ترموستات، نمونه‌هایی از این نوع هویات‌اند که هر چند شیوه‌های ساخت و حتی مکانیزم‌های عمل آنها در گذر زمان به‌شدت تغییر و تنوع یافته‌اند، ماهیاتشان همسان باقی مانده است، چون کارکردی که از آنها انتظار می‌رود، همچنان همان است. امروز کسی ساعت را به شیشه و شن، یا تیغه‌ای که برابر آفتاب نهاده می‌شود، یا حتی چرخ‌دنده و عقربه تعریف نمی‌کند، چون نرم‌افزارهای کوچکی که درون سیستم‌های عامل برای نشان دادن زمان نصب می‌شوند نیز به همان اندازه، مصداق مفهوم «ساعت» هستند. این به‌معنای آن است که ساعت بودن، اساساً یک کارکرد است، و مفهوم ساعت، مفهومی کارکردی است و به‌نحوه‌ی تحقق یا سخت‌افزار خاصی مشروط نیست.

### ۱.۵ کارکردهای فضای سایبر

با گسترش کاربرد اینترنت در زندگی روزمره، و لوازم گوناگون آن از جمله واسطه‌های انتقال سریع و گسترده‌ی اطلاعات، و ابزارهای ارتباطاتی، و خصوصاً شبکه‌های اجتماعی، و دیگر کارکردهای اینترنتی، مفهوم «سایبر» و به‌ویژه مفهوم «فضای سایبر» نیز عملاً بر مهم‌ترین کارکردهای ابزارهای سایبری، یعنی تولید و انتقال گسترده‌ی اطلاعات، و تسهیل و تسریع ارتباطات و اعمال برخی دستورها و تمشیت امور<sup>۳۶</sup> در شبکه‌های

Multiple Realization؛ این ایده را نخستین بار، هیلاری پاتنم در نقد نظریه‌ی این‌همانی نوعی در فلسفه‌ی ذهن مطرح کرد.

کلارک در جایی دیگر، فضای سایبر را به «مجموعه‌ای از رایانه‌ها» یا دستگاه‌های پردازشی تعریف می‌کند (Clark, MIT, 2010).

هر چند با نگاه دقیق‌تر، دو کارکرد دیگر هم خود مبتنی بر تولید و انتقال اطلاعات و نتیجه‌ی آن است؛ لکن در نگاه عرفی - که معیار نام‌گذاری یا کاربرد کلمات و اصطلاحات در زبان روزمره است - این سه کارکرد جدای از هم لحاظ می‌گردند.

ارتباطی انسانی-ماشینی منصرف شد؛ و به تدریج و خصوصاً با تغییرات و تنوعی که در ساختارها و فناوری‌های سخت‌افزاری رخ داد، جنبه‌های سخت‌افزاری و مفاهیمی که بر نحوه‌ی تحقق فضای سایبر اشاره داشتند، در تعریف هویت آن کمرنگ‌تر شد و عملاً لایه‌های سخت‌افزاری و حتی نرم‌افزاری و منطقی که پایه‌ی پشتیبان انتقال اطلاعات است، خصوصاً میان عموم کاربران از نقطه‌ی توجه و اهتمام خارج شد و آنچه در تلقی عمومی، به عنوان فضای سایبر متداول گشت، فضای انتقال اطلاعات و مدیریت امور، یعنی لایه‌ی سوم از ساختار اشاره شده در تحلیل پیشین بود.<sup>۳۷</sup>

بدین سان، انجام کار و تمشیت امور (مانند خرید یا فروش اینترنتی یا پرداختن وجه یک قبض یا سفارش یک کالا یا تحویل از راه دور یا انجام یک بازی و ...) از طریق اعمال کنترل انسان بر ماشین، انتقال اطلاعات، و ایجاد ارتباطات، که کارکردهای اصلی فضای سایبر هستند<sup>۳۸</sup> را باید محورهای اصلی و اجزای تشکیل دهنده‌ی مثلث مفهومی اصطلاح سایبری دانست؛ کارکردهایی که حدوداً از بستر سخت‌افزارهای کامپیوتری ظهور کرده، و مبتنی بر امکان انتقال داده‌ها و ارتباط‌گیری سهل و فراگیر بود، لکن بقائاً وابسته به آن نیست و ممکن است همیشه و لزوماً دیجیتال و الکترونیکی و کامپیوترنیاد، نماند. بدین سان، به نظر می‌رسد که مفهوم سایبر، از منشأ اصلی آن، یعنی مکانیزم‌های کنترل ماشین‌های محاسباتی توسط انسان‌ها فاصله گرفته، به سوی کارکردهای آن متمایل گشته، و اساساً مفهومی کارکردی شده است. در حقیقت، این مفهوم، از معنای پیش به یکی از لوازم آن منتقل گشته است.

