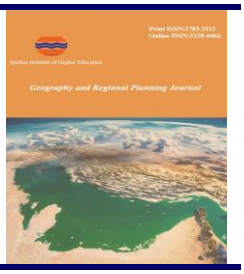
Iranian Association of Geopolitical

Geography and Regional Planning

ISSN (Print): 2783-2112 - ISSN (Online): 2228-6462

Homepage: https://www.jgeoqeshm.ir/



Dimensions of the security geography of artificial intelligence in the European Union

Vahid Mohammadi[1], Ardeshir Sanaei[2]✉, Arsalan Ghorbani[3], Ali Tabatabai[4]

1.PhD Student, Political Sciences, Department of International Relations, Islamic Azad University, Center Branch,Tehran, Iran. Email: mahdimohammad11@yahoo.com

2.Associate Professor, Political Sciences, Department of International Relations, Islamic Azad University, Center Branch, Tehran, Iran. Email: ardeshir_sanaie@yahoo.com

3.Associate Professor, Political Sciences, Department of International Relations, Kharazmi University, Tehran, Iran. Email: ghorbani@khu.ac.ir

4.Assistant Professor, Political Sciences, Department of International Relations, Islamic Azad University, Center Branch, Tehran, Iran Email: ali_tabatabaie@yahoo.com

ARTICLE INFO

Article type:
Research Paper

Article history:
Received: 1 July 2025
Revised: 10 August 2025
Accepted: 1 November 2025
Published: 30 November 2025

Keywords:
Artificial Intelligence
Digital Governance of the European Union
Cybersecurity
Algorithmic Bias
AI Regulations and Standardization

Abstract

Artificial Intelligence (AI), as one of the advanced technologies of the present era, has profound impacts on various aspects of society, particularly in the fields of cybersecurity and digital governance. This research aims to examine the challenges and opportunities of AI in enhancing security within the European Union, analyzing the role of this technology in strengthening digital governance and addressing cyber threats. The research methodology is qualitative and analytical, conducted through documentary studies and content analysis of relevant laws and reports concerning AI and cybersecurity in the European Union. The findings indicate that the European Union faces numerous challenges in regulating the use of AI, with the most significant issues being algorithmic bias, ethical concerns, and a lack of international coordination in AI regulation. However, this research also revealed that AI provides substantial opportunities to strengthen cybersecurity and foster international collaboration. Therefore, it is suggested that the European Union engage in international interactions with allied countries to enhance cybersecurity and AI governance, and develop global frameworks for the safe and ethical use of this technology.

How to cite: Mohammadi, V., Sanaei, A., Ghorbani, A., & Tabatabaei, S. A. (2025). Dimensions of the security geography of artificial intelligence in the European Union. *Geography and Regional Planning*, 15 (61), 239-255. https://doi.org/ 10.22034/jgeoq.2025.562996.4376

Publisher: Qeshm Institute of Higher Education

DOI: https://doi.org/10.22034/jgeoq.2025.562996.4376

Introduction

Artificial Intelligence (AI) has rapidly become a transformative strategic technology with significant implications for global security, geopolitics, and digital governance. While major powers such as the United States and China are leveraging AI to strengthen their economic, military and cyber capabilities, the European Union faces a dual challenge: managing the security risks associated with AI-such as algorithmic bias, privacy violations, cyber vulnerabilities, and ethical concerns-while simultaneously trying to harness AI as an opportunity to enhance digital sovereignty, cyber resilience, and its geopolitical standing. Despite recent regulatory efforts, including the 2024 EU Artificial Intelligence Act, the Union still struggles with structural dependencies, fragmented innovation capacity, and the need for international regulatory alignment. The core problem addressed in this study is how the EU can effectively mitigate emerging AI-driven security threats while exploiting the opportunities of AI to strengthen digital sovereignty, cybersecurity, and its competitive role in the international system.

