Iranian Journal of Public Policy
2024 , Vol. 10 , No. 4 , 54-74
Online ISSN: 2538-5089
Home Page: jppolicy.ut.ac.ir

RESEARCH ARTICLE

Artificial Intelligence and Fundamental Transformation in Security-Defense Policies: Understanding the Position of Human Security

Ali Ashraf Nazari

Associate Professor of Political Science, University of Tehran, Tehran, Iran

Corresponding Author's Email: aashraf@ut.ac.ir

https://doi.org/10.22059/jppolicy.2024.99826

Received: 5 October 2024
Accepted: 30 November 2024

ABSTRACT

In the last decade, fundamental changes have been made in relation to the place of technology in human life, and new issues have been raised in relation to the digitalization of politics and changes in political and security attitudes. Today, artificial neural networks and algorithmic governance are used to monitor, control and regulate human actions. One of the areas in which artificial intelligence has found an important application is security in its broadest sense, including defense or military security, human security (information, internal security and economic and financial security), occupational security, health security and cyber security (information security). and the Internet of Things). These innumerable application areas and the inability of humans to exercise full control like machines force people in the security community to think about the possible vulnerabilities and security gaps caused by this evolving technology. Hence, technology is always a constant source of uncertainties. There have been risks, changes and in many cases disruptions. The main question of the current article is how artificial intelligence causes the evolution of human abilities in the field of national security policymaking? The central hypothesis is that considering that the use of large-scale analysis supports data analysis and managerial decision-making, the adoption of new technologies plays a vital role in decision-making at organizational levels. And someone plays a security role. In this article, by focusing on this question and hypothesis, the consequences of the use of artificial intelligence in the field of security will be considered.

Keywords: Artificial Intelligence, Security, Human Security, Algorithm, Digitization.

Citation: Ashraf Nazari, Ali (2024). Artificial Intelligence and Fundamental Transformation in Security-Defense Policies: Understanding the Position of Human Security. *Iranian Journal of Public Policy,* 10 (4), 54-74,
DOI: https://doi.org/10.22059/jppolicy.2024.99826

Published by University of Tehran.

فصلنامه سیاستگذاری عمومی

دوره ۱۰، شماره ۴، زمستان ۱۴۰۳. صفحات ۷۴-۵۴

شاپا الکترونیکی: ۵۰۸۹ - ۲۵۳۸

آدرس سایت: jppolicy.ut.ac.ir

مقاله پژوهشی

هوش مصنوعی و تحول بنیادین در سیاستگذاری‌های امنیتی- دفاعی: درک جایگاه امنیت انسانی

علی اشرف نظری

دانشیار علوم سیاسی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران

رایانامهٔ نویسنده مسئول: aashraf@ut.ac.ir

تاریخ دریافت: ۱۴ مهر ۱۴۰۳
تاریخ پذیرش: ۱۰ آذر ۱۴۰۳

https://doi.org/10.22059/jppolicy.2024.99826

چکیده

در یک دههٔ اخیر تغییرات بنیادینی در رابطه با جایگاه -فناوری در زندگی انسان ایجاد شده و موضوعات جدیدی در رابطه یا دیجیتالی شدن سیاست و تحول در نگرش‌های سیاسی و امنیتی مطرح شده است. امروزه، شبکه‌های عصبی مصنوعی و حاکمیت الگوریتمی برای پایش، کنترل و نظم دادن به کنش‌های انسانی استفاده می‌کند. یکی از حوزه‌هایی که هوش مصنوعی در آن کاربرد مهمی پیدا کرده است، امنیت به معنای وسیع آن شامل امنیت دفاعی یا نظامی، امنیت انسانی (اطلاعات، امنیت داخلی و امنیت اقتصادی و مالی)، امنیت شغلی، امنیت بهداشتی و امنیت سایبری (امنیت اطلاعات و اینترنت اشیا) است. این حوزه‌های کاربردی بی‌شمار و ناتوانی بشر در اعمال کنترل کامل مانند ماشین‌ها، افراد جامعه امنیتی را وادار می‌کند تا به آسیب‌پذیری‌های احتمالی و شکاف‌های امنیتی ناشی از این فناوری در حال تکامل فکر کنند از این رو، فناوری همیشه منبع دائمی عدم قطعیت‌ها، مخاطرات، تغییرات و در بسیاری موارد اختلال بوده است. پرسش اصلی مقاله حاضر این است که هوش مصنوعی چگونه موجب تحول در توانایی‌های انسان در حوزهٔ سیاستگذاری ملی در رابطه با امنیت می‌شود؟ فرضیه محوری این است که با توجه به اینکه استفاده از تجزیه و تحلیل در مقیاس بزرگ از تجزیه و تحلیل داده‌ها و تصمیم‌گیری مدیریتی پشتیبانی می‌کند، پذیرش فناوری‌های جدید نقشی حیاتی در تصمیم‌گیری در سطوح سازمانی و فردی حوزهٔ امنیت ایفا می‌کند. در این مقاله با تمرکز بر این پرسش و فرضیه به صورت هدفمند تلاش خواهد شد پیامدهای ناشی از کاربست هوش مصنوعی در حوزه امنیت مورد نظر قرار گیرد.

واژگان کلیدی: هوش مصنوعی،امنیت، امنیت انسانی، الگوریتم، دیجیتالی‌شدن.

استناد: اشرف نظری، علی (۱۴۰۳). هوش مصنوعی و تحول بنیادین در سیاستگذاری‌های امنیتی- دفاعی: درک جایگاه امنیت انسانی. *فصلنامه سیاستگذاری عمومی*، ۱۰ (۴)، ۷۴-۵۴.

DOI: https://doi.org/10.22059/jppolicy.2024.99826

ناشر: دانشگاه تهران.

مقدمه

«هوش مصنوعی»[1] نوعی فن‌آوری و شاخه‌ای در علوم رایانه و مطالعه و توسعه نرم‌افزارها و «علم و مهندسی ساخت دستگاه‌های هوشمند» است. در سال‌های اخیر بحث و گفتگو دربارۀ هوش مصنوعی بسیار جدی شده است. درک شرایط پیچیده، شبیه‌سازی فرایندهای تفکری و شیوه های استدلالی انسانی، توانایی یادگیری و کسب دانش و استدلال برای حل مسائل و در چشم‌اندازی کلان، توانایی یک سیستم برای انجام وظایفی مانند یادگیری، برنامه‌ریزی و توانایی تعمیم دادن از دلایل اهمیت‌یافتن جایگاه هوش مصنوعی است. هوش مصنوعی در بسیاری از نقاط جهان تحولاتی را در حوزه عمومی و در فرآیندهای آموزش و مالیات، در زمینه شهرهای هوشمند، سیستم‌های قضایی و کارزارهای انتخاباتی و همچنین در بخش‌های بیمه، بانکداری و سایر بخش‌های تجاری ایجاد کرده است. در واقع، هوش مصنوعی یکی از اجزای اصلی «انقلاب» در حال ظهور در تولید کالاها به نام Industry 4.0 باشد، مفهومی که ترکیبی از اینترنت اشیا، داده‌های بزرگ، رسانه‌های اجتماعی، محاسبات ابری، حسگرها، هوش مصنوعی، رباتیک و کاربرد ترکیبی از این فن‌آوری‌ها در تولید، توزیع و استفاده از کالاهای فیزیکی است. امروزه دستگاه‌های پزشکی هوشمند، تلفن‌ها و رایانه‌های مجهز، منابع انسانی هوش مصنوعی و مدل‌های تصمیم‌گیری شبه قضایی هوش مصنوعی که از نسخه‌های مدل‌های آماری/پیش‌بینی در همه دسته‌های هوش مصنوعی پشتیبانی می‌شوند، بدون دخالت انسان مستقل عمل می کند و می‌توانند الگوهایی را برای تصمیم‌گیری و رسیدن به نتایج متفاوت بر اساس تجزیه و تحلیل داده های مختلف با تقلید از عملکردهای شناختی و رفتار هوشمندانه انسان ها بیاموزد و شناسایی کند. «هوش مصنوعی» به معنای «کنترل و هدایت وظایف خاصی بر اساس صلاحیت فکری انسان» است. علاوه بر این، هوش مصنوعی یک سیستم یکپارچه است که اهدافی نظیر دریافت اطلاعات، اصول استدلال منطقی و قابلیت‌های خود اصلاح را یکپارچه می‌کند (Zekos, 2022: 1). مغز انسان، اگرچه بسیار قدرتمند است، اما بر اساس نوع و میزان آموزش، استفاده از آن محدود است. از این رو، هیچ گاه دو مغز انسانی به طور یکسان فکر نمی کنند، ارزیابی نمی کنند، یا یک مشکل را درک نمی کنند و از این رو ممکن است محدودیت های خاص خود را داشته باشند که با افزایش سن و خستگی بیشتر می‌شوند. برعکس، هوش مصنوعی به نحوی برنامه‌ریزی شده است که مغز انسان را با یادگیری یکسان و با توانایی داشتن چندین ماشین (مغز) که به طور یکسان فکر می‌کنند، بدون تأثیر سن یا خستگی در حالی که کارها را سریعتر و با دقت و کنترل بیشتر انجام می دهند، تکرار کند(Salas-Pilco, 2021: 242). بنابراین، دگرگونی در رابطه «انسان–فن‌آوری»[2] تنوع جدیدی از موضوعات مرتبط با دیجیتالی‌شدن سیاست و ویژگی‌های کاربرد هوش مصنوعی سیاسی در عصر دیجیتال را به همراه دارد. شبکه‌های عصبی مصنوعی[3] از سیستم‌های پردازش اطلاعات بیولوژیکی تقلید می‌کنند و از نورون‌های مصنوعی تشکیل می‌شوند که سیگنال‌ها را در سیستم‌های تقویت‌کننده به یکدیگر منتقل می‌کنند. حاکمیت الگوریتمی از الگوریتم‌ها هم برای نظم دادن به کنش‌های انسانی هم در ساختارهای سیاسی سنتی و هم در ساختارهای سیاسی پیشرفته استفاده می‌کند. وجه مشخصۀ سیاست در شکل جدید آن، این است که حجم قابل توجهی از داده های تجزیه و تحلیل شده توسط الگوریتم ها به نهادها اجازه می‌دهد یا کالاها و خدمات کاملاً جدیدی را ارائه دهند یا کالاهای موجود را با دقت و مقرون به صرفه تر ارائه دهند. فن‌آوری همیشه منبع دائمی عدم قطعیت ها، مخاطرات، تغییرات و در بسیاری موارد اختلال بوده است. علاوه بر این، فن آوری به تنظیم‌کننده‌هایی نیاز دارد تا تصمیمات پیچیده‌ای اتخاذ کنند: اینکه آیا و چه زمانی باید مداخله کنند؟ چه نوع مداخله قانونی به کار گرفته شود؟ پرسش اصلی مقاله حاضر این است که هوش مصنوعی چگونه موجب تحول در توانایی‌های انسان در حوزۀ سیاستگذاری ملی در رابطه با امنیت می‌شود؟ فرضیه محوری این است که با توجه به اینکه استفاده از تجزیه و تحلیل در مقیاس بزرگ از تجزیه و تحلیل داده‌ها و تصمیم‌گیری مدیریتی پشتیبانی می‌کند، پذیرش فن‌آوری‌های جدید نقشی

1. Artificial Intelligence (AI)
2. Human-Technology
3. Artificial Neural Networks

حیاتی در تصمیم‌گیری در سطوح سازمانی و فردی حوزهٔ امنیت ایفا می‌کند. در این مقاله با تمرکز بر این پرسش و فرضیه به صورت هدفمند تلاش خواهد شد پیامدهای ناشی از کاربست هوش مصنوعی در حوزه امنیت مورد نظر قرار گیرد.

ادبیات موجود و ضرورت پژوهش

منابع جدیدی در سال‌های ۲۰۲۲ و ۲۰۲۳ نظیر کتاب *آثار سیاسی، اقتصادی و حقوقی هوش مصنوعی: حکمرانی، اقتصاد دیجیتال و جامعه* (۲۰۲۲)، کتاب به سوی اقتصاد سیاسی بین‌المللی هوش مصنوعی(۲۰۲۱)، مقاله ای با عنوان دموکراتیک‌کردن حکمرانی هوش مصنوعی: از انحصارات فن‌آوری بزرگ تا تعاونی ها که در کتاب. *هوش مصنوعی، آسیب های اجتماعی و حقوق بشر* (۲۰۲۲) و مقاله‌ای با عنوان شوک هوش مصنوعی و قطبی شدن سیاسی–اجتماعی(۲۰۲۴)، چاپ شده است که می‌توان با درک عمیق و هدفمند از میان مباحث آن، بحث‌هایی را در رابطه با هوش مصنوعی و سیاستگذاری عمومی در حوزه‌های دفاعی و امنیتی استنباط کرد. بنابراین، *نوآوری مقالهٔ حاضر* در این است که هیچ منبع مستقل و جامعی در رابطه با هوش مصنوعی و تغییر در حوزه امر سیاسی وجود ندارد و باید با نگرشی دقیق و هدفمند، به ارائه نگرشی تألیفی و اجتهادی در این زمینه و از چشم‌انداز علمی و تجویزی–راهبردی پرداخت. در بیان اهمیت مقاله حاضر می‌توان گفت که شناسایی روندهای جدید علمی، ایستادن در لبه‌های نواوری علمی – تحلیلی و درک پیشدستانه و عمیق تحولات کاربردی و دقیق ناشی از ظهور هوش مصنوعی در حوزه سیاسی یکی از مهمترین اولویت‌های ما برای تحلیل سیاسی، بازتعریف اولویت‌های مفهومی و چشم‌اندازهای جدید نظری در حوزهٔ سیاستگذاری ملی در شرایط نوظهور بین‌المللی است. این فن‌آوری امکان درک شرایط پیچیده، شبیه‌سازی فرایندهای تفکری و شیوه های استدلالی انسانی، توانایی یادگیری و کسب دانش و استدلال برای حل مسائل و در چشم‌اندازی کلان، توانایی یک سیستم برای انجام وظایفی مانند یادگیری، برنامه‌ریزی و توانایی تعمیم دادن را فراهم کرده است.