بدین روی، فضای سایبر بر اساس این تعریف، امری است که کارکردهای پیش‌گفته را تحقق می‌بخشد. البته امروز این امر، عمدتاً دیجیتال و الکترونیکی است؛ هر چند اجزای غیرالکترونیکی، و اساساً غیرسخت‌افزاری نیز دارد که در تحقق بخشیدن به این کارکردها نقش دارند، مانند لایه‌های منطقی و نرم‌افزاری و حتی لایه‌ی انسانی به‌عنوان کاربران.

کارکردهای سه گانه فوق‌الذکر البته ممکن است بعداً گسترش یابد. هر چند بعید می‌نماید کارکردی جدید برای فضای سایبر پدید آید که از زیرعنوان کلی «تمشیت» امور یا انجام کار و مانند آن بیرون باشد؛ لکن ممکن است موردی از آن، در کاربردهای روزمره وجه غالب یافته و برجسته شود و در شناسایی هویت فضای سایبری در تلقی و ذهنیت عمومی، ملاک نام‌گذاری و کاربرد اصطلاح گردد و با کاربرد اصطلاح فضای سایبر، در اذهان تداعی شود.

تعریف کارکردگرایانه از فضای سایبر علاوه بر اینکه نسبت به نحوه‌ی تحقق آن، و بسترهای سخت‌افزاری و مدل‌های آن، و از جمله نسبت به دیجیتالی بودن، لایشرط است، انتزاعی‌تر از تعریف پیشین است؛ بنابراین، بنیادی‌ترین، کامل‌ترین و ثابت‌ترین تعریف از فضای سایبر است که در برابر تغییرات احتمالی، دچار تضاد یا بی‌مسامی نخواهد گشت و وجه تسمیه‌ی خود را از دست نخواهد داد. بنابراین، آن را می‌توان پایه‌ی ثابت همه‌ی تعاریف دیگر دانست به‌نحوی که نظریه‌های دیگر درباره‌ی فضای سایبر، هرکدام بیان وجهی از آن، یا تعریف بخشی یا لازمه‌ای از لوازم وجودی آن، یا اشاره به حیثیتی از آن خواهد بود. بنابراین، تعریف کارکردگرایانه برای مطالعات علوم انسانی، نظیر نگرش‌های حقوقی، سیاسی، جامعه‌شناختی، تربیتی،

<sup>37</sup>Nunes, 1995: 1

<sup>38</sup>این کارکردها از طریق تعاملات گوناگون میان انسان-ماشین، ماشین-ماشین، و ترکیب آنها تحقق می‌یابد.



روان‌شناختی، اخلاقی، و اقتصادی به فضای سایبر مناسب‌ترین است. چنان‌که ما نیز در اینجا، این تعریف را پایه‌ی نظریه‌ی فضای سایبری به مثابه ذهن-جهان قرار داده‌ایم.

## ۲.۵ فضای سایبری یا فضای مجازی؟

در این تعریف، به‌ویژه مفهوم «فضا» برخلاف تعریف نخست - که این کلمه در آن، اشاره به شبکه‌ای از سخت‌افزارهای الکترونیکی داشت، فیزیکی و مادی نیست، بلکه دریافتی انتزاعی‌تر از مفهوم «فضا» در میان است که گاه با عنوان «مجازی» به آن اشاره می‌کنند، و حتی بسیاری اوقات، فضای سایبر با این ویژگی یعنی مجازی بودن نامیده می‌شود. گرچه در مجازی نامیدن این فضا، می‌توان تشکیک و اشکال کرد، چرا که فضای سایبری، کارکردهایی کاملاً «حقیقی» و «واقعی» را محقق می‌سازد؛ مگر اینکه مقصود از مجازی، غیرفیزیکی باشد - که با توجه به کاربردهای این اصطلاح به نظر می‌رسد چنین هم بوده است - در این صورت، می‌توان یکی از ویژگی‌های آن را «مجازی» بودن آن دانست، اما تعریف فضای سایبری به «فضای مجازی» یا برابر دانستن آن دو، اشکالات زیادی دارد. از جمله اینکه: مجازی بودن، نه‌تنها مساوی با همه‌ی هویت فضای سایبری نیست، ویژگی اصلی یا دخیل در هویت بخشی به آن نیز نیست، و صرفاً یکی از لوازم آن است. همچنین، امور دیگری هم هستند و می‌توانند باشند که به‌همین اندازه و بیشتر، مصداق امور یا فضای مجازی باشند؛ بنابراین تعریف به این ویژگی، به‌هیچ‌وجه مانع اغیار نیست. البته معمولاً فضای سایبری با این عنوان تعریف نمی‌شود و مجازی بودن صرفاً مناسبی برای نام‌گذاری در نظر گرفته می‌شود؛ لکن تأکید بر این مناسبت و وجه فضای سایبری، و نامیدن آن به این عنوان می‌تواند غلط‌انداز باشد؛ از این روی بهتر است چنین نامیده نشود. البته آن بخشی از کارکردهای فضای سایبری که واقعیت‌های مجازی را به ظهور می‌رساند، تناسب بسیاری با این عنوان دارند و بهتر است فضای مجازی صرفاً به آن بخش از فضای سایبری اطلاق شود و اگر روزی، واقعیت مجازی داشتن، تبدیل به جنبه‌ی غالب فضای سایبری شد، می‌توان نام‌گذاری به فضای مجازی برای فضای سایبری را هم وجه تسمیه‌ی قابل قبولی دانست.