Methodology

This study is qualitative and descriptive-analytical in nature, aiming to examine the challenges and opportunities of artificial intelligence (AI) in enhancing digital sovereignty and security in the European Union (EU). Data were collected using a library-based and documentary approach, including scientific sources, research articles, European Commission reports, and legal documents. The data were processed through qualitative content analysis and comparative analysis. Qualitative content analysis provided an in-depth examination of scientific and legal texts, identifying patterns, trends, and relationships in the use of AI for cybersecurity and digital governance, while comparative analysis evaluated EU policies against other global powers, such as the United States and China, to identify strengths and weaknesses. This research is grounded in the existing literature on AI, cybersecurity, and the legal and ethical challenges and opportunities of this technology in the EU. In particular, studies addressing global competition and its impact on EU policies regarding digital governance and AI regulation were examined. The study population consists of reputable scientific sources, including legal documents, research articles, international reports, and existing analyses on cybersecurity and AI. Limitations include restricted access to certain EU internal sources and the rapid evolution of AI technologies, which may quickly render some findings outdated. Ultimately, this research seeks to answer the central question: how can the European Union address AI-driven security challenges while leveraging the opportunities of this technology to strengthen its digital sovereignty and regional security?

Results and Discussion

In the contemporary world, artificial intelligence (AI) has emerged as a transformative technology with profound impacts on society, the economy, and security. The European Union (EU) has made significant efforts to leverage AI to enhance cybersecurity and digital governance, yet its application faces multiple challenges that require careful examination. A major challenge is algorithmic bias, which can lead to discrimination and human rights violations, particularly in the EU's pursuit of a transparent and fair regulatory system (Azin et al., 2024; Verma, 2019). The EU AI Act of 2024 seeks to mitigate such risks while supporting innovation by establishing clear guidelines for high-risk AI applications, aligning with the recommendations of Brynjolfsson & McAfee (2017) regarding oversight and regulation. Regulatory and infrastructure gaps persist, especially in implementing data protection and cybersecurity standards across public and private sectors, which may slow innovation compared to less regulated environments like the United States and China (Birkstedt et al., 2023; Rodrigues, 2020; European Commission, 2020). Globally, competition in AI-particularly in military and economic domains-has intensified, with the United States and China outpacing the EU in investment and industrial leadership, a trend exacerbated by geopolitical crises such as the Ukraine conflict (Mokry & Gurol, 2024). Nevertheless, AI offers significant opportunities for the EU, including strengthening cybersecurity, crisis

management, and digital infrastructure, while international collaborations, for instance with Brazil and Singapore, can enhance the EU's role in setting global AI standards and advancing digital governance(Chiappetta, 2023). These findings collectively indicate that while AI presents regulatory, ethical, and strategic challenges, it simultaneously offers a pathway for the EU to reinforce its cybersecurity, digital sovereignty, and global influence in the AI landscape.

Conclusion

Artificial intelligence (AI) has emerged as a transformative technology with wide-ranging impacts on all aspects of human life. While many global actors are leveraging AI to advance their economic, social, and security objectives, the European Union (EU) faces unique challenges and opportunities in this domain. This study found that although the EU has made significant strides in strengthening digital governance and oversight through innovative legislation, such as the 2024 AI Act, it continues to confront major challenges related to algorithmic bias, ethical concerns, human rights protection, and international regulatory coordination. A critical challenge is the lack of a leading AI industry, which limits the EU's capacity to compete with advanced actors like the United States and China, despite its strong research and innovation capabilities. Regulatory complexity and insufficient investment have further constrained the region from fully exploiting AI opportunities. Nevertheless, international collaborations-particularly in cybersecurity and crisis management-offer avenues to enhance the EU's global position in AI. Strengthening digital infrastructure, supporting private and public sector adoption, and increasing investment in AI, especially for startups and SMEs, are essential for the EU to become a leading global AI actor. Future research should focus on analyzing AI's impacts on EU security policies, exploring strategies for international cooperation, examining long-term effects of AI in cybersecurity, and developing effective regulatory and ethical frameworks for AI applications in defense and security. Comparative studies of different national AI regulatory approaches could also provide valuable insights for managing global AI challenges and promoting safe and ethical AI governance.