تاریخچه هوش مصنوعی

«آلن تورینگ»[1] برای اولین بار در سال ۱۹۵۰ درکی از رایانه هایی را مطرح کرد که می‌توانند فکر کنند. در همان مقاله، او بازی تقلید را که امروزه به طور گسترده به عنوان «تست تورینگ»[2] شناخته می شود، پیشنهاد کرد تا ارزیابی کند که آیا یک سیستم رایانه ای هوشمند است یا خیر. اگر در یک مکالمه تایپ شده به زبان طبیعی، نتوانید تشخیص دهید که با یک رایانه چت می کنید یا با یک شخص، در این صورت رایانه امتحان را خوب پس داده است. شش سال بعد، کنفرانس دارتموث در مورد هوش مصنوعی در کالج دارتموث[3]، برگزار شد. در پیشنهاد کنفرانس که در سال ۱۹۵۵ منتشر شد، برای اولین بار از عبارت "هوش مصنوعی" استفاده شده بود. خود کنفرانس یک گردهمایی آزاد از کارشناسانی بود که در تابستان ۱۹۵۶ به تبادل نظر پرداختند. در طول دهه های بعد، بسیاری از کاربردهای کاربردی و مفید هوش مصنوعی در حوزه‌های تخصصی مانند تشخیص پزشکی، طیف‌سنجی، اکتشاف مواد معدنی و طراحی رایانه توسعه یافتند(David Kiggins &Keskin, Tugrul, 2021: V). در واقع، از دهه ۱۹۵۰، دوره‌هایی با عنوان «بهارهای هوش مصنوعی»[4] و «زمستان‌های هوش مصنوعی»[5] وجود داشته است که در آن‌ها علاقه عمومی، دانشگاهی و دولتی به هوش مصنوعی افزایش و سپس کاهش یافته است. با این حال، در دهه گذشته، تحقیقات هوش مصنوعی به طور پیوسته در حال رشد بوده و علایق پژوهشی کاملاً رو به رشد بوده و به پیشرفت های مهمی دست یافته است. چنان که در حال حاضر یکی از دگرگون‌کننده‌ترین نیروهای قرن بیست و یکم، هوش مصنوعی است و عمیقاً جهان را تغییر خواهد داد. با توجه به توسعه سریع هوش مصنوعی در دهه گذشته، هوش مصنوعی چنان نقش بزرگی را در جامعه ما بازی می‌کند که به صورت

1. Alan Turing
2. Turing Test
3. Dart- mouth College, NH
4. AI springs
5. AI winters

عمومی همه از اهمیت آن در سطوح اقتصادی، فن آوری، اجتماعی و سیاسی آگاه شده‌اند. بنابراین، حکمرانی هوش مصنوعی به عنوان بخشی از توسعه طبیعی سیاست‌ها برای ایجاد مقررات و استانداردهای جدید با تمرکز بر تأمین منافع جامعه و اجتناب از تأثیرات منفی آن است. در سال‌های اخیر، بسیاری از دولت‌ها در سراسر جهان چندین سیاست در رابطه با هوش مصنوعی را منتشر کرده‌اند و شروع به توسعه استراتژی‌های هوش مصنوعی ملی کرده‌اند. بنابراین، بسیاری از دولت ها سیاست های استراتژیک ملی هوش مصنوعی را برای هدایت توسعه هوش مصنوعی در کشورهای خود ارائه کرده اند. این سیاست‌ها دستورالعمل‌ها، مقررات و اولویت‌ها را با توجه به شرایط هر کشور توضیح می دهند(Salas-Pilco, 2021: 195-196). متأثر از این تحولات، توسعه فن آورانه در حوزهٔ هوش مصنوعی به مسئله غالب در سیاست ملی و جهانی تبدیل شده است که بر مسائل قدرت و هویت تأثیر می گذارد. الکساندر[1]، هوش مصنوعی را از منظر تکنیک بررسی می‌کند و پیشنهاد می‌کند که هوش مصنوعی به عنوان یک روش یا مجموعه‌ای از روش‌هایی بدانیم که به طور منطقی برای به حداکثر رساندن کارایی مشتق شده‌اند. با حداکثر کارایی، اشاره به میزان تأثیر تکنیک بر عاملیت انسان برای مطابقت با هنجارها و ساختارهای اجتماعی رایج در جامعه است. هر گونه اختلال در منطق جامعه به طور همزمان برای عوامل تحت تأثیر تکنیک برای انطباق رفتار با ساختارهای اجتماعی در حال ظهور مطابق با هوش مصنوعی رخ می دهد. این اختلال ممکن است به عنوان تغییری ظریف و نه رادیکال تجربه شود. بنابراین، هوش مصنوعی تکنیکی را شکل می‌دهد که ساختارهای اجتماعی و رفتار عامل را مطابق با الگوریتم‌های هوش مصنوعی تغییر می‌دهد. هوش مصنوعی با جمع‌آوری میلیون‌ها مشاهدات انتخابی انسان، این داده‌ها را برای تعیین الگوی رفتاری که برای پیش‌بینی انتخاب‌های آینده انسان بر آن تکیه می‌کند، تجزیه و تحلیل می‌کند. قدرت پیش‌بینی عاملیت انسانی به دولت و شرکت‌ها این ظرفیت را می‌دهد که مستقیماً بر انسان‌ها تأثیر بگذارند تا مطابق با منطق دولت و منطق بازار، اهداف امنیت عمومی را انجام دهند. از نظر عملکردی، هوش مصنوعی مجموعه ای از تکنیک ها برای محاسبه احتمال وقوع یک نتیجه است. به این ترتیب، هوش مصنوعی اساساً فن آوری‌ای است که پیش‌بینی‌های احتمالی را انجام می‌دهد. پیش‌بینی، فرآیند پر کردن اطلاعات از دست رفته است. پیش‌بینی اطلاعاتی را که در اختیار دارید، که اغلب «داده» نامیده می‌شود، می‌گیرد و از آن برای تولید اطلاعاتی که ندارید استفاده می‌کند. با ظهور اینترنت و فن آوری‌های رسانه‌های اجتماعی، هزینه اطلاعات به صفر نزدیک می‌شود و در نتیجه هزینهٔ پیش‌بینی کاهش می‌یابد. پیش‌بینی ارزان‌قیمت هوش مصنوعی منجر به پذیرش گسترده این فن‌آوری می‌شود (Keskin, Tugrul & David Kiggins, 2021: 8-11).

تحول در تحلیل داده‌های سیاسی در عصر هوش مصنوعی

در عصر مدرن، داده ها به عنوان مهم‌ترین دارایی که مبارزات سیاسی حول آن می چرخد، جایگزین زمین و ابزار تولید شده است. همان‌طور که هراری[2] می‌گوید: «کسانی که داده ها را کنترل می‌کنند، آینده نه فقط بشریت، بلکه آینده خود زندگی را نیز کنترل می‌کنند». امکان نظارت و کنترل افراد به شرکت‌هایی که بر توسعه هوش مصنوعی کنترل دارند قدرت سیاسی عظیمی می‌دهد. دایر–ویترفورد و همکاران به یک نکته برجسته اشاره می‌کند: «هوش ماشینی نه تنها محصول یک منطق تکنولوژیکی، بلکه همزمان از یک منطق اجتماعی، منطق تولید ارزش اضافی است.» نویسندگان هوش مصنوعی را نقطه اوج فرآیند بیگانگی کارگران از کنترل آنچه می‌سازند، نحوه ساخت آن و روابطشان با همنوعانشان می‌دانند. علاوه بر این، از آنجایی که فن‌آوری‌های جدید باعث منسوخ شدن بسیاری از مشاغل کارگران می‌شود، پیشرفت هوش مصنوعی همچنین منجر به از دست‌دادن ارزش اقتصادی افراد می‌شود. به نظر می‌رسد که در چند دهه آینده، هوش انسانی همچنان در زمینه‌های مختلف از هوش کامپیوتری فراتر خواهد

1. Alexander
2. Yuval Noah Harari

رفت و با شروع ناپدیدشدن مشاغل قدیمی، مشاغل جدید ظاهر خواهند شد. با این حال، این مشاغل جدید به سطح بالایی از تخصص فنی نیاز دارند و همه کسانی را که کار معمولی انجام می دهند بیکار می‌کنند. همانطور که هوش مصنوعی به بهبود ادامه می‌دهد، حتی مشاغلی که به توانایی‌های شناختی بالا (پویا) نیاز دارند، به تدریج ناپدید می‌شوند(Simonc̆ic̆ and Jerele, 2022: 246). سازمان‌های دولتی (مانند سیا و آژانس امنیت ملی در ایالات متحده امریکا[1])، کارزارهای سیاسی (مانند کارزار انتخاب مجدد اوباما در سال ۲۰۱۲) و سایر نهادها به طور فزاینده‌ای از رایانش ابری تجاری و خدمات کلان داده استفاده می‌کنند و «رهبران را در کنار هم قرار می‌دهند. سرمایه‌داری دیجیتال و نظارت دولت برای ایجاد پیوندی که مطمئناً به نفع هر دو طرف خواهد بود. این تنها قدرت سیاسی و اجتماعی این شرکت ها را تقویت می‌کند و نشان‌دهنده گام دیگری در دستور کار آنها برای قرار گرفتن خود به عنوان خدمات ضروری است(Simonc̆ic̆ and Jerele, 2022: 244). هر چند، ظهور بازیگران قدرتمند خصوصی یا فراملی، شبکه‌ها و حوزه‌های هنجاری جدیدی را ایجاد می‌کند که از دولت ملت متمایز است. ظهور نهاد فراملی، بلوک تجاری منطقه‌ای و ایجاد حکمرانی چند سطحی[2]، سیاست‌های در هم تنیده و شبکه‌های سیاستگذاری، موضوع حیاتی ماهیت و نوع مناسب حکمرانی معاصر را برجسته کرده است. سیستم های هوشمندی که قادر به تعیین و انجام وظایف در محیط‌های پیچیده‌تر باشند. پردازنده‌های کامپیوتری به توان فنی لازم برای کوچک‌سازی، پیچیدگی و قدرت لازم برای رشد هوش مصنوعی دست یافته‌اند. علاوه بر این، توسعه چارچوب‌های متن یا منبع باز[3] به توسعه‌دهندگان اجازه می‌دهد تا به طور هم‌افزایی بر روی پلتفرم‌های یکسانی کار کنند تا زیرساخت‌های مورد نیاز دستگاه‌های مجهز به هوش مصنوعی را بسازند و بنابراین پردازنده‌های کامپیوتری متصل به هم که پردازش موازی را انجام می‌دهند توسط شبکه‌های عصبی مصنوعی تحقق می‌یابند. علاوه بر این، شبکه‌ها از داده‌های تاریخی و الگوهای شناخته‌شده یاد می‌گیرند و آن‌ها را در تشخیص بالینی و تجزیه و تحلیل تصویر به کار می‌گیرند. نظام‌های سیاسی می‌توانند از هوش مصنوعی برای تأثیرگذاری بر بخش‌های خاصی از جمعیت خود از طریق دستکاری و تحریف اجتماعی[4]، نظارت، متقاعدسازی و فریب عمل کنند و از هوش مصنوعی برای گسترش حملات سایبری و افزایش تهدید حملات فیزیکی و تجاوز تدریجی به حریم خصوصی افراد استفاده شود(Zekos, 2022: 5-6). در نتیجه، اگر این فن‌آوری‌ها در دست عده کمی باقی بمانند، هوش مصنوعی پتانسیل تشدید نابرابری های اجتماعی را دارد. کمیسیون اروپا در سال ۲۰۱۸ این دیدگاه را اتخاذ کرده است که «هیچ کس [نباید] در تحول دیجیتال عقب بماند» و همه باید فرصت بهره مندی از انقلاب صنعتی چهارم را داشته باشند. با توجه به رقابت سایر مناطق، و همچنین برای پرداختن به موضوع نابرابری بین کشورها، اتحادیه اروپا رویکرد خود را برای «هوش مصنوعی برای اروپا» ارائه کرد که بر نیاز به توسعه هوش مصنوعی در اروپا تاکید می‌کند و در عین حال بر اساس رویکردی ارزش‌محور، انسان را مخاطب قرار می‌دهددر همین حال، اندیشکده AI Now مستقر در ایالات متحده یک «بحران اخلاقی» را در هوش مصنوعی با استناد به مسائلی مانند بهره برداری از داده های خصوصی کاربران در تحقیق و توسعه مشخص کرده است. روند اخیری که به طور فزاینده‌ای پذیرفته شده است، دموکراتیک‌کردن هوش مصنوعی است و هدف آن این است که هوش مصنوعی را برای افراد بیشتری در دسترس قرار دهد (Clough and Otterbacher, 2023: 402). بنابراین، ما باید فن‌آوری هوش مصنوعی را دموکراتیک کرده و آن را به طور گسترده در دسترس قرار دهیم. ایلان ماسک می‌گوید: «و این دلیلی است که ... ما OpenAI را ساختیم تا به گسترش فن‌آوری هوش مصنوعی کمک کنیم تا در دستان عده‌ای معدود متمرکز نشود. مأموریت واقعی ما جشن‌گرفتن هیچ یک از این پیشرفت‌های

1. National Security Agency (NSA)
2. Multilevel Governance
۳. Open-Source : علاوه بر این، یک رقابت دیجیتالی جهانی وجود دارد که رقابت جهانی بین اشکال دموکراتیک و اقتدارگرایانه حکمرانی یکی از ابعاد ضروری رابطه بین دیجیتالی شدن و دموکراسی در سطح جهانی است. شبکه‌های دیجیتالی فعالیت‌ها را با سازمان‌دهی زنجیره‌های تامین جهانی و ایجاد اشکال پیچیده حکمرانی جهانی با ارائه فرصت‌های جدید برای مشارکت دیجیتالی فعال، مسئولیت‌پذیری و شفافیت که دموکراسی را افزایش می‌دهد، هماهنگ می‌کنند، اما همچنین به بازیگران نخبگان ثروتمندتر یا متخصص‌تر اجازه می‌دهند تا به‌طور شخصی از آنها بهره‌برداری کنند (Zekos, 2022: 388).
4. Social Manipulation