فضای سایبر به تعریف نخست آن هم اساساً امری فیزیکی است؛ بنابراین در تلقی‌های فنی و نگرش‌های مهندسی و سخت‌افزار محور به فضای سایبر، مفهوم مجازی اصلاً مناسبی ندارد.

## ۶ فضای سایبر به مثابه امری سایبری

### ۱.۶ سایبر و امر سایبری

چنان‌که اشاره کردیم، «فضای سایبر» به‌مثابه کارکرد، یکی از لوازم آن به‌معنای پیشین است که بر اساس آن، این فضا به «امری سایبری» تعریف می‌شود که کارکردهای خاص آن را تحقق می‌بخشد. بنابراین، شاید دقیق‌تر و بهتر آن باشد که آن را به فضای سایبری تعریف و ترجمه کنیم نه فضای سایبر؛ چرا که هیچ امری با کارکردها یا لوازم آن، نمی‌تواند یکی انگاشته شود.

پیش‌تر اشاره کردیم که سایبر برگرفته از سایبرنتیک است که وصف سیستم‌های کامپیوتری و غالباً اینترنت قرار می‌گیرد و از باب استعمال صفت به‌جای موصوف، اغلب در معنای خود اینترنت به کار می‌رود؛ از

این رو ترکیب «فضای سایبر» تقریباً معادل با «فضای اینترنت» است. در اینجا این پرسش رخ می‌نماید که امر سایبری، و از جمله «فضای سایبری» چه نوع ترکیبی است و چه معنا و کاربردی دارد؟ و اساساً تعبیر «فضای سایبر» درست است یا «فضای سایبری»؟ آیا فرقی میان آنها هست؟ کدامیک دقیقاً معادل Cyberspace است؟

## ۲.۶ فضای سایبر یا فضای سایبری؟

به لحاظ لغوی و زبانی، ترکیب «فضای سایبر» در زبان فارسی، ترکیب اضافی است، و «فضای سایبری» ترکیب وصفی. اما هر دوی اینها معمولاً در ترجمه‌ی Cyberspace به کار می‌روند. بنابراین باید دید این تعبیر در زبان انگلیسی چه معنا و کاربردی داشته یا می‌تواند داشته باشد.

لفظ Cyber در زبان انگلیسی دو گونه به کار می‌رود<sup>۳۹</sup>: به صورت پیشوند در یک ترکیب مزجی<sup>۴۰</sup> - همانند پیشوند «الکترو» در کلمه‌ی الکترومغناطیس - که به همراه کلمه‌ای که با آن ترکیب می‌شود کلمه یا اصطلاح تازه‌ای را بر می‌سازد و به آن، معنای کامپیوتر یا اینترنت یا همان سایبر را می‌افزاید؛ مانند Cyberspace که در فارسی به «فضای سایبر» ترجمه می‌شود. هر چند بهتر و دقیق تر آن است در فارسی نیز به صورت کلمه‌ی مرکب برگردانده شود نه ترکیب وصفی یا اضافی؛ نظیر «سایبرجهان» که شاید بهترین معادل فارسی این اصطلاح باشد. البته کلمات مرکب گاهی به صورت ترکیب اضافی نیز به کار می‌روند؛ بنابراین، ترجمه‌ی آن به «فضای سایبر» نیز درست است.

صورت دوم کاربرد آن، ترکیب وصفی است که به موصوف خود معنای وابستگی یا انتساب به، یا درباره‌ی کامپیوتر یا اینترنت بودن را می‌دهد، و به مفهوم یا امری سایبری دلالت می‌کند. مانند The cyber marketplace به معنای فروشگاه سایبری. صورت ترکیب وصفی، به شکل دو کلمه‌ی جدا از هم یعنی Cyber Space نوشته می‌شود؛ پس در فارسی نیز باید آن را به صورت وصفی، یعنی «فضای سایبری» معنا کرد. بنابراین، میان دو صورت نوشتاری این اصطلاح، تفاوت اندکی وجود دارد: در دومی کلمه‌ی سایبر، در نقش وصف قرار می‌گیرد، و فضا را به مثابه امری سایبری توصیف می‌کند، فضایی که خصلت سایبری بودن دارد؛ یعنی فضایی که نوعی از انتساب و ربط و وابستگی با جهان سایبرنتیک را داراست؛ بنابراین می‌توان و باید آن را «سایبری» ترجمه کرد. ولی اولی یعنی صورت مرکب و به هم چسبیده‌ی آن، خود سایبر را به مثابه یک فضا و جهانی خاص در نظر می‌گیرد و به عبارت دیگر، خود سایبر را از سنخ جهان و عالم یا فضا می‌شمارد. از همین جا معلوم می‌شود که از لحاظ معنای لغوی، ترجمه‌ی این اصطلاح به مثابه یک محیط سخت‌افزاری یا دیجیتال به «فضای سایبر» صحیح‌تر و بهتر است.