Ethical considerations

Following the principles of research ethics

The authors have observed the principles of ethics in conducting and publishing this scientific research, and this is confirmed by all of them.

Data Availability Statement

Data available on request from the authors.

Acknowledgements

First author: Preparation of samples, conducting experiments and collecting data, performing calculations, statistical analysis of data, analysis and interpretation of information and results, preparing a draft of the article.

Second author: Preparation of samples, conducting experiments and collecting data, performing calculations, statistical analysis of data, analysis and interpretation of information and results, preparing a draft of the article.

Third author: Preparation of samples, conducting experiments and collecting data, performing calculations, statistical analysis of data, analysis and interpretation of information and results, preparing a draft of the article.

Fourth author: Preparation of samples, conducting experiments and collecting data, performing calculations, statistical analysis of data, analysis and interpretation of information and results, preparing a draft of the article.

Ethical Considerations

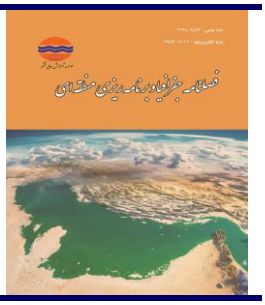
The authors affirm that they have adhered to ethical research practices, avoiding plagiarism, misconduct, data fabrication or falsification, and have provided their consent for this article's publication.

Funding

This research was conducted without any financial support from Payam Noor University.

Conflict of Interest

The authors declare no conflict of interes



فصلنامه جغرافیا و برنامه ریزی منطقه ای

شاپا چاپی: ۶۴۶۲- ۲۲۲۸ شاپا الکترونیکی: ۲۱۱۲ -۲۷۸۳

Homepage: https://www.jgeoqeshm.ir/

انجمن ژئوپلیتیک ایران

ابعاد جغرافیای امنیتی هوش مصنوعی در اتحادیه اروپا

وحید محمدی[۱]، اردشیر ثنایی[۲]✉، ارسلان قربانی[۳]، سید علی طباطبائی[۴]

۱. دانشجوی دکتری، رشته علوم سیاسی، گروه روابط بین الملل، دانشگاه آزاد اسلامی واحد تهران مرکز، تهران، ایران. رایانامه: mahdimohammad11@yahoo.com

۲. دانشیار رشته علوم سیاسی، گروه روابط بین‌الملل، دانشگاه آزاد اسلامی واحد تهران مرکز، تهران، ایران. رایانامه:ardeshir_sanaie@yahoo.com

۳. دانشیار رشته علوم سیاسی، گروه روابط بین‌الملل، دانشگاه خوارزمی تهران، تهران، ایران. رایانامه: ghorbani@khu.ac.ir

۴. استادیار رشته علوم سیاسی، گروه روابط بین‌الملل، دانشگاه آزاد اسلامی واحد تهران مرکز، تهران، ایران. رایانامه:ali_tabatabaie@yahoo.com

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۰ تیر ۱۴۰۴

تاریخ بازنگری: ۱۹ مرداد ۱۴۰۴

تاریخ پذیرش: ۱۰ آبان ۱۴۰۴

تاریخ انتشار: ۹ آذر ۱۴۰۴

کلیدواژه ها:

هوش مصنوعی

حاکمیت دیجیتال

اتحادیه اروپا

امنیت سایبری

سوگیری الگوریتمی

مقررات و استانداردگذاری

هوش مصنوعی

چکیده

هوش مصنوعی به عنوان یکی از فناوری‌های پیشرفته در عصر حاضر، تأثیرات عمیقی بر ابعاد مختلف جامعه، به‌ویژه در زمینه امنیت سایبری و حاکمیت دیجیتال، دارد. این تحقیق با هدف بررسی چالش‌ها و فرصت‌های هوش مصنوعی در ارتقای امنیت در اتحادیه اروپا، به تحلیل نقش این فناوری در تقویت حاکمیت دیجیتال و مقابله با تهدیدات سایبری پرداخته است. روش تحقیق به‌صورت کیفی و تحلیلی بوده و از طریق مطالعه اسنادی و تحلیل محتوای قوانین و گزارش‌های مربوط به هوش مصنوعی و امنیت سایبری اتحادیه اروپا انجام گرفت. یافته‌ها نشان می‌دهند که اتحادیه اروپا با چالش‌های متعددی در زمینه نظارت بر استفاده از هوش مصنوعی مواجه است که مهم‌ترین آن‌ها شامل سوگیری الگوریتمی، نگرانی‌های اخلاقی و عدم هماهنگی بین‌المللی در تنظیم مقررات هوش مصنوعی است. با این حال، این تحقیق همچنین نشان داد که هوش مصنوعی فرصت‌هایی قابل توجه برای تقویت امنیت سایبری و توسعه همکاری‌های بین‌المللی فراهم می‌آورد. بنابراین، تحلیل تعاملات بین‌المللی اتحادیه اروپا و کشورهای هم‌پیمان در زمینه امنیت سایبری و هوش مصنوعی و توسعه چارچوب‌های جهانی برای استفاده ایمن و اخلاقی از این فناوری پیشنهاد می‌گردد.

استناد: محمدی، وحید؛ ثنایی، اردشیر؛ قربانی، ارسلان؛ طباطبائی، سید علی. (۱۴۰۴). ابعاد جغرافیای امنیتی هوش مصنوعی در اتحادیه اروپا. *جغرافیا و برنامه‌ریزی منطقه‌ای*، ۱۵(۶۱)، ۲۳۹-۲۵۵. DOI:10.22034/jgeoq.2025.562996.4376

ناشر: موسسه آموزش عالی قشم

مقدمه

در دنیای امروزی، هوش مصنوعی (AI) به یکی از مهم‌ترین و تحول‌آفرین‌ترین فناوری‌ها در عرصه‌های مختلف زندگی انسانی تبدیل شده است. این فناوری، که ابتدا تنها به‌عنوان یک ابزار علمی و تحقیقاتی در نظر گرفته می‌شد، اکنون به ابزاری پیچیده و حیاتی برای حل مسائل پیچیده و بهبود فرآیندهای مختلف در زمینه‌های اقتصادی، اجتماعی، نظامی و امنیتی تبدیل شده است. در این راستا، هوش مصنوعی به‌ویژه در حوزه امنیت سایبری و مدیریت داده‌های کلان، نقش برجسته‌ای پیدا کرده است. در گذشته، تصور می‌شد که این فناوری تأثیر چندانی بر سیاست‌های جهانی و روابط بین‌الملل نخواهد داشت، اما در سال‌های اخیر، به دلیل پیشرفت‌های سریع و کاربردهای گسترده آن، هوش مصنوعی به‌عنوان یک ابزار استراتژیک در رقابت‌های ژئوپلیتیکی و امنیتی جهانی مطرح شده است.(Brynjolfsson & McAfee, 2017)

امروزه، فناوری‌های هوش مصنوعی نه‌تنها در عرصه‌های اقتصادی و نظامی بلکه در بخش‌های دیپلماتیک و امنیتی نیز به یکی از ارکان اصلی قدرت کشورها تبدیل شده است. در این میان، اتحادیه اروپا به‌عنوان یک قدرت جهانی، به‌ویژه در زمینه امنیت سایبری، با چالش‌ها و فرصت‌های زیادی در استفاده از این فناوری مواجه است. برخلاف کشورهای پیشرفته مانند ایالات متحده و چین که در حال سرمایه‌گذاری‌های عظیم در زمینه هوش مصنوعی هستند، اتحادیه اروپا هنوز با مشکلاتی نظیر عدم توسعه صنعت پیشرو در این فناوری و وابستگی به بازیگران خارجی روبه‌روست .(Mokry & Gurol, 2024) به‌ویژه در حوزه امنیت سایبری، هوش مصنوعی می‌تواند ابزاری مؤثر در مقابله با تهدیدات نوین و پیچیده باشد، اما چالش‌های زیادی همچون سوگیری الگوریتمی، مسائل اخلاقی و نقض حریم خصوصی نیز در این مسیر وجود دارد.(Verma, 2019)