بزرگ تحقیقاتی نیست، بلکه دموکراتیزه‌کردن هوش مصنوعی است تا هر توسعه دهنده بتواند این برنامه‌ها را بسازد» (Clough and Otterbacher, 2023: 402). . البته بیشتر علاقه فعلی به هوش مصنوعی بر یادگیری ماشین متمرکز است. اصل ساده این است: به یک شبکه عصبی مصنوعی بزرگ هزاران نمونه از تصاویر یا اشکال دیگر داده را نشان دهید و یاد می‌گیرد که آن نمونه‌ها را با طبقه‌بندی صحیح آنها مرتبط کند. مهمتر از همه، شبکه یاد می‌گیرد که تعمیم دهد به طوری که وقتی با یک تصویر یا الگوی داده‌ای ارائه می‌شود که قبلاً ندیده است، بتواند به طور قابل اعتماد آن را طبقه‌بندی کند، مشروط بر اینکه نمونه‌های مشابهی در مجموعه آموزشی وجود داشته باشد. این یک تکنیک قدرتمند است که به عنوان مثال، یک ماشین بدون راننده را قادر می‌سازد تا علامت توقف را در خیابان تشخیص دهد. با این حال، مهم است که به یاد داشته باشید که الگوریتم معنای آن طبقه‌بندی را درک نمی‌کند. فراتر رفتن از یک برچسب طبقه‌بندی ساده نیازمند هوش مصنوعی مبتنی بر دانش است. این همان هوش مصنوعی است که ریشه در سیستم های خبره ای دارد که در دهه های بعد از کنفرانس دارتموث شروع به تکامل کردند. با همه‌گیری کووید-۱۹[1] در سال‌های ۲۰۲۱-۲۰۱۹، هوش مصنوعی با حمایت از دانشمندان در برنامه‌های کاربردی که شامل استفاده مجدد از داروهای موجود، تفسیر تشخیصی تصاویر ریه، تشخیص افراد آلوده بدون علامت، شناسایی عوارض جانبی واکسن و پیش‌بینی شیوع عفونت بود، ارزش خود را نشان داد(Keskin, Tugrul & David Kiggins, 2021: vi-vii). بنابراین مهم است که سیستم‌های هوش مصنوعی از چه طریق، توسط چه کسی و بر اساس چه داده‌هایی ساخته می‌شوند و این چه پیامدهایی برای تک تک کاربران دارد. چنان که در حال حاضر، توسعه اکثر برنامه های کاربردی هوش مصنوعی تنها در ۹ شرکت بزرگ – گوگل[2]، اپل[3]، آمازون[4]، فیس بوک[5]، آی بی ام[6]، مایکروسافت[7] در ایالات متحده، تنسِنت[8]، بایدو[9]، و علی بابا[10] در چین انجام می شود. تعهد بسیاری از شرکت‌های بزرگ به افزایش سود برای سهامداران‌شان همیشه با آنچه که برای رفاه، آزادی‌های فردی و ارزش‌های دموکراتیک بخش بزرگی از جمعیت جهان بهترین است مطابقت ندارد. شن[11] (۲۰۱۷) اشاره می کند که در حالی که حدود ۷.۹ میلیارد نفر در این سیاره زندگی می‌کنند، تنها ۱۰۰۰۰ نفر در هفت کشور در حال نوشتن کد برای تمام هوش مصنوعی هستند که در حال توسعه است. اگر انسان‌ها در مسیر ایجاد هوش عمومی مصنوعی[12] هستند که نشان‌دهنده شرایط انسانی است که بر کل بشریت تأثیر می‌گذارد، پس هوش مصنوعی و هوش عمومی مصنوعی در حال توسعه نیاز دارند که طیف وسیعی از شرایط انسانی را در نظر بگیرند، نه صرفاً دایره کوچکی از افرادی که توانسته‌اند به آموزش نخبگان (حرفه‌ای)[13] دسترسی پیدا کنند یا موقعیت بسیار مطلوبی را در یکی از «۹ شرکت بزرگ» به دست آورند (Simonc˘ic˘ and Jerele, 2022: 239-240). از این منظر، فن‌آوری و توسعه آن یکی از عوامل اساسی جهانی‌شدن بوده و نوآوری در فن‌آوری اطلاعات و ارتباطات فاصله بین مردم، کشورها، قاره‌ها و حتی فراتر از آن را کاهش می‌دهد. جهانی‌شدن اطلاعات بیش از هر زمان دیگری در تاریخ بشر، دانش بیشتری را در دست افراد بیشتری قرار داده است. در بسیاری از جوامع، فضای سایبری به دلیل دشواری در نگهداری اطلاعات، نقش رهایی بخش داشته است. از آنجایی که سیستم‌های هوش مصنوعی نقش بیشتری در تولید محتوا ایفا می‌کنند، تلاش‌ها برای مهار از طریق محلی‌سازی داده‌ها، فیلترکردن، یا کاهش سرعت جریان اطلاعات، خطر بی‌ثباتی پایه‌های اقتصاد دیجیتال را به همراه خواهد داشت.با این حال، به نظر می‌رسد که بسیاری از راه‌حل‌های

1. COVID-19
2. Google
3. Apple
4. Amazon
5. Face-book
6. IBM
7. Microsoft
8. Tencent
9. Baidu
10. Alibaba
11. Shen
12. Artificial General Intelligence (AGI)
13. Elite Education

پیشنهادی به احتمال زیاد صرفاً دایره چند نفر در رأس قدرت را گسترده‌تر می‌کنند، بدون اینکه هیچ قدرت واقعی را به آن‌هایی که در جایگاه‌های پایین‌تری هستند تغییر دهند. در نتیجه، در عین حال که هوش مصنوعی مبرم‌ترین و نزدیک‌ترین نگرانی برای گونه ما است که گاه به عنوان ابزاری برای دستیابی به رفاه بی‌سابقه بشری به تصویر کشیده شده است، اما گاهی دیگر، به عنوان بزرگترین تهدید برای گونه ما، با پتانسیل تضعیف حقوق و آزادی‌های بشر، از بین‌بردن هویت انسانی، و تهدید انقراض انسان توصیف می شود. از این رو، اینترنت اشیا مجهز به هوش مصنوعی نقش مهمی در توسعه چنین «اقتدارگرایی قوی»[1] ایفا می کند. در واقع، برخی استدلال می‌کنند که فن‌آوری اطلاعات دیجیتال به نفع استبداد است، زیرا حکومت‌های استبدادی در برداشت و استفاده از جریان‌های وسیعی از داده‌های شخصی‌شده بدون محدودیت‌های آزادی مدنی آزاد هستند. اورول[2] می ترسید که حقیقت از ما پنهان شود. هاکسلی[3] می‌ترسید که حقیقت در دریای بی‌ربطی غرق شود. همانطور که هاکسلی خاطرنشان کرد کسانی که همیشه آماده مقابله با استبداد هستند، «اشتهای تقریبا بی‌پایان انسان برای حواس‌پرتی را در نظر نگرفتند». درست همان‌طور که امپراتوران روم باستان «نان و سیرک» می‌دادند تا شهروندان خود را مطیع نگه دارند، « دولت‌های هوشمند» مجهز به اینترنت اشیا نیز ظرفیت افزایش مصرف و حواس‌پرتی را دارند و در عین حال مخالفت‌ها را مهار می‌کنند. این همه حواس پرتی بیش فعال باعث مصرف سریع و تکانشی می شود. رشد شناختی و انضباط مورد نیاز برای پرورش مهارت های مدنی را تقویت نمی‌کند (Paul Thiele, 2021: 50-51). همچنین، فن‌آوری‌های دیجیتال در اینترنت اشیا در سطوح فوق‌انسانی از اتصال، سرعت و عملکرد عمل می‌کنند و به تلاش‌های انسانی رو به کاهشی نیاز دارند. برای میلیاردها نفر از مردمی که از اینترنت اشیا استفاده می‌کنند، نیاز و فرصت برای تمرین حافظه، استدلال، توانمندی، قضاوت و استعدادهای اجتماعی متنوع به طور پیوسته در حال کاهش است. در حالی که اینترنت اشیا ظرفیت بی‌سابقه‌ای برای ضبط و مدیریت داده‌ها، شبکه‌سازی و عملکرد نشان می‌دهد، افراد در این وب دیجیتال ممکن است اختیار بسیار کمی داشته باشند. انسان‌ها موضوع بسیاری از داده‌های جمع‌آوری‌شده و تجزیه‌وتحلیل‌شده باقی خواهند ماند (به عنوان مثال، داده‌های بهداشتی تولید شده توسط افرادی که از حسگرهای بیومتریک استفاده می‌کنند) Paul). (Thiele, 2021: 44 با این حال، ماشین‌ها به اندازه انسان‌ها از نظر فکری همه‌کاره نیستند، اما سیستم‌های هوش مصنوعی از نظر حافظه کوتاه‌مدت و بلندمدت، همراه با ظرفیت‌شان برای دستیابی به یک سری عملیات منطقی، قابل اعتمادتر هستند. باید در نظر داشت که مزایای قضات انسانی نسبت به قضات ماشینی این است که قضات انسانی می‌توانند روی داده‌های کمتر قابل اندازه‌گیری، مانند تفاوت‌های ظریف شرایط یک متهم یا محکومیت‌های قبلی حساب کنند. قضات انسانی یا داوران حس انسانی ایجاد تغییرات به افراد برای آینده ای بهتر را دارند، در حالی که قضات هوش مصنوعی رابطه و نتیجه داده‌ها را به عنوان یک نتیجه آماری و نه چیز دیگر، به صورت مکانیکی نگاه می‌کنند (Zekos, 2022: 18). بر اساس گزارش کمیته فرعی ۲۰۲۰، فیسبوک، شرکتی که درآمد خود را عمدتاً از فروش آگهی‌های تبلیغاتی به دست می‌آورد، در تبلیغات آنلاین و همچنین در بازارهای شبکه‌های اجتماعی قدرت انحصاری دارد. از سوی دیگر، آمازون قدرت انحصاری بر اکثر فروشندگان شخص ثالث خود (که عموما به عنوان "شریک" و پشت درهای بسته به عنوان "رقبای داخلی" توصیف می شوند) و همچنین بر بسیاری از تامین کنندگان خود دارد. بر اساس ارقام رسمی، سهم بازار این شرکت از تجارت الکترونیک ایالات متحده حدود ۴۰ درصد است، اما بر اساس اطلاعاتی که کارکنان کمیته فرعی در طول تحقیقات خود جمع‌آوری کرده اند، این رقم نزدیک به ۵۰ درصد یا بیشتر است. طبق گزارش‌ها، این شرکت حدود ۶۵ تا ۷۰ درصد از کل فروش بازار آنلاین ایالات متحده را کنترل می کند. اپل قدرت انحصاری بر توزیع نرم‌افزار در دستگاه‌های iOS را در اختیار دارد و به این شرکت اجازه می‌دهد تا سودهای فوق‌العاده‌ای از فروشگاه App و کسب و کار خدمات آن کسب کند. این سود از طریق استخراج رانت از توسعه دهندگانی به دست می آید که یا افزایش قیمت را به مصرف کنندگان منتقل می کنند یا سرمایه‌گذاری در خدمات جدید را کاهش می دهند. به گفته کارکنان کمیته فرعی: «ممنوعیت

1. Robust Authoritarianism
2. George Orwell (Eric Arthur Blair)
3. Aldous Huxley

اپل از فروشگاه‌های برنامه‌های رقیب و پردازش پرداخت جایگزین، رقابت را قفل می‌کند و سود اپل را از اکوسیستم اسیر توسعه دهندگان و مصرف‌کنندگان افزایش می‌دهد. در نهایت، طبق این گزارش، گوگل که به عنوان نوعی زیرساخت برای خدمات ضروری آنلاین عمل می کند، انحصار بازار جستجوی عمومی و جستجوی تبلیغات آنلاین را در اختیار دارد. (Simonˇicˇ and Jerele, 2022: 242). برای مثال، این شرکت مالک کروم، محبوب‌ترین مرورگر جهان است. یوتیوب؛ Google Mapsکه با آن بیش از ۸۰ درصد از بازار خدمات نقشه‌برداری ناوبری و Google Cloud را در اختیار دارد که این شرکت امیدوار است با آن بر اینترنت اشیا تسلط یابد .شرکت‌های فن آوری بزرگ کنونی نه تنها انحصاری بر پایگاه کاربر خود در زمینه‌های مربوطه خود دارند – که به آنها امکان می‌دهد مقادیر زیادی از داده‌های دیجیتال شخصی (همچنین به عنوان کلان داده Big Data نیز شناخته می‌شود) – و درآمد تبلیغاتی را جمع‌آوری کنند، آنها فعالانه به عنوان ارائه دهندگان محاسبات ابری روی دستیابی به موقعیتی هژمونیک کار می‌کنند. در پنج یا چند سال اخیر، محاسبات ابری به یک سرویس مهم‌تر و سریع‌ترین بخش در حال رشد در بخش فن آوری اطلاعات و پلتفرم‌های فن‌آوری تبدیل شده است. با توجه به افزایش تقاضا برای قدرت محاسباتی بیشتر برای اجرای الگوریتم‌های یادگیری ماشین و ذخیره مقادیر زیادی داده، شرکت‌ها به طور فزاینده‌ای به سمت ابر روی می‌آورند. رایانش ابری را به عنوان "الگویی برای فعال کردن دسترسی به شبکه بر اساس تقاضا به یک مجموعه مشترک از منابع محاسباتی قابل تنظیم و همه جا حاضر (به عنوان مثال، شبکه ها، سرورها، ذخیره سازی، برنامه ها و خدمات) تعریف می‌کند که می‌تواند به سرعت انجام شود و ذخیره‌سازی، پردازش و توزیع داده‌ها، برنامه‌ها و خدمات از راه دور را برای افراد و سازمان ها امکان‌پذیر می‌کند. شرکت‌های پیشرو در محاسبات ابری در حال حاضر، خدمات وب آمازون ، یکی از شرکت‌های تابعه آمازون، که در حال حاضر ۳۲ درصد از سهم بازار را در اختیار دارد، مایکروسافت آژور با ۲۰ درصد، موتور محاسباتی گوگل (۹ درصد) با غول‌های چینی علی‌بابا (۶ درصد) و تنسِنت (۲ درصد) هستند (Simonˇicˇ and Jerele, 2022: 243). توزیع مالکیت هوش مصنوعی در میان شرکت های فراملیتی و ایالات متحده ممکن است به عنوان بازتابی از تکنیک تغلب لیبرالیسم در جامعه جهانی در نظر گرفته شود.