با اینکه موضوع تفاوت دو صورت نوشتاری اشاره شده، برای برخی جالب و محل سؤال بوده است،<sup>۴۱</sup> تا جایی که ما جست‌وجو کردیم به پژوهشی که به تفاوت معنایی این دو اصطلاح و تحلیل زبانی آن پرداخته

<sup>39</sup>See: Cyber. 2022. In Merriam-Webster.com Retrieved August 28, 2022, from <https://www.merriam-webster.com/dictionary/Cyber>

<sup>40</sup>Combining form

<sup>41</sup>Thomas W. Edgar, David O. Manz.Edgar, Thomas W. (2017), p 42

باشد، دست نیافتیم. لکن، مسئله‌ی اصلی و مهم در فهم معنا و ترجمه‌ی این دو اصطلاح، مراجعه به کاربرد آن است که ممکن است لزوماً با مفهوم لغوی آن مطابق نباشد.

ما در ابتدای پژوهش نگاهی به کاربردشناسی تاریخی این اصطلاح انداختیم، و همان‌طور که دیدیم نخستین کاربرد این اصطلاح، استعمال آن به‌مثابه «نام» یک فضای موهوم و خیالی بر ساخته شده توسط ویلیام گیبسون بود. بنابراین، در این نوع از کاربردهای این اصطلاح، ساختار و معنای لغوی کلمه اساساً اهمیت و دخالتی در شناخت مدلول آن نخواهد داشت. چرا که اسمای خاص<sup>۴۲</sup> - چنان‌که علمای اصول فقه و برخی از فلاسفه‌ی زبان تحلیلی مانند کریپکی<sup>۴۳</sup> بیان کرده‌اند - به‌مثابه نشان‌ها یا دال‌های ثابتی<sup>۴۴</sup> هستند که هیچ معنای تضمینی وصفی یا محتوای توصیفی<sup>۴۵</sup> ندارند و صرفاً بر مصداق<sup>۴۶</sup> یا مسمای خود ارجاع می‌دهند و از آن حکایت می‌کنند بی‌آنکه محتوای سمانتیکی آنها دخالتی در دلالت<sup>۴۷</sup> بر مدلول خود داشته باشد.<sup>۴۸</sup> از این روی، اگر کلمه‌ی Cyberspace را اسم علم مرتجلی بدانیم که گیبسون آن را بر فضای خیالی بر ساخته‌ی خویش ابداع<sup>۴۹</sup> و وضع کرده است - چنان‌که خود او نیز در مصاحبه‌ای بر این امر تأکید می‌ورزد<sup>۵۰</sup> - یا آن را به عنوان اسمی برای تعریف خاصی از فضای سایبر به کار بریم که حاکی از پدیده‌ی عینی مشخصی باشد، هیچ نیازی به بررسی لغوی و ساختار زبانی آن نخواهیم داشت، و فقط باید به دنبال مشخص کردن چیستی و ویژگی‌های مدلول آن باشیم. اما آن‌گاه که در صدد بیان مفهوم انتزاعی خاصی هستیم، و این کار را با وصف آن به «سایبری» انجام می‌دهیم، باید مراد از لفظ سایبری و معنا و سبب انتساب آن مفهوم به این عنوان را بررسی کنیم.

بنابراین، حداقل تعریف این فضا بر اساس کارکردهای آن که اتفاقاً متداول‌ترین معنای مراد در استعمالات این اصطلاح است، قاعدتاً باید به‌مثابه امری سایبری در نظر گرفته و در فارسی به «فضای سایبری» ترجمه شود. در زبان انگلیسی نیز بهتر است اگر این اصطلاح، یا هر اصطلاح مشابه آن به‌مثابه یک «نام» به یک مصداق عینی دلالت کند، چسبیده نوشته شود، و اگر یک مفهوم یا امری که منسوب به امری دیگر است از آن قصد شود، به صورت ترکیب اضافی یا وصفی که نشان‌دهنده‌ی دو مفهوم و نسبت میان آنهاست نوشته شود. مثلاً در اموری مانند پول سایبری، اگر وجه دلالت بر مصداق، در نظر گرفتن دو امر و نسبت آنها باشد، به صورت جداگانه (Cyber Cash = پول سایبری) و اگر صرفاً نامی بر آن در نظر گرفته شود به صورت

<sup>42</sup>Proper Names

<sup>43</sup>See: Keripke, 1972,3.

<sup>44</sup>Rigid Designator.