در این راستا، اتحادیه اروپا در سال ۲۰۲۴، قانونی را به نام "قانون هوش مصنوعی" تصویب کرد تا با ایجاد چارچوب‌های نظارتی دقیق‌تر، از خطرات این فناوری جلوگیری کرده و از آن برای تقویت حاکمیت دیجیتال و امنیت سایبری خود بهره‌برداری نماید .(European Commission, 2024)با این حال، این قوانین به‌تنهایی نمی‌توانند راه‌حل‌های کامل برای چالش‌های ناشی از هوش مصنوعی باشند. به‌ویژه با توجه به نیاز به هماهنگی بین‌المللی در زمینه مقررات هوش مصنوعی، این مسئله به یکی از بزرگ‌ترین چالش‌های اتحادیه اروپا تبدیل شده است. اتحادیه اروپا در تلاش است تا از یک‌سو با توسعه مقررات سخت‌گیرانه، نظارت بیشتری بر بازار داخلی خود اعمال کند و از سوی دیگر، به‌عنوان یک بازیگر جهانی در تنظیم مقررات هوش مصنوعی نقش‌آفرینی کند (European Parliament, 2021).

تحقیقات مختلف نشان داده‌اند که استفاده از هوش مصنوعی در زمینه امنیت، همچون استفاده از این فناوری در صنایع دفاعی و نظامی، به یکی از اصلی‌ترین جنبه‌های رقابت جهانی تبدیل شده است. به‌ویژه پس از بحران اوکراین، رقابت‌های استراتژیک میان قدرت‌های بزرگ به‌ویژه در حوزه هوش مصنوعی شدت یافته است. در این راستا، تحقیقات پیشین در مورد چالش‌ها و فرصت‌های هوش مصنوعی، به‌ویژه در زمینه امنیت سایبری، نشان می‌دهند که اگر چه هوش مصنوعی می‌تواند ابزاری برای تقویت امنیت و مقابله با تهدیدات سایبری باشد، اما همزمان با چالش‌هایی چون سوگیری الگوریتمی، نقض حریم خصوصی و تهدیدات اخلاقی نیز مواجه است .(Azin et al., 2024; Oseni et al., 2020) این چالش‌ها می‌تواند بر اعتماد عمومی به فناوری‌های هوش مصنوعی تأثیر منفی بگذارد و منجر به افزایش نگرانی‌ها در سطح بین‌المللی شود (Birkstedt et al., 2023; Verma, 2019). علاوه بر این، برخی از پژوهش‌ها نیز به بررسی نقض حریم خصوصی ناشی از استفاده از هوش مصنوعی در تصمیم‌گیری‌های امنیتی پرداخته‌اند. به‌ویژه در اتحادیه اروپا، تلاش‌ها برای ایجاد قوانین و مقررات برای محافظت از حقوق فردی در برابر تهدیدات سایبری و دستکاری داده‌ها، همچنان به چالش‌هایی بزرگ تبدیل شده است (Horowitz,

.(2018در این راستا، کمیسیون اروپا با توجه به نگرانی‌های امنیتی، قوانین جدیدی را تصویب کرده است که هدف آن حفاظت از داده‌های شخصی و ایجاد استانداردهای مناسب برای استفاده از هوش مصنوعی در بخش‌های مختلف، از جمله امنیت سایبری است (European Commission, 2020). ضرورت انجام این پژوهش نیز به‌ویژه از آنجا اهمیت پیدا می‌کند که اتحادیه اروپا در تلاش است تا با وضع قوانین و استانداردهای هوش مصنوعی، نه‌تنها از تهدیدات امنیتی ناشی از این فناوری جلوگیری کند، بلکه بتواند به‌عنوان یک بازیگر پیشرو در عرصه جهانی در زمینه مقررات هوش مصنوعی شناخته شود. در این راستا، مطالعه و تحلیل چالش‌ها و فرصت‌های قانونی و امنیتی هوش مصنوعی در اتحادیه اروپا، می‌تواند به‌عنوان یک راهکار برای تقویت حاکمیت دیجیتال و امنیت سایبری در این منطقه عمل کند.