کارکردهای امنیتی و دفاعی هوش مصنوعی: اولویت‌یابی امنیت انسانی

یکی از حوزه‌هایی که هوش مصنوعی در آن کاربرد مهمی پیدا کرده است، امنیت به معنای وسیع آن است، هم برای صنعت و هم در دولت. این حوزه ها شامل امنیت دفاعی یا نظامی، امنیت انسانی (اطلاعات، امنیت داخلی و امنیت اقتصادی و مالی)، امنیت شغلی، امنیت بهداشتی و امنیت سایبری (امنیت اطلاعات و اینترنت اشیا) است. این حوزه‌های کاربردی بی‌شمار و ناتوانی بشر در اعمال کنترل کامل مانند ماشین‌ها، افراد جامعه امنیتی را وادار می‌کند تا به آسیب‌پذیری‌های احتمالی و شکاف‌های امنیتی ناشی از این فن آوری در حال تکامل فکر کنند (Salas-Pilco, 2021: 242). بنابراین کشورها از شهروندان خود، منافع آنها در داخل و خارج از کشور و ثبات سیاسی خود در برابر استفاده های مخرب یا متقلبانه احتمالی از هوش مصنوعی محافظت می کنند. برخی از تحلیلگران ابراز نگرانی می‌کنند که هوش مصنوعی دارای پتانسیل مخرب چشمگیر است، به طوری که یک معاهده جهانی برای مدیریت مسابقات تسلیحاتی هوش مصنوعی و محافظت در برابر پتانسیل مخرب اولین جنگ هوش مصنوعی ضروری است. کارشناسان به طور فزاینده‌ای نگرانی‌هایی را در مورد خطراتی که سیستم‌های هوش مصنوعی پیشرفته ممکن است برای صلح و امنیت ایجاد کنند، ابراز کرده‌اند. ایلان ماسک هشدار داد که هوش مصنوعی این پتانسیل را دارد که از سلاح‌های هسته‌ای خطرناک‌تر باشد. استیون هاوکینگ نگران بود که هوش مصنوعی به معنای پایان نوع بشر باشد. یک شماره ویژه اخیر بولتن دانشمندان اتمی شامل چندین هشدار در مورد مسابقه تسلیحاتی هوش مصنوعی آینده بود. برای مثال، در آستانه انتخابات اندونزی در سال ۲۰۱۹ مشهود است، جایی که اینستاگرام و توییتر (شبکه X فعلی) مملو از اتهامات توطئه‌آمیز درباره سیاستمداران خیانتکار بودند که باید با هر وسیله‌ای از جمله از طریق ترور، تهدید و کشتار از پیروزی در صندوق‌های رأی جلوگیری می‌کردند. در میانمار،

جنایات مداوم علیه گروه اقلیت روهینگیا از طریق عکس‌نوشته‌های ناسیونالیستی در توییتر و فیس بوک تقویت شده است که روهینگیا را خارجی‌های خطرناکی معرفی می کنند که یک تهدید وجودی برای یکپارچگی و بقای کشور هستند و باید ریشه کن شود. در این موارد و بسیاری موارد دیگر، رسانه های اجتماعی نقش تعیین‌کننده ای در تداوم غیرانسانی‌سازی و تسهیل خشونت داشته اند. در حالی که، هوش مصنوعی و تحقیقات علمی اجتماعی در مورد خشونت سیاسی می‌تواند به منظور کمک به پیشگیری عملی از درگیری به کار گرفته شود. سیستم‌های هوش مصنوعی می‌توانند به‌طور قابل توجهی کار صلح‌سازی را به روش‌های خاص ارتقا دهند، زیرا هوش مصنوعی ابزارهای منحصربه‌فردی را برای شناسایی و تحلیل روندها و تهدیدات نوظهور در رابطه با حجم عظیمی از داده‌های بلادرنگ در اینترنت، بسیار فراتر از ظرفیت‌های اکثر سیستم های هشدار اولیه خشونت سیاسی فراهم می‌آورد. این که چگونه انتشار اطلاعات نادرست، شایعات و دروغ‌پردازی‌ها در رسانه‌های اجتماعی – اساساً تبلیغات نفرت – در زمینه‌های سیاسی از قبل ناپایدار می‌تواند به عنوان شاخص‌های هشدار اولیه خشونت در مقیاس بزرگ قریب‌الوقوع عمل کند (Yankoski, et.al, 2021: 148).بر این اساس، حوزه کاربردهای امنیتی که در آن هوش مصنوعی هم توسط صنعت و هم توسط دولت استفاده شده است شامل موارد زیر است:

الف. امنیت نظامی

امنیت نظامی یکی از ابزارهای موجود در سیاست بین‌الملل است که به دولت–ملت اجازه می‌دهد تا برای پیشگیری از درگیری، مدیریت بحران، و فعالیت‌های صلح‌ساز درخواست دهد تا با مشارکت مشترک در فعالیت‌های کنترل تسلیحات، مدیریت مرز، مبارزه با تروریسم، پلیس، درگیری و اصلاحات نظامی، امنیت را ارتقا بخشیده و تقویت کند. مانند بسیاری از جنبه‌های زندگی انسان، امنیت نظامی یکی از حوزه‌هایی است که هوش مصنوعی در آن تأثیر بزرگی خواهد داشت. اگرچه کاربردهای احتمالی هوش مصنوعی در ارتش بسیار زیاد است، اما برخی از آنها، که در آنها از هوش مصنوعی استفاده می شود و بر عملکرد امنیت نظامی متعارف تأثیر می گذارد عبارتند از:

آ. ربات های زمینی که از راه دور کنترل می شوند و از راه دور توسط انسان کنترل می شوند.

ب تسلیحات خودمختار مانند وسایل نقلیه هوایی بدون سرنشین، وسایل نقلیه بدون سرنشین زیر آب و وسایل نقلیه هوایی خودران که روش‌های ارسال نظارت و محموله‌ها را تغییر می‌دهند.

ج سوله‌ها از روبات‌های زیردریایی مستقل تشکیل شده‌اند که به اعوجاج‌های کوچک در میدان مغناطیسی زمین حساس هستند که می‌تواند تلاش‌ها برای پنهان کردن زیردریایی‌ها را پیچیده کند.

د انبوهی از زیردریایی های بدون سرنشین که می توانند قواعد کنونی جنگ دریایی را تغییر دهند.

ه. استفاده از هوش مصنوعی در لجستیک، اطلاعات و نظارت، و حتی طراحی تسلیحات، نحوه انجام این فعالیت‌ها را متحول خواهد کرد.

ک. نظارت بر تهدید و آگاهی از موقعیت برای به دست آوردن و پردازش اطلاعات برای پشتیبانی از طیف وسیعی از فعالیت های نظامی .

ب. امنیت انسانی

جنبه‌های مختلف امنیت انسانی توسط هوش مصنوعی مورد توجه قرار می گیرد. فهرست به قدری طولانی است که بحث در مورد هر یک از آنها در اینجا غیرممکن است، اما برخی از آنها که ضروری تلقی می شوند و جامعه را تغییر می‌دهند عبارتند از:

۱ .استفاده از داده‌های شناسایی بیومتریک انسانی برای امنیت اجتماعی، کمک‌های بشردوستانه، تأیید فیزیکی، برای نام بردن از چند مورد، نحوه مدیریت و رسیدگی به انسان‌ها را در جامعه تغییر می‌دهد. اگرچه چنین استفاده ای تقلب ها را کاهش می دهد، اما می توان از آن برای سرکوب سیاسی استفاده کرد.

۲ .فن‌آوری تشخیص چهره

۳ .راه‌حل‌های امنیت انسانی با استفاده از هوش مصنوعی با استفاده از تحلیل داده‌ها، یادگیری ماشین و الگوریتم‌های تئوری بازی برای جلوگیری از جرایم با ارائه تحلیل‌های توصیفی، تشخیصی، پیش‌بینی‌کننده و تجویزی که از طریق استفاده ازCompStat، Armorway، و DARMS دیده می‌شود، توسعه می‌یابند. چنین برنامه‌هایی هم تهدیدهای داخلی و هم تهدیدات امنیتی محوطه فیزیکی را برای یک سازمان فراهم می‌کنند.

۴. امنیت انسانی به دلیل گرم شدن کره زمین، ارتباط رو به رشد به دلیل رسانه های اجتماعی، تغییر در نیروی کار و تولید به دلیل پیشرفت فن آوری، پتانسیل ایجاد چالش‌های سیستمی مانند جنگ، اختلالات اجتماعی، اقتصادی یا سیاسی را دارد. پیش‌بینی چنین خطرات احتمالی برای پاسخگویی موثر با استفاده از هوش مصنوعی امکان پذیر بوده است.

۵. استفاده از هوش مصنوعی، کلاهبرداری از کارت اعتباری را کاهش داده است(Salas-Pilco, 2021: 243-145) . با وابستگی متقابل و ارتباط متقابل بین حوزه‌های هوش مصنوعی کشورهای مختلف، شرکت‌ها، دانشگاه‌ها، سازمان‌های جامعه مدنی، افراد و حتی نهادهای دولتی در کشورهای مختلف ممکن است در زمینه‌های تحقیقاتی هوش مصنوعی، از پردازش زبان طبیعی تا تشخیص تصویر، همکاری کنند. بسیاری از اهداف تحقیقاتی مرتبط با هوش مصنوعی این گروه‌های مختلف حداقل از نظر فن‌آوری، نسبتاً همسو هستند و مبتنی بر بازی حاصل جمع صفر نیستند.علاوه بر این، بیشتر تحقیقات جهانی هوش مصنوعی نیز منبع باز هستند و عمدتاً در حوزه عمومی در سایت‌های اشتراک‌گذاری کد مانندGitHub، سایت‌های اشتراک‌گذاری داده مانند Kaggleو سایت‌های اشتراک‌گذاری کاغذ مانند Arxiv.org رخ می‌دهند. هرچند همیشه استثناهایی وجود دارد؛ مثلاً وقتی کشورها به طور مخفیانه سلاح های خودمختار مرگبار را در مراکز تحقیقاتی نظامی تولید می‌کنند ,Rogerson and Sherman). (65 :2021روشن است که کشورهایی که صلاحیت ساختن سیستم‌های هوش مصنوعی به تنهایی را دارند نیز در حوزه سیاستگذاری مشابه رفتار می‌کنند، اگرچه همه آنها این موضوع را انکار می‌کنند. از این رو در مقابل وابستگی متقابل و ارتباط متقابل بین حوزه های هوش مصنوعی کشورهای مختلف، ، ناسیونالیسم فنی وجود دارد و به سرعت حمایت بیشتری برای ایجاد مکانیسم های کنترلی برای پیکربندی بازار مبتنی بر سیاست به دست می‌آورد. علاوه بر ناسیونالیسم فنی، حمایت‌گرایی یک عامل اضافی است که احتمال یک نتیجه عمومی را به نفع چندپارگی نامطلوب افزایش می‌دهد و بنابراین، نهادهای اتحادیه اروپا و ایالات متحده در مکانیسم‌های موجود برای نظارت بر سرمایه‌گذاری خارجی در بخش‌های کلیدی و در نظر گرفتن تدابیر حفاظتی برای فن آوری‌های مورد نظر تجدیدنظر می‌کنند .(Zekos, 2022: 385) . در چارچوب سیاست‌های ملی، در اکتبر ۲۰۱۶، دولت باراک اوباما، رئیس جمهور ایالات متحده، دو سند مهم در مورد استراتژی هوش مصنوعی منتشر کرد. اولین مورد، آماده‌سازی برای آینده هوش مصنوعی، توصیه‌هایی را به آژانس‌های فدرال و سایر بازیگران برای توسعه بهتر و آمادگی برای آینده مبتنی بر هوش مصنوعی ارائه کرد. دوم، برنامه استراتژیک تحقیق و توسعه هوش مصنوعی ملی، یک برنامه استراتژیک برای سرمایه‌گذاری فدرال در توسعه هوش مصنوعی ارائه کرد. در ژوئن ۲۰۱۹ دولت ترامپ به برنامه استراتژیک ملی تحقیق و توسعه هوش مصنوعی به طور خلاصه به بهبود آموزش هوش مصنوعی اشاره کرد، اما بیشتر بر هوش مصنوعی و آموزش در زمینه توسعه نیروی کار متمرکز بود در همین حال، بودجه دولت ایالات متحده برای تحقیقات هوش مصنوعی به شدت در ارتش متمرکز شده است، از جمله به این دلیل که بسیاری از تحقیقات هوش مصنوعی ارتش بر پشتیبانی لجستیکی و فرماندهی –نه صرفاً سلاح‌های خودمختار– متمرکز است.(Rogerson and Sherman, 2021: 66). همچنین، دولت کانادا استراتژی هوش مصنوعی پان–کانادایی خود را با بودجه‌ای معادل ۱۲۵ میلیون دلار کانادا (۹۵ میلیون دلار آمریکا) در مارس ۲۰۱۷ منتشر کرد که به تفصیل یک برنامه استراتژیک پنج ساله (۲۰۱۷–۲۰۱۸ تا ۲۰۲۱–۲۰۲۲) است که دارای چهار هدف اصلی است: (الف) افزایش تعداد محققان و فارغ‌التحصیلان برجستهٔ هوش مصنوعی. در کانادا؛ (ب) ایجاد سه مرکز مهم به هم پیوسته برای هوش مصنوعی در ادمونتون، مونترال و تورنتو. (ج) توسعه رهبری فکری جهانی در زمینه پیامدهای اقتصادی، اخلاقی و قانونی پیشرفت‌های هوش مصنوعی؛