<sup>45</sup>Connotation

<sup>46</sup>Object

<sup>47</sup>Denotation

<sup>48</sup>در فلسفه‌ی زبان تحلیلی، و پیش‌تر در مباحث الفاظ علم اصول فقه، بحث شده است که آیا اعلام یا اسمی خاص معنا دارند یا فقط دارای مدلول‌اند و به‌طور مستقیم و بدون واسطگی مفهوم ذهنی، بر مصداق خود دلالت می‌کنند. طبق دیدگاه پذیرفته شده در اسمای خاص، وجه تسمیه هر چه باشد، دخالتی در دلالت بر مدلول یا مصداق آن ندارد؛ بنابراین در این گونه اسم‌ها اساساً معنای لغوی کلمه اهمیتی ندارد برای مثال، وقتی نام کسی را «عبدالله» می‌گذاریم، وقتی آن را به کار می‌بریم، هیچ توجه و اهمیتی به معنای لغوی آن نمی‌دهیم، بلکه صرفاً کسی که به آن نام نامیده شده است را قصد می‌کنیم.

<sup>49</sup>Coinage

<sup>50</sup>Kneale, 1999

چسبیده (CyberCash = سایبرپول) نوشته شود؛ نظیر رمزارز که در ترجمه‌ی Cryptocurrency به کار گرفته می‌شود. تفاوت در این است که: وجه دلالت اولی بر مدلول خود، اسمی و در دومی به نحو وصفی است.<sup>۵۱</sup>

به عنوان پیشنهاد، می‌توان برای نشان دادن تفاوت دو تلقی، در زبان فارسی از دو تعبیر «فضای سایبر» و «فضای سایبری» بهره برد. و برای اشاره به زیرساخت سخت‌افزاری، تعبیر نخست؛ و درباره‌ی فضایی که کارکردهای اشاره شده در آن تحقق می‌یابد، تعبیر دوم را به کار برد. چرا که چنان که اشاره کردیم، مفهوم «سایبر» که کوتاه شده و برگرفته از «سایبرنتیک» است، بیشتر اشاره به سخت‌افزارها دارد و سایبر در این معنا، به معنای شبکه‌ای از کامپیوترها و به عبارت دیگر اینترنت است؛ بنابراین در تعریف اول که یک تلقی سخت‌افزارمحور است، فضا با سایبر (یا سیستم‌های سایبرنتیکی) این همان است (گویا گفته می‌شود، فضای کامپیوتر، یا کامپیوترها). برخلاف تعریف دوم که در آن، مفهوم فضا، نه خود سایبر، بلکه امری سایبری و منتسب به سایبر و از لوازم آن و مبتنی یا منتزع از آن است؛ بنابراین، «فضای سایبری» برای تعبیر از آن، مناسب‌تر است. هر چند چنان که گفتیم، امکان دارد در آینده، این فضا، اساساً حتی سایبری (یعنی مبتنی بر ماشین‌های محاسباتی) نباشد، و این نام‌گذاری مناسب خود را از دست بدهد. از این رو، تعبیر «فضای سایبر» مناسب جنبه‌ی فنی-مهندسی است و «فضای سایبری» با بُعد انسانی-شناختی تناسب دارد.

با اینکه از زاویه‌ی نگاه زبانی این دو اصطلاح، باید تفاوت معنایی داشته باشند، پژوهشی که درباره‌ی نحوه‌ی کاربرد این دو صورت نوشتاری، و ویژگی‌های معنایی مراد از آنها در گستره‌ی اینترنت صورت گرفته است نشان می‌دهد که در عمل، هر دو صورت نوشتاری اصطلاح Cyberspace تقریباً<sup>۵۲</sup> به یک اندازه، در تداول عمومی کاربرد دارد. لکن برای جعل اصطلاح جدید، بهتر آن است به تفاوت معنایی و زبانی این اصطلاح در کاربرد آنها توجه شود. بنابراین همه‌ی امور مربوط و منتسب و درباره‌ی فضای سایبر بهتر است در انگلیسی به صورت وصفی و جدا از هم نوشته و در فارسی به «فضای سایبری» برگردانده شود.

## ۷ فضای سایبری به مثابه ذهن-جهان

واقعیت این است که تعاریف فوق و تعاریف دیگر و نویی که می‌توانند به آنها افزوده شوند، هر کدام به دنبال مشخص کردن بُعدی از واقعیت چیزی است که به اصطلاحات گوناگون، فضای سایبر نامیده می‌شود. بنابراین، اشکالی ندارد که هر کدام از آنها را در جای خود و به تناسب بحث و موضوع پژوهش و منظر نگاه، به کار گرفت؛ به شرط اینکه مقصود خود را به طور مشخص روشن کنیم. البته ما استدلال کردیم که در مطالعات غیر فنی-مهندسی تعریف کارکردگرایانه بهترین تعریف از فضای سایبری است، چرا که دلالت مطابقی کاملی بر معرف

<sup>۵۱</sup> درباره‌ی دو اصطلاح Cyber Security و Cybersecurity و اینکه کدام یک صحیح است و باید به کار گرفته شود، در برخی پژوهش‌ها، پرسش مطرح شده است؛ و چنان که از پژوهش متن برمی‌آید، چون موضوع امنیت سایبری، دلالت بر هیچ مصداق عینی مشخصی نیست و کاربرد اسمی نمی‌توان برای آن تصور کرد، به لحاظ زبانی درست‌تر آن است که به صورت وصفی و جدا از هم نوشته شود، چرا که امنیت سایبری، امری مرتبط با فضای سایبر است نه نامی بر پدیده‌ای خاص. هر چند بررسی کاربرد آن نشان می‌دهد، هر دو صورت آن به قصد معنای واحد به کار می‌رود (Madnick, Stuart (2012), p 7).