مسئله اصلی این تحقیق این است که اتحادیه اروپا چگونه می‌تواند ضمن رفع چالش‌های امنیتی ناشی از هوش مصنوعی، فرصت‌های این فناوری را برای تقویت حاکمیت دیجیتال و امنیت منطقه‌ای خود به کار گیرد. همچنین، چگونه اتحادیه اروپا می‌تواند در شرایط کنونی، که رقبای جهانی در حال پیشرفت سریع در این حوزه هستند، از فرصت‌های هوش مصنوعی برای بهبود جایگاه خود در نظام بین‌الملل استفاده کند؟ با این حال، تنظیم مقررات برای هوش مصنوعی و مدیریت چالش‌های آن در مقیاس جهانی همچنان موضوعی پیچیده است. یکی از مسائل کلیدی، تعارض میان قوانین ملی و استانداردهای بین‌المللی است که می‌تواند منجر به ایجاد بازارهای مجزا و رقابتی نابرابر شود. علاوه بر این، نظارت بر توسعه فناوری‌های نوین هوش مصنوعی و پیش‌بینی اثرات بلندمدت آن‌ها بر جامعه و حقوق بشر، به چالشی بزرگ برای اتحادیه اروپا تبدیل شده است (European Parliament, 2021). این مطالعه با هدف بررسی چالش‌ها و فرصت‌های هوش مصنوعی در اتحادیه اروپا، به ویژه در زمینه تقویت امنیت سایبری و حاکمیت دیجیتال، به تحلیل قوانین تصویب‌شده در این زمینه می‌پردازد. همچنین، به بررسی این نکته می‌پردازد که اتحادیه اروپا چگونه می‌تواند ضمن حفظ امنیت دیجیتال و حقوق بشر، به عنوان یک بازیگر مؤثر در عرصه جهانی هوش مصنوعی شناخته شود. سوال اصلی این تحقیق این است که اتحادیه اروپا چگونه می‌تواند چالش‌های امنیتی ناشی از هوش مصنوعی را برطرف کند و از فرصت‌های این فناوری برای تقویت حاکمیت دیجیتال و امنیت منطقه‌ای خود بهره‌برداری نماید؟

پیشینه پژوهش

هوش مصنوعی در حوزه‌ها و بخش‌های مختلف در اغلب کشورهای دنیا مورد تحقیق و پژوهش قرار گرفته است. بخش سیاستگذاری دولتی و ابعاد آن یکی از این بخش‌ها می‌باشد که در این تحقیق پیشینه‌های تحقیقاتی آن خصوصا تحقیقات مرتبط با این حوزه در اتحادیه اروپا مرور شده است. آذین و همکاران (۱۴۰۳) دریافتند که آمریکا و روسیه با استفاده از قابلیت‌های هوش مصنوعی در حوزه نظامی، تهدیدی متقابل ایجاد کرده‌اند که ناشی از بی‌اعتمادی و رقابت راهبردی میان آن‌هاست، وضعیتی که پس از بحران اوکراین تشدید شده و به برداشت‌های اشتباه و چرخه‌ای از تنش‌های غیرقابل‌بهبود منجر شده است. در همین راستا، محمدی و همکاران (۱۴۰۲) نشان دادند که تأثیرات هوش مصنوعی تنها به حوزه نظامی محدود نبوده و در عرصه سیاسی و اجتماعی نیز موجب افزایش پیچیدگی، عدم‌قطعیت و شکل‌گیری فضایی مبهم، به‌ویژه در ایالات متحده آمریکا، شده است. این وضعیت، که نتیجه گسترش سریع ابزارهای هوش مصنوعی است، نشان‌دهنده تغییرات بنیادین در فرایندهای تصمیم‌گیری و سیاست‌گذاری است. ون نوردت و میسوراکا[1] (۲۰۲۲) نیز دریافتند که در اتحادیه اروپا، هوش مصنوعی عمدتاً برای