و (د) حمایت از یک جامعه ملی تحقیقاتی هوش مصنوعی. این اهداف در نظر گرفته شده اند تا کانادا را به عنوان یک کشور پیشرو در جهان از نظر هوش مصنوعی و نوآوری، همانطور که توسط موسسه تحقیقات پیشرفته کانادا (CIFAR) بیان داشته است، ارتقا دهند. اولویت‌های سیاست‌های استراتژیک کانادا عمدتاً تحقیق و توسعه استعدادها را در اولویت قرار می‌دهد تا کانادا را به عنوان مقصدی پیشرو در جهان برای شرکت‌هایی که به دنبال سرمایه‌گذاری در هوش مصنوعی و نوآوری هستند قرار دهد (Salas-Pilco, 2021: 198). در مارس ۲۰۱۸، رئیس جمهور امانوئل ماکرون، برنامه استراتژیک هوش مصنوعی فرانسه را با نام هوش مصنوعی برای بشریت: استراتژی فرانسوی برای هوش مصنوعی ارائه کرد. این طرح استراتژیک هوش مصنوعی دارای چهار جزء اصلی است: (الف) تقویت اکوسیستم هوش مصنوعی برای جذب بهترین استعدادها (ب) توسعه یک سیاست داده باز در بخش هایی که فرانسه در حال حاضر پتانسیل برتری دارد، مانند مراقبت های بهداشتی. (ج) ایجاد یک چارچوب قانونی و مالی به نفع ظهور "قهرمانان هوش مصنوعی"، بنابراین از پروژه های تحقیقاتی هوش مصنوعی و استارت آپ ها حمایت می‌کند و (د) اجرای مقررات و اصول اخلاقی هوش مصنوعی برای اطمینان از وجود بهترین استانداردهای مقبولیت برای شهروندان (Salas-Pilco, 2021: 200). در مارس ۲۰۱۷، ژاپن استراتژی فن‌آوری هوش مصنوعی را که توسط شورای راهبردی فن آوری هوش مصنوعی تدوین شد، منتشر کرد. این سند نقشه راه صنعتی‌شدن کشور را در سه مرحله ترسیم می‌کند. مرحله اول استفاده و کاربرد هوش مصنوعی مبتنی بر داده است که در حوزه‌های مختلف توسعه یافته است (تقریباً تا سال ۲۰۲۰). مرحله دوم استفاده عمومی از هوش مصنوعی و داده‌های توسعه یافته در دامنه های مختلف (تقریباً تا سال ۲۰۲۵ تا ۲۰۳۰) است. مرحله سوم ایجاد اکوسیستم هایی است که با اتصال دامنه‌های متعدد (پس از تقریباً ۲۰۲۵ تا ۲۰۳۰) ساخته شده‌اند. استراتژی فن آوری هوش مصنوعی ژاپن دارای اهداف زیر است: (الف) ترویج پروژه های تحقیق و توسعه مبتنی بر همکاری صنعت، دانشگاه و دولت؛ ب) تقویت منابع انسانی؛ (ج) ارائه نگهداری محیطی برای داده‌ها و ابزارهای متعلق به صنعت، دانشگاه و دولت. (د) ارائه پشتیبانی از راه اندازی؛ و (ه) ارتقاء درک توسعه فن‌آوری هوش مصنوعی در میان ارائه دهندگان و کاربران. همچنین دارای چهار اولویت است: (۱) بهره وری. (۲) بهداشت، مراقبت‌های پزشکی و رفاه؛ ۳) تحرک (حمل و نقل)؛ و (۴) امنیت اطلاعات. از دیدگاه ژاپنی‌ها، بزرگترین چالش مربوط به بودجه یا رقابت بین‌المللی نیست، بلکه تغییر ذهنیت فرهنگی یا سازگاری فرهنگی است. اولویت اصلی هوش مصنوعی دولت ژاپن تحقیق و توسعه با هدف صنعتی‌سازی هوش مصنوعی است که به ستون "انقلاب بهره وری" تبدیل خواهد شد.(Salas-Pilco, 2021: 200-203)

در جمهوری کره، در دسامبر ۲۰۱۶، وزارت علوم، فن‌آوری اطلاعات و ارتباطات و برنامه‌ریزی آینده کره، طرح جامعی با عنوان طرح جامع میان‌مدت تا بلندمدت در آماده‌سازی برای جامعه اطلاعاتی هوشمند: مدیریت انقلاب صنعتی چهارم منتشر کرد. این سند چشم‌انداز دولت کره را برای «تحقق یک جامعه اطلاعاتی هوشمند با محوریت انسان» ترسیم می‌کند. مسئولیت‌های اصلی آن عبارتند از (الف) تقویت اکوسیستم سالم رقابت بر سر فن‌آوری اطلاعات و خدمات نوآورانه و هوشمند. ب) افزایش خلاقیت، درک فن‌آوری اطلاعات هوشمند، و دیگر قابلیت‌های اصلی لازم برای هدایت جامعه به آینده؛ ج) حمایت از توسعه فن‌آوری‌ها و منابع انسانی؛ و (د) توسعه زیرساخت برای حمایت از تلاش‌های کارآفرینانه و سرمایه‌گذاری خصوصی با استفاده از فن‌آوری اطلاعات هوشمند در خدمات عمومی. همچنین، در ماه می ۲۰۱۸، استراتژی تحقیق و توسعه هوش مصنوعی برای تحقق کره هوشمند (I – Korea) منتشر شد. این استراتژی سه هدف را برجسته می کند که باید طی پنج سال آینده (۲۰۱۸–۲۰۲۲) به آن دست یافت: (الف) ارائه فن‌آوری هوش مصنوعی در سطح جهانی، (ب) پرورش بهترین استعدادهای هوش مصنوعی و ج) ایجاد یک زیرساخت هوش مصنوعی باز و نوآورانه (هاب هوش مصنوعی).

ابتدا، اولویت دولت کره بر روی صنعت بود، اما بعداً بر دانشگاه‌ها تأکید شد و در نتیجه استعدادهای هوش مصنوعی پرورش یافت. بنابراین، دولت این کشور قصد دارد دانشگاه‌ها را در استراتژی توسعه استعدادهای هوش مصنوعی که در سرمایه‌گذاری‌های قبلی در هوش مصنوعی که عمدتاً از صنعت حمایت می‌کرد، وجود نداشت، بگنجاند Pangyo Techno Valley . یک مرکز

نوآوری است که بر تحقیقات عمومی–خصوصی با مشارکت استارت آپ‌های جهانی متمرکز شده است. علاوه بر این، کره با مشارکت سامسونگ، ال‌جی الکترونیکس، شرکت هیوندای موتور، غول مخابراتیKT ، SK Telecom، و پورتال اینترنتی ناور Iglauerیک مرکز تحقیقاتی دولتی و خصوصی ایجاد می‌کند. علاوه بر این، دولت کره اسناد متعددی را منتشر کرده است که چشم انداز و استراتژی‌های دقیق خود را در مورد استراتژی تحقیق و توسعه هوش مصنوعی و آمادگی برای جامعه اطلاعاتی هوشمند نشان می دهد(Salas-Pilco, 2021: 204-206). در ژوئیه ۲۰۱۷، شورای دولتی چین برنامه توسعه هوش مصنوعی نسل جدید خود را منتشر کرد که یک طرح بسیار دقیق است که مراحل مختلف زمانی و بودجه مربوطه را تعریف می‌کند. در این برنامه، شش وظیفه اصلی هوش مصنوعی عبارتند از: (الف) توسعه یک سیستم فن‌آوری هوش مصنوعی باز و همکاری (ب) ایجاد یک اقتصاد هوش مصنوعی کارآمد (ج) ایجاد جامعه ایمن هوش مصنوعی، (د) تقویت هوش مصنوعی در زمینه ادغام نظامی و غیرنظامی، (ه) ایجاد یک سیستم زیرساخت هوش مصنوعی کارآمد و (و) طرح‌ریزی همه پروژه‌های علمی و فن‌آوری اصلی هوش مصنوعی. چین قصد دارد ارزش صنعت هوش مصنوعی خود را در سه مرحله افزایش دهد. اول، تا سال ۲۰۲۰، این کشور امیدوار است که با توسعه جهانی هوش مصنوعی پیش بیاید و رقابتی شود و صنعت هوش مصنوعی را به ارزش بیش از ۱۵۰۰۰۰ میلیون یوان (۲۲۰۰۰ میلیون دلار) توسعه دهد. سپس، تا سال ۲۰۲۵، هوش مصنوعی نیروی محرکه اصلی صنعت و اقتصاد چین خواهد بود و صنعت هوش مصنوعی بیش از ۴۰۰۰۰۰ میلیون یوان (۶۰۰۰۰ میلیون دلار آمریکا) ارزش خواهد داشت. در نهایت، تا سال ۲۰۳۰، چین قصد دارد به رهبر هوش مصنوعی جهان تبدیل شود و صنعت هوش مصنوعی آن بیش از ۱,۰۰۰,۰۰۰ یک میلیارد یوان (۱۵۰,۰۰۰ میلیون دلار آمریکا) ارزش خواهد داشت. در سطح جهانی، چین رتبه اول را در (الف) تعداد کل مقالات تحقیقاتی هوش مصنوعی، (ب) مقالات هوش مصنوعی با استناد بالا، (ج) ثبت اختراعات هوش مصنوعی، و (د) سرمایه‌گذاری سرمایه‌گذاری خطرپذیر هوش مصنوعی است. بر اساس مطالعه ارائه شده توسط مؤسسه سیاست علمی و فن آوری چین در دانشگاه Tsinghua (2018)، چین رتبه دوم در (ه) تعداد شرکت‌های هوش مصنوعی و (و) استعدادهای هوش مصنوعی است. علاوه بر این، بنیاد ملی علوم آمریکا پیش‌بینی کرد که "چین تا پایان سال ۲۰۱۸ از ایالات متحده در سرمایه گذاری های تحقیق و توسعه پیشی بگیرد.(Salas-Pilco, 2021: 198-199)«. دولت چنین نوآوری‌های فن آوری را به عنوان یک موتور اقتصادی می‌بینند که منجر به افزایش سرمایه‌گذاری در تحقیق و استفاده از پلتفرم‌ها و دستگاه‌های مبتنی بر هوش مصنوعی می شود، اما همچنین به عنوان راهی برای نظارت موثرتر بر جمعیت است. در عین حال، شرکت‌های فن‌آوری مانند) GAFAM گوگل، اپل، فیس‌بوک، آمازون، مایکروسافت، بایدو، علی‌بابا، تنسنت) و دیگران پیشرو در تحقیق، توسعه و پیاده‌سازی پلتفرم‌های هوش مصنوعی در خدمات و محصولات خود بوده‌اند. قرار دادن آنها در خط مقدم دسترسی و استفاده از داده ها، تعجب آور نیست که در سال‌های اخیر، به ویژه پس از ۱۱ سپتامبر ۲۰۰۱، هوش مصنوعی به طور فزاینده ای در نظارت به کار گرفته شده است. قابلیت‌های جدید در نظارت با اجرای گسترده فن‌آوری های هوش مصنوعی، جمع آوری داده های بزرگ، دیجیتالی کردن خدمات و هزینه های مقرون به صرفه دستگاه‌ها تسهیل شده است. بسیاری از محققان تا حدودی رابطه بین فن‌آوری، جوامع و نظارت مرتبط با امنیت عمومی و تأثیرات آن را مطالعه کرده اند. در زمینه نظارت، نرم افزارها، برنامه‌ها و ابزارهای هوش مصنوعی روند کنترل اجتماعی را تسریع و تقویت می کنند. بازیگران درگیر در تنظیم استانداردهای نظارتی از استراتژی هایی برای ترویج و استفاده از برنامه هوش مصنوعی استفاده می کنند. عموم مردم همیشه در تصمیم‌گیری‌های مربوط به پیشرفت فن‌آوری درگیر و نمایندگی نمی‌شوند، زیرا عمدتاً توسط دولت‌ها و شرکت‌های فراملی اداره می‌شود. در حالی که فن‌آوری را می‌توان به عنوان یک موجودیت خنثی در نظر گرفت، استفاده از آن توسط نهادهای خاص در فرآیندهای اجتماعی چنین نیست و رابطه بین جامعه و توسعه هوش مصنوعی و نقش بازیگران قدرتمند که اجرای هوش مصنوعی را رهبری می کنند، بیانگر شکل‌گیری امکانات و ظرفیت‌های نظارتی جدیدی در حوزهٔ نظارت تصویری و دیجیتالی است. نظارت را می‌توان به عنوان مشاهده سیستمی افراد، گروه‌ها یا فضا با ابزارهای دیداری، شنیداری، عکاسی و الکترونیکی برای نظارت بر رفتارها، فعالیت ها یا اطلاعات برای اهداف خاص مانند تأثیرگذاری، مدیریت یا