<sup>۵۲</sup> پژوهشی که درباره‌ی فراوانی کاربرد این دو کلمه در اینترنت صورت گرفته است که نشان می‌دهد، تداول صورت مرکب کلمه، قدری بیشتر است (Madnick, Stuart (2012).

خود دارد؛ ولی بر بنیاد آن می‌توان و باید تعاریف دیگری از آن نیز به دست داد که شامل وجوه دیگر و خاصی از فضای سایبری باشند. آنچه مهم است، تفکیک و معرفی دقیق ابعاد امری است که در پی برجسته‌سازی و نام‌گذاری آن هستیم؛ به‌خصوص در بحث‌های انتزاعی و فلسفی. کشف و معرفی لوازم فضای سایبر، و تفکیک دقیق ابعاد مختلف آن از هم و نظریه‌پردازی در آن باره، قدمی مهم و مقدمه‌ای واجب در مطالعات مربوط به فلسفه فضای سایبری و مطالعات علوم انسانی دیگر وابسته به آن است.

بنابراین توجه به هویت کارکردی فضای سایبری، هر چند دقیق و کاربردی است، لکن به فضای سایبری می‌شود فلسفی‌تر هم نگریست. در این نگاه که انتزاعی‌تر از نگرش قبلی است، حتی کارکردهای فضای سایبر نیز کانون توجه اصلی نیستند، بلکه صرفاً روابط بین‌الذهانی که میان کاربران - با وساطت ابزارهای ارتباطاتی و در اثر تحقق کارکردهای آن - ایجاد می‌شود، موضوع توجه قرار می‌گیرد. در این نگاه، بُعد شناختی فضای سایبری، کانون توجه است. بر این اساس فضای سایبری جهانی بین‌الذهانی است که در آن انسان‌ها به‌وسیله‌ی ابزارهای ارتباطاتی با همدیگر یا با ماشین‌ها روابط ذهنی و شناختی برقرار می‌سازند. این رابطه‌ها، اغلب از طریق گفت‌وگو (شنیداری، دیداری یا نوشتاری)، ارسال و دریافت انواع اطلاعات (داده‌های خام، یا اطلاعات پردازش‌شده)، و تعاملات (مانند دادوستد سایبری، بازی، و اجرای فرایندهای اداری) صورت می‌گیرد. این تعریف از فضای سایبری، در حقیقت اشاره به فضای دیگری دارد که از لوازم و آثار فضای سایبری به معنای متداول و پیشین است و بیش از آنکه تعریف باشد نظریه است؛ چون اثبات‌کننده‌ی حقیقتی جدا و عالمی واقعی با ویژگی‌ها و آثاری متفاوت است.

عالم یا جهان، بر ساخته از اجزا و اعضای حاضر در آن است؛ به‌عبارت دقیق‌تر، حاصل نسبت‌های برقرار شده میان آن اجزا و اعضاست؛ بنابراین مفهومی انتزاعی‌تر است. بر خلاف مفهوم «فضا» که تداعی‌گر خصوصیات مکان و ابعاد است؛ بنابراین تصویری خیالی و انضمامی مشابه با جهان مکانی و فیزیکی است، ولی مفهوم ذهن جهان مفهومی عقلی‌تر و به معنای نسبت‌های برقرار شده میان ذهن‌های مشارکت‌کننده در ارتباط از راه دور، و عاملان و پذیرنده‌های انتقال اطلاعات است.

فضای سایبری بدین معنا، زیست‌جهانی ذهنی و غیرفیزیکی است؛ دنیای ذهن‌های مرتبط است. بنابراین، نه از جنس زیرساخت‌های الکترونیکی و دیجیتال است، و نه با کارکردهای فضای سایبر - یعنی برقراری ارتباطات، فرستادن و گرفتن اطلاعات و اعمال کنترل‌های دیجیتال - تعریف می‌شود. در این تعریف، فضا در حقیقت فرض می‌گردد و به‌لحاظ هستی‌شناختی وجودی مستقل ندارد، گرچه واقعیتی مسلم است - مجازی به‌معنای غیر واقعی نیست، هر چند می‌توان آن را مجازی به‌معنای غیرمادی پذیرفت - اما نه واقعیت عینی و اصیل، بلکه واقعیتی انتزاعی و اعتباری و دارای هویتی فرضی. بنابراین، موجود مستقلی مثلاً در مرتبه‌ی خیال منفصل، یا عالمی مثالی نیست؛ بلکه صرفاً اشتراک محتوایی خیال متصل و مدرکات ذهنی انسان‌هاست؛ جهانی است برآمده از نسبت‌های برقرار شده میان ذهن‌های حاضر در آن. بدین جهت مناسب‌ترین تعبیر برای حکایت از آن «عالم مشترک بین‌الذهانی» است.

به‌عبارت فلسفی‌تر، این عالم بین‌الذهانی ما به‌الازاء ندارد، بلکه ما به‌الانتزاع داریم. منشأ انتزاع آن نیز ذهن‌ها و محتواهای ذهنی تک تک افراد با در نظر گرفتن نسبت‌های شناختی برقرار شده میان آنهاست که آن هم در حقیقت، توسعه‌ی نسبت‌های شناختی و ذهنی برقرار شونده در زندگی عادی و ارتباطات رو در



روی اشخاص است که به وسیله فضای سایبری به معنای پیشین، گسترش شگرف و بی سابقه‌ای یافته و از این رو ویژگی‌ها و آثار جدیدی پیدا کرده است.

بنابراین، بهتر است برای تفکیک این دو نگاه و تعریف، تلقی فلسفی‌تر از فضای سایبر را ذهن جهان سایبری بنامیم؛ زیرا چنان که اشاره کردیم، عناصر اصلی تشکیل دهنده شبکه‌ی این فضا، انسان‌ها و اذهان و قوای شناختی‌شان و به عبارت دیگر، سوژه‌ها هستند و سخت‌افزارها، یا الگوریتم‌ها، یا دیگر عناصر فضای سایبر، در آن لحاظ نمی‌گردند؛ چرا که صرفاً نقش واسطه در ثبوت و تحقق دارند، و حتی روزی ممکن است حذف و با واسطه‌های دیگری جایگزین شوند. همچنین کارکرد تمشیت امور که ناظر به عمل و فعل است، در این تعریف ملحوظ نیست. مهم‌ترین جهت نسبت برساننده‌ی این عالم هم، اشتراک در محتواهای شناختی فعالان و حاضران در این باشگاه ذهنی است که متأثر از فعالیت ذهنی افراد، و محتواهای ذهنی به اشتراک گذاشته شده، و تأثیر و تأثرات اذهان و ایده‌های ذهنی در هم، با سرعتی سرسام‌آور هر لحظه صورتی دیگر به خود می‌بیند و رنگ و بویی نو می‌گیرد، و در جهتی توسعه یا تضییق می‌یابد. بنابراین این فضا، ساخت یافته از عناصری زنده و ذهن‌مند به معنای واقعی است و جنبه‌ی ذهنی - شناختی دارد. جامعه‌ی سوژه‌هاست. فضایی پر از سروصدا و هیاهو و رنگ و تصویر و تصور و نویزهای فکری، خیالی، وهمی که میان اذهان با ترافیکی بسیار حجیم، رد و بدل می‌شود. گویا مجموعه‌ی یک انسان بسیار بزرگ است که درون آن، هر لحظه میلیاردها پالس و پیام ذهنی به وسیله شبکه‌های درهم پیچیده‌ای از عصب‌های ارتباطی جریان دارد.

البته این جامعه، غیر از اجتماع تک تک سوژه‌ها، و نسب میان آنها، واقعیت مجزای دیگری ندارد؛ درست مانند مفهوم «جامعه» که در تحلیل فلسفی، نمی‌توان جز ترکیب انضمامی از مجموع انسان‌ها برای آن واقعیتی منحاز لحاظ کرد. بنابراین فضای سایبری به این معنا چیزی جز نسبت‌هایی که میان اذهان برقرار می‌شود نیست. روابط و نسبت‌هایی که البته واقعا برقرار می‌شوند، و آثار واقعی و عینی هم دارند، و اهمیتی ندارد که به لحاظ هستی‌شناختی نمی‌توان برای آن، وجودی منحاز و جدای از وجود اجزا و عناصر قائل شد. چنان که اجتماع انسان‌ها نیز هر چند نتوان برای «جامعه» وجودی جدا از وجود افراد در نظر گرفت و آن را مرکبی حقیقی دانست، آثاری غیر از مجموع آثار وجود انسان‌ها دارد؛ چرا که از اجتماع و ترکیب وجود اشخاص، آثاری غیر از مجموع آثار وجودی اشخاص، ظهور می‌یابد، و واقعیتی به نام جامعه پدید می‌آید که آثار و احکام خاص خود را دارد؛ شبیه مرکبات صناعی (مثلاً یک خودرو) که شکل و صورت ترکیبی، فعلیت جدیدی در آنها پدید می‌آورد که مساوی با مجموع فعلیت‌های عناصر یا قطعات شکل دهنده‌ی آنها در حالت غیر مرکب نیست. بنابراین، این جامعه‌ی متشکل از اذهان، گو اینکه هستی مستقلی جز هستی مجموع فاعل‌های شناسایی ندارد، صورت‌ها، فعلیت‌ها، و آثاری بیشتر و به شدت متفاوت از آن دارد، به نحوی که اساساً با همان آثار ریشه گرفته از این صورت و فعلیت ساختاری‌اش تعریف می‌شود؛ و با صرف نظر از دقت نظری‌های هستی‌شناختی فلسفی می‌توان برای آن هویتی واقعی در نظر گرفت و آن را تعریف کرد و از خواص و آثار واقعی‌اش سخن گفت؛ زیرا هر چند وجودش اصالت نداشته باشد، آثارش اصالت و واقعیت دارند؛ بنابراین نحوه‌ی وجود خاص خود را دارد که هویت خود را از آن می‌گیرد و به آن، تعریف می‌شود.