هدایت درک کرد. برای هدف قرار دادن یک یا مجموعه ای از اهداف به چندین روش انجام می شود. هدف این اهداف عادی‌سازی جمعیت و حذف رفتارهای نابهنجار یا نامطلوب از جامعه است. نقش نظارت اطمینان از انطباق با ارزش‌های اجتماعی و تنظیم چالش ها یا تغییرات این مجموعه ارزش ها است. ارزش‌های اجتماعی معیارهایی را تعیین می کنند که برای ثبات اجتماعی مهم تلقی می شوند. فن‌آوری‌های نظارتی جدید برای همه اعمال می‌شود و به عنوان «بررسی افراد، گروه‌ها و زمینه‌ها از طریق استفاده از ابزارهای فنی برای استخراج یا ایجاد اطلاعات» تعریف می‌شود. مدیریت و امنیت عمومی از جمله فن‌آوری‌های مورد استفاده می‌توان به حسگرها، دوربین‌های تشخیص چهره، دوربین‌های بدن پلیس و شبکه‌های مخابراتی سریع اشاره کرد. سیستم‌های تشخیص چهره فن‌آوری‌های بیومتریک هستند که تصاویر یا فیلم‌ها را با پایگاه‌های داده ضبط، ذخیره و مطابقت می‌دهند. هوش مصنوعی بخشی از یک نظارت تصویری بی‌رویه است که شهروند خاصی را هدف قرار نمی‌دهد، بلکه افراد را در یک فضا زیر نظر دارد. مدل نظری فوکو از زندان سراسربین را می‌توان برای درک نیروهای محرک نظارت تصویری استفاده کرد. پس، نظارت تصویری یک ابزار خنثی نیست، بلکه بیان اهداف اجتماعی و سیاسی خاص است. نظارت تصویری هوش مصنوعی به مالک یا کنترل کننده فن‌آوری کمک می کند تا به طور موثرتری به اهداف خود دست یابد، زیرا دوربین‌ها اکنون دارای قابلیت‌های هوشمند با الگوریتم هستند. قادر به مشاهده ناهنجاری‌های خاص و ارسال مستقیم اطلاعات، امکان کارآمدترشدن و قلمرو گسترده‌تر نظارت است. تخمین ۵۰ میلیارد دستگاه متصل در سراسر جهان که داده تولید می‌کنند نشان می دهد که اطلاعات در حال تبدیل شدن به یک ابزار اصلی برای توسعه، هماهنگی، ترغیب و اجبار است. ردیابی، تشخیص چهره، چاپ شکل و ابزارهای دیگر. تکامل سریع این سیستم ها امکان نظارت دقیق تر، قاطعانه و گسترده‌تر از جمعیت را فراهم می کند. دولت الکترونیک نمایشی از انطباق‌یابی با قدرت سیاسی است. شبکه‌های دیجیتال مدرن، خوشه‌های سیاسی و خصوصی را با افزایش قدرت از طریق دسترسی و استفاده از داده‌های شخصی، به شکل بی‌سابقه‌ای کنترل و دستکاری. می‌کنند. ابزارهای مختلف نظارتی هوش مصنوعی اکنون در همه جا حضور دارند و امکان ردیابی عمیق تر، دقیق تر و مداوم را فراهم می‌کند. هوش مصنوعی روشی کارآمدتر، کم‌کارتر و ارزان‌تر برای نظارت و سرکوب جمعیت ارائه می‌کند.(Rosiers, 2021: 113-122) . چشم‌انداز نظارتی بر هوش مصنوعی در قالب دو مدل نظارتی جهانی و ملی گرایانه در حال شکل‌گیری است. مشخصه اصلی چشم انداز نظارتی این است که رویکردهای خودتنظیمی و قانون نرم، انتخاب ترجیحی اولیه در هنگام تنظیم فن آوری بوده است. ماهیت غیر الزام‌آور قوانین حریم خصوصی، در کنار دخالت‌های موجود قانونگذار در قوه قضاییه، حمایت از حریم خصوصی را تا حد زیادی غیرعملی می‌کند. به رغم وجود اصول جهانی بی‌شماری برای حاکمیت یا توسعه اخلاقی سیستم‌های هوش مصنوعی از منابع مختلف، شامل سازمان‌های بین‌المللی، دولت‌ها و سازمان‌های غیردولتی بین‌المللی، در وضعیت فعلی سطح بالایی از اجماع در مورد اصول هوش مصنوعی وجود ندارد(Zekos, 2022: 522) . نگرانی اصلی این است که الگوریتم‌های هوش مصنوعی می‌توانند در نظارت برای هدف قرار دادن داوطلبانه گروه‌های اجتماعی خاص استفاده شوند. سازمان‌های امنیتی از داده‌های پلتفرم‌های شبکه‌های اجتماعی یا جمع‌آوری‌کننده‌های داده‌های بخش خصوصی برای به اشتراک‌گذاری اطلاعات بخش بزرگی از جمعیت آمریکا استفاده می‌کنند. حتی اگر این سازمان‌ها برای جلوگیری از تروریسم و سایر تهدیدات اجتماعی فعالیت کنند، اما امکان سوء استفاده نیز گزارش شده است. چنین مراکزی با تجاوز به سیاست‌ها در شیوه‌های خود، در پروفایل‌های نژادی، پروفایل‌های سیاسی، داده‌کاوی غیرقانونی و جمع‌آوری داده‌های غیرقانونی مشارکت داشته‌اند. ابزارهای ارزیابی آنها حاوی سوگیری‌هایی علیه افراد یا گروه‌ها بود. ابزار ارزیابی آسیب‌های خطر یک فن‌آوری مبتنی بر هوش مصنوعی است که از تاریخچه ۱۰۴۰۰۰ نفری که قبلاً در دورهام دستگیر شده‌اند، استفاده می‌کند. این ابزار کمک می‌کند تا خطر ارتکاب مجدد جرم را از بالا به پائین افزایش دهد. محدودیت این ابزار این بوده است که تصمیم‌گیرندگان انسانی می توانند فوراً خود را تطبیق دهند دقت کلی این ابزار در مطالعه قبلی ۶۳ درصد بوده است. عدم دقت، نگرانی هایی را در مورد شناسایی نادرست افراد به خصوص در رابطه با سیاه پوستان و زنان ایجاد می‌کند. با این حال، ابزارهای الگوریتمی مانند CORELS40 وجود دارند که کارایی بیشتری را نشان داده‌اند. بحث ما در این جا نادیده گرفتن

توانمندی‌های این ابزارها نیست، بلکه آگاهی از سوگیری‌هایی است که می‌تواند در آنها گنجانده شود و عواقبی که می‌تواند بر جمعیت‌های خاص داشته باشد. جمع‌آوری داده‌ها از طریق فرآیند نرم‌تر نظارت انجام می‌شود که به این ایده اشاره دارد که کمتر قابل مشاهده و اجباری شده است. با این وجود، اینترنت امکان نظارت بر همه کاربران خود را از طریق موتورهای جستجو، رسانه های اجتماعی، برنامه ها و موارد دیگر فراهم می کند. کاربران اطلاعات بسیار کمی در مورد اطلاعات جمع آوری شده بر روی آنها دارند که می توان آن را به عنوان بهره برداری و از دست دادن کنترل بر روی داده‌های شخصی توصیف کرد. اغلب مصرف‌کنندگان برای استفاده از پلتفرم‌ها یا خدمات آنلاین باید با شرایط موافقت کنند. حتی اگر برخی از مصرف‌کنندگان نظارت انجام شده در رسانه‌های اجتماعی را به عنوان سوء استفاده از داده‌ها در نظر بگیرند، مزایای بالقوه دسترسی به آن پلت‌فرم‌ها از معایب آن بیشتر است. این امر با ادغام بیشتر خدمات و فعالیت‌های اجتماعی در پلت‌فرم‌های دیجیتال و افزایش وابستگی کاربران به انجام راحت‌تر روزانه ایجاد می‌شود. اقداماتی مانند ارتباطات، پرداخت ها، سفارشات، دسترسی به خدمات و موارد دیگر. در حالی که شیوه‌هایی که آن‌ها ترویج می‌کنند، منجر به نوعی کنترل اجتماعی می‌شود. استراتژی گوگل جمع‌آوری داده‌ها از طریق برنامه‌های کاربردی متعدد خود برای تجزیه و تحلیل بهتر رفتار مصرف‌کننده است در حالی که فیس‌بوک نظارت دائمی بر کاربران خود انجام می‌دهد. نظارت امکان کنترل خاصی بر رفتار افراد، اطلاعات به اشتراک گذاشته شده و شناسایی رفتارهای مشکوک را فراهم می کند. دستکاری، انتقال و جمع آوری آن داده ها بسیار مبهم است. بسیاری از سیستم های تصمیم‌گیری دیجیتالی دولت های آنلاین به سختی به شهروندان امکان دسترسی به منطق کلی سیستم را می دهند (Rosiers, 2021: 123-124-126). باید در نظر گرفت که فضای سایبری در نظر گرفته شده بود که سیستم خودگردانی باشد که بدون توجه به جغرافیا و اجبار مبتنی بر سرزمینی به مردم اجازه دهد تا به جوامع بپیوندند و بدون توجه به جغرافیا و بدون توجه به ساختارهای اجباری از بالا به پایین بر خود حکومت کنند. نظام های حکومتی سرزمینی، و بدون آسیب شناسی‌ها و مفاسد معمولی که نشان دهنده حاکمیت سرزمینی است. تلاش‌های حاکمیت فضای مجازی تا به امروز متفاوت بوده است، زیرا خطرات ناشی از مداخله دولت ملی، تمرکز مجدد و افزایش سیاسی‌سازی به‌عنوان راه‌هایی که ساختارهای حاکمیتی فضای سایبری نتوانسته‌اند چشم‌انداز اصلی فضای سایبری را حفظ کنند و باعث ایجاد مشکلاتی در زمینه ظرفیت نوآورانه شده است. به عنوان مثال، ماده ۲ قانون امنیت سایبری، صلاحیت سرزمینی خاصی را بر موضوعات مرتبط با شبکه در چین، اعم از اینکه جنبه مدنی، کیفری یا اداری داشته باشد، تعیین می‌کند، به این معنی که افرادی که فعالیت‌هایشان با فضای سایبری در قلمرو، مواد، شبکه چین مرتبط است. اطلاعات، علاوه بر خود فعالیت‌های سایبری، مانند فعالیت‌های سایبری غیرقانونی و مجرمانه با هدف سیستم اطلاعاتی، همگی مشمول این صلاحیت هستند. در نتیجه، تا زمانی که فعالیت‌های سایبری در قلمرو سرزمین اصلی چین رخ می‌دهد، صرف نظر از هویت یا ملیت بازیگران، همه آنها مشمول قانون هستند. علاوه بر این، ماده ۵ قانون امنیت سایبری ۱۳۷ حق دفاع چین در فضای سایبری را تأیید می‌کند و به دولت چین اجازه می‌دهد تا حملات و تهدیدهای سایبری خارجی را نظارت، دفاع و مجازات کند. در اینجا شایان ذکر است که در سال ۲۰۲۱، یک حمله سایبری به سیستم های تبادل مایکروسافت صورت گرفت و باید ثابت شود که چه نهادی پشت آن بوده است. علاوه بر این، ماده ۷۵ تصریح می‌کند که برای کسانی که حملات، نفوذ، مداخله، تخریب یا سایر فعالیت‌ها را به منظور به خطر انداختن زیرساخت‌های اطلاعاتی اساسی جمهوری خلق چین انجام می‌دهند، اعم از سازمان‌ها یا افراد، در صورتی که اثرات حیاتی داشته باشند، دولت چین باید اقداماتی را مطابق با قانون برای مسدودکردن دارایی‌های آنها یا اتخاذ سایر اقدامات تنبیهی مورد نیاز انجام دهد. شایان ذکر است که چین در حال ایجاد استانداردهای جهانی جدید برای تجارت داده است. در سال ۲۰۱۷، شرکت اپل یکی از اولین شرکت‌هایی بود که یک مرکز داده سرمایه‌گذاری مشترک جدید در چین ایجاد کرد تا از قانون امنیت سایبری چین در همان سال پیروی کند که از همه شرکت‌ها خواسته بود از «زیرساخت اطلاعات حیاتی» برای ذخیره داده‌های خود در یک چینی حمایت کنند. سرور متعلق به باید در نظر گرفت که تصمیم شرکت‌ها برای افتتاح یک مرکز داده با مالکیت عمده توسط یک شرکت چینی، سیاست قدرت و دسترسی به داده ها را در داخل شرکت و در میان مصرف کنندگان آن تغییر می دهد. تا این حد،

به نظر می‌رسد که اپل از دسترسی به داده‌ها استفاده کرده است که به تسلط در فن‌آوری آینده‌گر هوش مصنوعی کمک می‌کند. از سوی دیگر، چین با تلاش‌های جمع‌آوری اطلاعات توسط شرکت‌های خارجی تحت صلاحیت ملی خود با شکایت از اپل به دلیل نقض قانون با نگهداری سرورهای خود در چین با جدیت برخورد می‌کند و بنابراین اپل سرورهای خود را به سرورهایی منتقل کرد که توسط دولت استانی ارائه دهنده خدمات ابری.Guizhou Yunshang چین اداره می‌شوند. تا این حد، ایالات متحده انحصار جهانی در فضای مجازی دارد و بقیه جهان نمی‌توانند به استقلال کامل در فضای سایبری دست یابند، به این معنی که حاکمیت فضای سایبری باید مظهر شکل مستقلی از حاکمیت یک کشور باشد. علاوه بر این، حق برابری از کشورها می‌خواهد به فضای سایبری یکدیگر دسترسی داشته باشند و به طور مساوی به یکدیگر متصل شوند، تأیید می‌کند که کشورهای مختلف صلاحیت یکسانی بر سیستم‌های شبکه خود دارند و مدیریت شبکه یک کشور آسیبی به شبکه‌های کشور دیگر وارد نمی‌کند. با این وجود، به دلیل ماهیت بدون مرز و وابسته به هم فضای سایبری، سیاست‌های فضای سایبری که توسط ایالات متحده آمریکا تحریک می‌شود، ممکن است به نفع منافع خود باشد به قیمت اینکه کشورهای در حال توسعه قدرت بسیار بیشتری به ایالات متحده می‌دهند در مقایسه با سایر کشورها در اداره فضای سایبری جهانی. باید در نظر گرفت که حفظ جریان آزاد داده ها در مقیاس جهانی برای گسترش اقتصاد دیجیتال به یک استراتژی توسعه برای بسیاری از کشورها و مناطق تبدیل شده است. با این وجود، با هدف تقویت حاکمیت ملی و امنیت فضای سایبری، کشورهای جهان قوانینی را برای محدود کردن ذخیره‌سازی خارجی و انتقال فرامرزی داده‌های خاص وضع کرده‌اند. با توجه به موضوع ذخیره‌سازی داده‌ها و انتقال برون مرزی، ایالات متحده مدت‌هاست که از جریان آزاد داده‌ها در سراسر جهان حمایت کرده و آن را تقویت می کند. اگرچه، اتحادیه اروپا رویکرد بسیار متفاوتی را در پیش گرفته است، هر دو دستورالعمل حفاظت از داده ۱۹۹۵ و GDPR 2016 محدودیت‌های شدیدی را برای انتقال داده‌های شخصی از شرکت های اتحادیه اروپا به شرکای خارجی ایجاد کرده‌اند. بنابراین، زیرساخت ذخیره‌سازی داده‌ها زمانی وجود دارد که میزبان اطلاعات طبقه‌بندی‌شده دولتی، شامل پرونده‌های دفاعی و اطلاعاتی باشد. به علاوه، فن‌آوری اطلاعات و نرم‌افزارهای مخابراتی برای بهره‌برداری از تأسیسات ذخیره‌سازی داده‌ها، انتقال داده‌ها و پردازش داده‌ها مورد بهره‌برداری قرار می‌گیرند. در نتیجه، فن‌آوری‌های دیجیتال در صورت داشتن گزینه‌های استفاده دوگانه، از فن‌آوری‌های پزشکی گرفته تا سیستم‌های تشخیص دفاع زیستی، بر پایه نیمه‌رساناها هستند، زیرا برای قدرت دفاعی و نظامی بسیار مهم هستند و به دلیل فراگیر بودن دستگاه‌های نیمه‌رسانا، برای کاهش خطرات امنیت سایبری ضروری هستند.