ذهن جهان سایبری نیز مانند فضای سایبری، نسبت به بنیادهای فیزیکی یا دیجیتال، لابلش است و



تغییرات احتمالی رخ داده در بنیادهای فیزیکی و نحوه‌ی تحقق آنها اثری کیفی یا هویتی در آن نخواهد داشت. همچنین چنان که فضای سایبری از لوازم فضای سایبر است، ذهن جهان سایبری نیز از لوازم فضای سایبری و به‌طور خاص از خواص ویژگی شبکه‌ای آن است؛ اما هر چند با فضای سایبری ملازمه دارد و بدون آن نمی‌تواند تحقق یا وجود یابد، ماهیتاً با آن تفاوت دارد. به‌عبارت فلسفی‌تر، ذهن جهان سایبری هر چند لازم وجود فضای سایبری است، لازم ماهیت آن نیست. و به‌خاطر اینکه ریشه در جهان واقعی دارد، آثار آن در تک تک افراد و کل جامعه، بازتاب و امتداد می‌یابد و تأثیر واقعی می‌گذارد. بنابراین، آثار روان‌شناختی و جامعه‌شناختی متعددی در پی می‌آورد و تمام شئون وجودی انسان را از طریق تغییراتی که در ذهن و روان او می‌گذارد، متأثر می‌سازد. تأثیراتی که هر کدام می‌تواند و باید موضوع مطالعات مرتبط با فضای سایبری قرار گیرد؛ نظیر روان‌شناسی ذهن جهان سایبری، جامعه‌شناسی ذهن جهان سایبری و غیره.

## ۱.۷ خرده‌جهان‌های ذهنی

ذهن جهان سایبری البته درون خود پیچیدگی‌های بسیاری دارد. داخل این فضای بسیار بزرگ، منطقه‌های ذهنی زبانی متفاوت و قابل تمایزی وجود دارد. این تمایزها بر اساس تراکم نسبت‌هایی است که میان اذهان مناطق خاص جغرافیایی ذهنی زبانی فرهنگی، و بین سوژه‌های هم‌ذهن برقرار می‌گردد. البته میان منطقه‌های ذهنی نیز به‌نوبه‌ی خود، روابط و نسبی برقرار است، لکن نه به تراکم و شدتی که درون آن مناطق هست. تبیین ویژگی‌های خرده‌جهان‌ها، و نیز پرداختن به سایر ویژگی‌های ذهن جهان سایبری، البته موضوعات بسیار پر اهمیتی است که طرح آنها در ادامه‌ی این مبحث ما را به شناخت این پدیده نزدیک‌تر خواهد ساخت؛ لکن قصه‌ی درازی است که اجمالاً این مقاله، مجال طرح آن را در اینجا از ما می‌گیرد.

چنان‌که با تفکیک این مفاهیم انتزاعی مبتنی بر واقعیات فضای سایبر، و تعریف و بیان ویژگی‌ها و روشن ساختن ابعاد گوناگون آن، کار پایان نمی‌یابد؛ بلکه این امر، مقدمه‌ای برای پژوهش‌های بعد، و آغاز جستارهای پردامنه‌ای خواهد بود که اکنون موضوع آن به‌دقت مشخص و تعریف شده است.

## مراجع

- [1] Gibson, William; Bruce Sterling (1986). *Burning Chrome*, New York: Harper Collins.
- [2] Gibson, William (1984). *Neuromancer*. ACE.
- [3] Keripke, Saul A. (1972). *Naming and Necessity*, 2nd. ed., UK: Basil Blackwell.
- [4] Kneale, J. (1999). *The Virtual Realities of Technology and Fiction: Reading William Gibson's Cyberspace*, in Crang, M. et al (eds.): *Virtual Geographies: Bodies, Space and Relations*, pp. 205-221; Routledge: London.
- [5] Madnick, Stuart; Choucri, Nazli; Camiña, Steven; and Woon, Wei Lee (2012). "Towards Better Understanding Cybersecurity: or are "Cyberspace" and "Cyber Space" the Same?," WISP 2012 Proceedings.
- [6] Nunes, M. (1995). *Baudrillard in Cyberspace: Internet, Virtuality, and Postmodernity*, Style 29, pp. 314-327

- [7] Wiener, N. (1948). *Cybernetics: Or, Control and Communication in the Animal and the Machine*. MIT University Press, Cambridge, MA, 212.
- [8] Edgar, Thomas W.; Manz, David, O. (2017). *Research methods for cyber security*, Cambridge, MA : Syngress, an imprint of Elsevier.