آین کوکاس استدلال می‌کند که «ایالات متحده باید رویکرد خود را تغییر دهد، زیرا سیاست‌های آزادسازی فعلی‌اش در نهایت نه از مصرف‌کنندگان محافظت می‌کند و نه از رقابت ملی... چین، با تنظیم مسائل امنیتی ارائه‌شده توسط سرمایه‌گذاری داده‌های شرکت‌های جهانی از طریق ترکیبی از سیاستگذاری ملی، تسلط شرکت ها و اقدامات نظارتی بین المللی، استانداردهای جهانی جدیدی را برای تجارت داده ایجاد می کند. با گسترش، چین مدل خود را از حاکمیت داده‌ها ارائه می‌کند. این مدل با ذخیره داده‌های تولید شده در کشور در سرورهای دولتی و همچنین آوردن داده ها از خارج به کشور، داده ها را در چین بومی‌سازی می کند. علاوه بر این، برای تأثیرگذاری بر اصول بین‌المللی بر اصول حاکمیت داده‌های داخلی متکی است.» در واقع، تأثیر چین بر حاکمیت داده‌های جهانی در مرکز آینده سیاست ارتباطات جهانی قرار دارد. باید در نظر گرفت که همانطور که اطلاعات یک شیوه حفظ امنیت است، یک نوع کنترل نیز هست و بنابراین زمانی که دولت ها قادر به کنترل اطلاعات تجاری و سیاسی هستند، نظارت خود را بر جمعیت افزایش می دهند که به این معنی است که آنها باید اطلاعات تجاری و سیاسی را کنترل کنند. دانشمندان داده به طور متفکرانه و دقیق با پیشبرد روش‌ها و هنجارهای جدید مؤثر بر اهداف و استراتژی‌های سیاسی به بهبود جامعه کمک می‌کنند. با فرض ریسک‌های سیاسی الگوریتم‌ها، دانشمندان داده باید تلاش‌های خود را در تعهدات سیاسی روشن و ارزیابی‌های دقیق از پیامدها استوار کنند. علاوه بر این، توسعه سریع سیستم‌های هوش مصنوعی، الگوریتم‌های دیجیتال مستقل و فن آوری‌های روباتیک، چشم‌انداز و ویژگی‌های زندگی اجتماعی–حقوقی و اجتماعی–سیاسی جامعه را متحول کرده است. این نشان می‌دهد که

استفاده از فن‌آوری های دیجیتال برای حفاظت از منافع افراد، مشاغل و دولت ضروری است و بنابراین امنیت شبکه های مخابراتی یکپارچه، دسترسی مداوم به فضای سایبری، ثبات شبکه‌های ارتباطی از اهمیت محوری برخوردار است. مورد استفاده مقامات دولتی، تعمیر و نگهداری سخت افزارهای مربوطه و غیره. در این راستا، دفاع از کشور و امنیت جامعه مدنی، وظایف کلیدی دولت را تشکیل می دهد، مانند مقررات لازم الاجرای مواد ۵۵، ۷۱، و ۱۱۴ قانون اساسی فدراسیون روسیه (Zekos, 2022: 356, 369-371, 384). اثرات سیاسی مرزهای دیجیتال ملی کدامند؟ توسعه مرزهای دیجیتال ملی اثرات سیاسی زیر را بر دولت ها خواهد داشت: اول از همه، حاکمیت داده‌ها علاوه بر وجود سیستم سانسور و نظارت، اقتدارگرایی دیجیتال را بیشتر تقویت می‌کند، به این معنی که الگوی سانسور و بومی‌سازی داده‌ها به سمت کل هدایت می‌شود. کنترل، توانایی دولت برای اجبار را بیشتر می کند. ثانیاً، تضادها بر سر حاکمیت داده‌ها، عرصه جدیدی را برای بسیاری از کشورها ایجاد می‌کند و بسیاری از دولت‌ها مقررات داده‌ای را آغاز کرده‌اند که منجر به قوانین ناسازگار می‌شود. ثالثاً، قوانین ملی یک کشور در مورد حفاظت از داده ها، زمانی که شرکت ها در کشورهایی با مقررات سختگیرانه داده سرمایه‌گذاری می کنند، مشکلاتی را ایجاد می کند. علاوه بر این، مرزهای دیجیتال ملی یک مانع تجاری جدید ایجاد می‌کنند و بنابراین چنین مرزهایی با هزینه‌های هنگفتی برای انطباق برای شرکت‌های فن‌آوری چندملیتی مواجه می‌شوند، زنجیره ارزش جهانی را متزلزل می‌کنند و اقتصاد مقیاس را به خطر می‌اندازند. می‌توان گفت که دولت‌ها به منظور حفظ حاکمیت قانون، فن‌آوری‌های جدیدی را به مکانیسم‌های حکمرانی خود وارد می‌کنند. نظارت هوش مصنوعی دو قابلیت عمده را به دولت ها ارائه می دهد. اولاً، نظارت هوش مصنوعی به رژیم‌ها اجازه می‌دهد تا بسیاری از عملکردهای ردیابی و نظارت را که قبلاً به اپراتورهای انسانی اختصاص داده شده بود، خودکار کنند و بنابراین باعث کاهش هزینه‌ها، کاهش اتکا به نیروهای امنیتی، و جایگزینی مشکلات احتمالی وفاداری عامل اصلی می‌شود. ثانیاً، فن‌آوری هوش مصنوعی شبکه نظارتی بسیار گسترده‌تری نسبت به روش‌های قدیمی ایجاد می‌کند و بنابراین، نظارت بر تمام فعالیت‌های فیزیکی و دیجیتالی برای پیش‌بینی رفتار نامطلوب استفاده خواهد شد. بنابراین، سیاست کلان داده بین هر کشوری و در مورد هر شرکت چند ملیتی که داده‌های شخصی را جمع‌آوری می‌کند، پدیدار می‌شود(Zekos, 2022: 507-508).

امکان شناسایی تهدیدات امنیتی و اقدام پیشدستانه

هوش مصنوعی در سال‌های اخیر به سرعت پیشرفت کرده است و ظرفیت‌های تقریباً انسانی یا مافوق بشری را در عرصه‌های گسترده‌ای از جمله مدل‌سازی پیش‌بینی‌کننده، تصمیم‌گیری استراتژیک و تشخیص الگوی پیچیده به دست آورده است. از آنجایی که این ظرفیت ها به هم پیوسته و ترکیب می شوند، هوش مصنوعی ممکن است به زودی استانداردهای هوش عمومی انسانی را فراگیرد و حتی از آن پیشی گیرد. در حال حاضر، سیستم‌های IoTIA عمدتاً انتخاب‌ها را فیلتر می‌کنند، با الگوریتم‌های هوش مصنوعی که از طریق مقادیر انبوهی از داده‌ها به فهرست کوتاه گزینه‌ها برای انتخاب انسان تبدیل می‌شوند. اما مرحله بعدی جابجایی تصمیم نزدیک است. با انتشار عملکرد جستجوی جریان فوق سریع Google Instant در سال ۲۰۱۰، سرگئی برین اعلام کرد که گوگل به «نیمه سوم مغز شما» تبدیل خواهد شد. در حالی که عبارت برین رمزآلود است، یک تفسیر معقول این است که هدف گوگل این است که «بداند در جستجو، چه می‌خواهید، شاید حتی قبل از اینکه خود بدانید». پیش‌بینی دیجیتال به طور پیوسته جایگزین تصمیم گیری انسان می شود (Paul Thiele, 2021: 47). شناسایی مسائل در زمان واقعی بسیار دشوارتر است، رویدادها و فرآیندهای کوتاه‌مدت و میان مدتی هستند که نشانگر تغییر شرایط پرخطر به خشونت واقعی هستند، یا آنچه معمولاً به عنوان هشدار اولیه شناخته می شود. به طور کلی، سه دسته از شاخص های هشدار اولیه وجود دارد. اول، لحظات یا گفتمان‌های نمادین خطرناکی وجود دارد که به طور قابل توجهی از جمعیت‌های آسیب‌پذیر، انسان‌زدایی می‌کند، یا شکاف‌های هویتی عمیق بین گروه‌ها را تقویت می‌کند و شامل گردهمایی ها و بزرگداشت رویدادهای تفرقه افکن یا گسترش تبلیغات نفرت

است. دوم، افزایش سرکوب دولتی، مانند انتقال نیروهای امنیتی به مکان‌هایی با جمعیت آسیب‌پذیر، سلب حقوق قانونی آن جمعیت، حمله به رهبران برجسته اقلیت یا مخالفان و پیروان آنها، یا دستگیری‌های گسترده غیرنظامیان. در نهایت، بحران‌های سیاسی و امنیتی که رهبران سیاسی فعلی را به چالش می‌کشند، شاخص‌های مهمی هستند و اینها می‌تواند شامل درگیری‌های مسلحانه جدید یا از سرگیری بین دولت و شورشیان، تغییرات سریع در رهبری دولت، یا گسترش اعتراض‌های تقابلی باشد. شوک‌های بیرونی پیش‌بینی‌نشده مانند بلایای طبیعی یا سرریز درگیری‌های همسایه نیز می‌توانند با به چالش کشیدن توانایی رهبران سیاسی برای حفظ کنترل، باعث خشونت شوند. در بسیاری از موارد، چندین شاخص هشدار اولیه به طور همزمان یا به صورت خوشه ای رخ می دهد(Yankoski, et.al, 2021: 151) . در نتیجه، هوش مصنوعی به کانون توجه شرکت های تجاری، دولت ها، سازمان های نظامی و محققان برای درک روندهای آینده و بالا بردن امکان پیش‌بینی‌پذیری سیاسی تبدیل شده است. آژانس پروژه های تحقیقاتی پیشرفته دفاعی ایالات متحده در حال حاضر در حال توسعه «موج سوم» هوش مصنوعی است. هوش مصنوعی موج اول از قوانین پیروی می کرد. هوش مصنوعی موج دوم درگیر تجزیه و تحلیل آماری پیشرفته است. هوش مصنوعی موج سوم استدلال و آگاهی زمینه ای را در یادگیری ماشینی گنجانده است. این به هوش مصنوعی اجازه می دهد تا با همکاری با طراحان، مهندسان و دانشمندان، فرضیه های خود را تولید، آزمایش و اصلاح کند .(Paul Thiele, 2021: 41)برای نمونه، یک مسأله مهم در مطالعات منازعه، شناسایی پیش سازه‌های خشونت سیاسی است که توسط عوامل انسانی تداوم می یابد. یانکوسکی و همکاران با تمرکز بر تبلیغات نفرت توزیع شده در شبکه های اجتماعی، تصمیم به توسعه مدلی کرد که ممکن است برای حل آن مشکل به کار گرفته شود و بتوانند روندها و تهدیدهایی را که منجر به خشونت سیاسی می‌شوند را شناسایی می‌کند. با این اطلاعات، مقامات دولتی می‌توانند قبل از وقوع خشونت سیاسی وارد عمل شوند و از این طریق صلح را در جامعه حفظ کنند. اما از سوی دیگر، به گفته سوئد و چاوز ، بازیگران غیردولتی خشن ممکن است بتوانند از فن‌آوری‌های هوش مصنوعی برای گول زدن تلاش‌های مقامات دولتی برای جلوگیری از خشونت سیاسی استفاده کنند (Keskin, Tugrul & David Kiggins, 2021: 11-12). این چیزی است که محققان مطالعات صلح اغلب از آن به عنوان «صلح منفی» یاد می‌کنند – فقدان درگیری مسلحانه و تهدید وجودی افراد، مانند قتل، حمله و شکنجه – و با مشارکت در مدل‌سازی و تحلیل‌های هشدار اولیه دربارهٔ خشونت سیاسی از طریق تصاویر دیجیتال در رسانه‌های اجتماعی است. تا سیاستگذاران و تحلیل‌گران دریابند که جوامع ناپایدار کجا و چه زمانی ممکن است به خشونت در مقیاس بزرگ دامن بزنند. ما متوجه هستیم که ایجاد اراده سیاسی برای جلوگیری یا توقف خشونت بسیار مهم و بسیار دشوار است، اما ارائه اطلاعات دقیق‌تر و عملی‌تر در مورد تشدید درگیری می‌تواند به کار پیشگیری کمک قابل توجهی کند. تمرکز منحصر به فرد ما بر روی تصاویر دیجیتال به دلیل روش‌های جدیدی است که افراد از طریق آن در اینترنت ارتباط برقرار می‌کنند و دیگر فقط مبتنی بر متن نیستند. با توجه به حجم عظیم داده‌های رسانه‌های اجتماعی که روزانه تولید می‌شود و نیاز به تجزیه و تحلیل به موقع و دقیق، سیستم‌های هوش مصنوعی قابلیت‌های منحصربه‌فردی را برای بهبود و حتی تغییر دستور کار کسانی که وظیفه پیش‌بینی و پاسخ به خشونت را دارند، ارائه می‌کنند. اینکه چگونه رسانه های اجتماعی به طور فزاینده‌ای برای ایجاد ترس و بی‌اعتمادی در جوامع شکننده و مشروعیت بیشتر خشونت علیه گروه های آسیب‌پذیر استفاده می‌شود. این نوع اطلاعات نادرست، شاخص مهمی از خشونت احتمالی در کوتاه مدت یا میان مدت است(Yankoski, et.al, 2021: 149). با این حال، با غوطه‌ور شدن در این شبکه های اجتماعی، پیچیدگی داخلی گسترده آنها آشکار می شود، به طوری که بسیاری از جوامع و جوامع فرعی در وب‌های پیچیده در پلتفرم هایی مانندReddit ، chan۴، Twitter، Facebookو Instagram وجود دارند. بنابراین، به کجا نگاه کنیم؟ پلتفرم‌های رسانه‌های اجتماعی همیشه در تلاش بوده‌اند تا عناصر ساختاری را به پست‌های خود اضافه کنند تا کاربران بتوانند موضوعات و نویسندگان مرتبط را بهتر شناسایی کنند. نمونه‌هایی از این عناصر ساختاری عبارتند از هشتگ‌های تعریف‌شده توسط کاربر (نماد «#» به دنبال رشته متن ساده) که به‌عنوان متا داده برای برچسب‌گذاری پست‌ها با موضوعات سفارشی در اکثر شبکه‌های اجتماعی و همچنین نام حساب‌ها (اغلب با نماد "@" نشان‌داده می‌شوند) استفاده می‌شود.

با این حال، قابلیت اطمینان این عناصر می‌تواند مشکوک باشد و برخی از پلتفرم‌ها تلاش خود را می‌کنند تا آنها را بی‌فایده جلوه دهند (به‌خصوص chan۴، که تقریباً هر کاربر ناشناس است). اشیاء رسانه‌ای مانند تصاویر و ویدیوها نیز عناصر ساختاریافته را در پست‌ها تشکیل می‌دهند، و برای اهداف ما، پست‌های حاوی این نوع رسانه‌ها مورد توجه اصلی هستند. نظارت انسانی حتی بر تعداد محدودی از منابع ثابت کرد که قادر به همگام‌شدن با سرعت تولید محتوا نیست. از تنها ۲۶ هشتگ و هشت کاربر در توییتر و اینستاگرام، بیش از دو میلیون تصویر را برای تجزیه و تحلیل جمع آوری شد. عددی خیره‌کننده که از ظرفیت انسان برای یافتن الگوها در داده های سازماندهی نشده فراتر است. مؤلفه هوش مصنوعی سیستم هشدار اولیه برای خودکارسازی تجزیه و تحلیل مجموعه‌های بزرگ محتوای رسانه‌ای که در مرحله دریافت داده جمع‌آوری شده‌اند، طراحی شده است. برای یک سیستم هشدار اولیه خشونت، ما به راهی برای توصیف تصاویر نیاز داریم که:

۱- از یک مجموعه اولیه، آنها را بتوان در ژانرهای متمایز قرار داد ۲- تصاویر جدید را می توان در ژانرهای شناخته شده یا ژانرهای جدید در صورت لزوم قرار داد ۳- درک معنایی محتوای بصری را می توان استخراج کرد، به طوری که پیام های تهدید کننده را می توان شناسایی کرد.

کل فرآیند به صورت خودکار و بدون نظارت انجام می‌شود و نیازی به دخالت انسانی ندارد. برای یافتن تصاویر مرتبط، ابتدا باید هر کدام بر اساس ویژگی‌هایی که سبک و محتوای تصاویر را توصیف می‌کنند، فهرست‌بندی شوند، اما به روشی فشرده که فضای مورد نیاز برای ذخیره داده‌ها را کاهش دهد. چنین نمایشی از داده‌ها را می‌توان با استفاده از تکنیک‌هایی از حوزه بازیابی تصویر مبتنی بر محتوا تولید کرد که مشکل تطبیق میلیون‌ها تصویر بر اساس ظاهر بصری را برطرف می‌کند. هدف ما باید توسعه مدل‌های شناختی واقع‌گرایانه باشد تا تأثیری را که دستکاری رسانه‌ها و استفاده از رسانه‌های جعلی بر کاربران، نیات آنها (بدخواهانه، بازیگوش، سیاسی) و همچنین احساسات تحریک‌شده آنها می‌گذارد، توسعه دهیم. هدف نهایی طراحی یک سیستم هشدار زودهنگام هوش مصنوعی است که قادر به نظارت بر پلتفرم‌های رسانه‌های سنتی و اجتماعی برای محتوای پرطرفدار است که ممکن است بخشی از یک کارزار تأثیرگذاری با هدف تحریک خشونت باشد.(Yankoski, et.al, 2021: 159-161). دو قرن و نیم پیش، آدام اسمیت استدلال کرد که «دست پنهان» بازار آزاد در حال ظهور، هماهنگی جامع عرضه و تقاضا را بدون نظارت یا حکومت اداری تضمین می‌کند. فن‌آوری در حال ظهور در بازار معاصر، در حال توسعه یک ذهن پنهان است. شرکت‌های مجهز به اینترنت اشیاء اکنون می‌توانند مصرف‌کنندگان و مشتریان را هدف قرار دهند و نیازها و خواسته‌های بیان‌نشده فردی را برآورده کنند و شکل دهند. مردم مجبور نخواهند بود تصمیم بگیرند چه می خواهند یا چه زمانی آن را می خواهند. آنها قبل از تقاضا، عرضه می شوند. از آنجایی که گزینه‌های موجود در بازار به طور فزاینده‌ای توسط ماشین‌های شبکه‌ای شکل می‌گیرند و انتخاب می‌شوند، انتظار می‌رود ظرفیت‌های تصمیم‌گیری انسان کاهش یابد(Paul Thiele, 2021: 47).

نتیجه

هوش مصنوعی برای بررسی مشکلات بزرگ و چندوجهی که نیاز به استراتژی، پیش‌بینی اثرات بلندمدت و تجزیه و تحلیل حجم وسیعی از داده‌ها را در بر می‌گیرد و برتر از هوش انسانی است. برتری هوش مصنوعی در جمع‌آوری داده‌ها و ماموریت‌های پیش‌بینی وجود دارد، زیرا پیش‌بینی توانایی استفاده از اطلاعات یا حقایق به‌دست‌آمده برای پیش‌بینی رویدادهای آینده و اقدامات انسانی است. باید در نظر داشت که در حال حاضر هوش مصنوعی توسط انسان کنترل می شود. اما این امکان غیرمحتمل نیست که هوش مصنوعی در آینده به نحوی توسعه یابد که از کنترل انسان خارج شود. بنابراین، حضور گسترده‌تر ماشین‌های بسیار تکامل‌یافته منجر به پرسش عمیق درباره مناسبت تصمیم‌گیری می‌شود. با این وجود، هوش مصنوعی می تواند انسان ها را در بازی‌ها و بسیاری از فعالیت‌های دیگر شکست دهد. نگرانی اصلی در این واقعیت نهفته است که شرکت‌های فن‌آوری بزرگ مالک حقوق مالکیت فکری هستند، با بودجه‌های تحقیقاتی عظیم کار می‌کنند، از پرطرفدارترین دانشمندان داده استفاده می‌کنند، حجم

وسیعی از داده‌ها و همچنین مراکز ذخیره آن را در اختیار دارند، شبکه‌های مخابراتی دارند و مهمتر از همه، ایجاد روابط مرتبط با صاحبان قدرت. آنها هستند که دستور کار توسعه هوش مصنوعی را تعیین می کنند. برای اینکه هوش مصنوعی واقعاً دموکراتیک شود، کاربران باید بر آنچه اجرا می‌کنند، زمان اجرا و نحوه استفاده از نتایج اجرا کنترل داشته باشند. اگرچه استفاده از هوش مصنوعی به نفع بشریت و در یک زمینه بزرگتر به نفع او است، اما این معضل وجود دارد که آیا روش هوش مصنوعی که در حال حاضر استفاده می شود درست است یا خیر و آیا هوش مصنوعی برای بشریت خوب است یا خیر؟ چنین معضلی منجر به عدم اطمینان در ذهن توسعه‌دهندگان و سیاستگذاران می‌شود و در نهایت یک خطر امنیتی ایجاد می‌کند. نتیجه ان که برخی از معضلاتی که ممکن است در حوزۀ هوش مصنوعی و امنیت رخ دهد، عبارتند از: (Salas-Pilco, 2021: 247-248).

معضل امنیت نظامی

فن‌آوری‌های جدید باعث ایجاد عدم اطمینان در مورد قدرت حریف می‌شود. هر یک از این پیشرفت‌های فن‌آوری، عدم اطمینان در مورد نحوه استفاده از فن‌آوری و قدرت آن را به همراه دارد، همان‌طور که در جنگ جهانی دوم مشاهده شد، زمانی که آلمان زمینه را برای استفاده از فن‌آوری‌های جدید مانند رادار، توپخانه مکانیزه و هواپیما به نفع خود فراهم کرد، چنین معضلی کشورها را مجبور به رقابت برای برتری فن‌آوری می‌کند و هوش مصنوعی یکی از این پیشرفت‌های فن‌آوری است که استفاده دقیق در جنگ برای آن یک معضل است. هیچ کس نمی‌داند که چگونه از آن استفاده خواهد شد و موفقیت احتمالی آن در میدان جنگ چگونه خواهد بود. در سطح تاکتیکی، هوش مصنوعی در حال حاضر در طیف گسترده‌ای از سیستم های تسلیحاتی و زیرساخت‌های اصلی به جای ایجاد یک سیستم تسلیحاتی واحد ساخته شده است. این امر به تانک‌ها، توپخانه‌ها، هواپیماها و زیردریایی‌ها اجازه می‌دهد تا اهداف را به‌تنهایی شناسایی کرده و پاسخی را ارائه دهند. پاسخ یک سیستم هوش مصنوعی چنین است که می تواند در نبردهای هوا به هوا شبیه‌سازی شده از یک خلبان نظامی با تجربه بهتر عمل کند. با این حال، مشخص نیست که چگونه این پیشرفت ها ماهیت درگیری را تغییر خواهند داد. اگرچه گمانه‌زنی‌ها بسیار زیاد است، اما عدم قطعیت‌ها در مورد تغییر و مزیت احتمالی هوش مصنوعی در سناریوی نبرد به دلیل ادغام آن در مراکز تسلیحات و فرماندهی و کنترل موجود وجود دارد. از آنجایی که اجزای اصلی هوش مصنوعی، یعنی الگوریتم‌ها، داده‌ها و قدرت محاسباتی به طور تصاعدی در حال بهبود هستند، پیش‌بینی آینده هوش مصنوعی دشوار است. آنچه باقی می‌ماند، پرسیدن سوال و حدس و گمان است که چگونه قدرت‌های رقیب ممکن است از هوش مصنوعی به روش‌های نوآورانه و غیرمنتظره استفاده کنند و سعی‌کنند جایگزین‌هایی برای چنین استفاده‌ای ایجاد کنند که منجر به یک رقابت قدرت بی پایان شود.

معضل امنیت انسانی

از آنجایی که تجزیه و تحلیل رفتار اجتماعی، تجزیه و تحلیل پیش بینی‌کننده و تجزیه و تحلیل رقابتی مبنای تعیین تهدیدهای بالقوه داخلی هستند، خطر "تهاجم به حریم خصوصی" وجود دارد. اگرچه چنین راه‌حل‌های پیش‌بینی‌کننده‌ای به امنیت یک سازمان کمک می‌کنند، اما بر داده‌های رفتاری انسان تمرکز می‌کنند که منجر به بازاریابی اجباری، قیمت‌گذاری انتخابی می‌شود و امکان جمع‌آوری داده‌ها را برای برنامه‌های هنوز اختراع نشده و الگوریتم‌های هنوز کشف نشده فراهم می‌کند. بنابراین این یک معضل ایجاد می‌کند که آیا داده‌ها باید توسط شرکت‌ها جمع‌آوری، ذخیره و استفاده شوند و آیا چنین برداشت و استفاده‌ای می‌تواند اخلاقی تلقی شود. موضوع داده‌کاوی و حریم خصوصی بسیار پیچیده است، اساساً به این دلیل که فن‌آوری‌های یادگیری ماشینی و داده‌کاوی از عواقب سوء استفاده یا تجاوز به قوانین حریم خصوصی شخصی غافل هستند. معضل درک تأثیر گرمایش جهانی، رسانه‌های اجتماعی و تغییرات نیروی کار و تولید از عدم تصمیم‌گیری درباره اینکه کدام داده‌ها باید جمع‌آوری شوند و به اشتراک

گذاشته می‌شوند، پدید می‌آیند، زیرا چنین داده‌هایی می‌توانند برای منافع سیاسی و سرکوب مردم عادی مورد سوءاستفاده قرار گیرند.

References

1. Khazaei, Saeed (2012). Ayandeh-Pajoohi (Future Studies), Tehran: Defense and Technology Sciences [in Persian].
2. Clough, Paul D. and Otterbacher Jahna (2023). Democratizing AI: from theory to practice, in: Carayannis, Elias G. & Grigoroudism Evangelos (Edited by). Handbook of Research on Artificial Intelligence, Innovation and Entrepreneurship. Cheltenham: Edward Elgar Publishing Limited.
3. Cover, Rob (2023). Identity and Digital Communication: Concepts, Theories, Practices. London: Routledge.
4. Gruber, Mirjam and Benedikter, Roland (2021). The Role of Women in Contemporary Technology and the Feminization of Artificial Intelligence and Its Devices. In :Keskin, Tugrul & David Kiggins, Ryan (Editors) (2021). Towards an International Political Economy of Artificial Intelligence. Switzerland: Palgrave Macmillan.
5. Jacobs Julian (2024). The artificial intelligence shock and socio-political polarization. Technological Forecasting & Social Change. Volume 199, February: 1-15.
6. Keskin, Tugrul & David Kiggins, Ryan (Editors) (2021). Towards an International Political Economy of Artificial Intelligence. Switzerland: Palgrave Macmillan.
7. Paul Thiele, Leslie (2021), Rise of the Centaurs: The Internet of Things Intelligence Augmentation, in: Keskin, Tugrul &David Kiggins, Ryan (Editors) (2021). Towards an International Political Economy of Artificial Intelligence. Switzerland: Palgrave Macmillan.
8. Rehorick, David Allan and Bentz, Valerie Malhotra (Edited by) (2008). Transformative Phenomenology: Changing Ourselves, Lifeworld's, and Professional Practice. Lanham: Lexington Books.
9. Rogerson, Kenneth and Sherman, Justin (2021). AI in Public Education: Humble Beginnings and Revolutionary Potential. In: Keskin, Tugrul & David Kiggins, Ryan (Editors) (2021). Towards an International Political Economy of Artificial Intelligence. Switzerland: Palgrave Macmillan.
10. Rosiers, David Perez-Des (2021). AI Application in Surveillance for Public Safety: Adverse Risks for Contemporary Societies. In: Keskin, Tugrul & David Kiggins, Ryan (Editors) (2021). Towards an International Political Economy of Artificial Intelligence. Switzerland: Palgrave Macmillan.
11. Salas-Pilco, Sdenka Zobeida (2021). Comparison of National Artificial Intelligence (AI): Strategic Policies and Priorities, in: Keskin, Tugrul & David Kiggins, Ryan (Editors) (2021). Towards an International Political Economy of Artificial Intelligence. Switzerland: Palgrave Macmillan.
12. Simonc˘ic˘, Katja and Jerele, Tonja, Democratizing the Governance of AI: From Big Tech Monopolies to Cooperatives in: Zavrsnik, Ales and Katja Simoncic (Editors) (2022). Artificial Intelligence, Social Harms and Human Rights. Cham, Switzerland: Palgrave Macmillan.
13. Yankoski, Michael; William Theisen, Ernesto Verdeja, and Walter J. Scheirer (2021). Artificial Intelligence for Peace: An Early Warning System for Mass Violence, In: Keskin, Tugrul & David Kiggins, Ryan (Editors) (2021). Towards an International Political Economy of Artificial Intelligence. Switzerland: Palgrave Macmillan.
14. Zekos, Georgios I. (2022). Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society. Switzerland: Springer.