[1] Van Noordt & Misuraca

بهبود خدمات عمومی و مدیریت داخلی دولت‌ها به کار می‌رود و تنها در موارد محدودی بر تصمیم‌گیری‌های سیاسی تأثیر مستقیم دارد، که نشان‌دهنده تفاوت در نحوه بهره‌گیری از این فناوری میان قدرت‌های جهانی است. بااین‌حال، همان‌طور که جوستو هانانی[1] (۲۰۲۲) مطرح می‌کند، یکی از چالش‌های اساسی در سیاست‌گذاری هوش مصنوعی در اتحادیه اروپا، مدیریت اعتماد شهروندان به سیاست‌های دولتی است، چراکه ممکن است سطح واقعی اعتماد عمومی با میزان قابل‌اعتماد بودن هوش مصنوعی در عمل همخوانی نداشته باشد. در مجموع، یافته‌های این تحقیقات نشان می‌دهد که هوش مصنوعی در عرصه‌های نظامی، سیاسی، اجتماعی و حکمرانی، در حال ایجاد تغییرات اساسی است که نه‌تنها به رقابت‌های راهبردی میان قدرت‌های جهانی دامن زده، بلکه بر ساختارهای تصمیم‌گیری و اعتماد عمومی نیز تأثیر گذاشته است.

روش تحقیق

این تحقیق از نوع کیفی و توصیفی–تحلیلی است که با هدف بررسی چالش‌ها و فرصت‌های هوش مصنوعی در تقویت حاکمیت دیجیتال و امنیت اتحادیه اروپا انجام شده است. برای گردآوری داده‌ها، از روش کتابخانه‌ای و اسنادی استفاده شده و منابع مختلف علمی، مقالات تحقیقاتی، گزارش‌های کمیسیون اروپا و اسناد قانونی بررسی شده‌اند. داده‌ها از طریق تحلیل محتوای کیفی و تحلیل مقایسه‌ای پردازش شده‌اند. تحلیل محتوای کیفی به تحلیل دقیق و عمقی متون علمی و قانونی پرداخته و به شناسایی الگوها، روندها و روابط موجود در استفاده از هوش مصنوعی در امنیت سایبری و حاکمیت دیجیتال کمک می‌کند، در حالی که تحلیل مقایسه‌ای به مقایسه سیاست‌های اتحادیه اروپا با سایر کشورها و قدرت‌های جهانی همچون ایالات متحده و چین می‌پردازد تا نقاط قوت و ضعف آن را شناسایی کند. این تحقیق بر پایه پیشینه پژوهشی موجود در زمینه هوش مصنوعی، امنیت سایبری، و چالش‌ها و فرصت‌های قانونی و اخلاقی این فناوری در اتحادیه اروپا استوار است. به‌ویژه مطالعات مرتبط با رقابت‌های جهانی و تأثیرات آن بر سیاست‌های اتحادیه اروپا در زمینه حاکمیت دیجیتال و تنظیم‌گری هوش مصنوعی در این تحقیق مورد بررسی قرار گرفته است. جامعه آماری این پژوهش شامل منابع علمی معتبر در زمینه‌های مختلف از جمله اسناد قانونی، مقالات تحقیقاتی، گزارش‌های بین‌المللی و تحلیل‌های موجود در زمینه امنیت سایبری و هوش مصنوعی است. محدودیت‌های این تحقیق شامل دسترسی به برخی منابع داخلی اتحادیه اروپا و تغییرات سریع در فناوری‌های هوش مصنوعی است که ممکن است به سرعت قدیمی شوند. در نهایت، این تحقیق به‌دنبال پاسخ به سوال اصلی خود است که اتحادیه اروپا چگونه می‌تواند چالش‌های امنیتی ناشی از هوش مصنوعی را برطرف کند و از فرصت‌های این فناوری برای تقویت حاکمیت دیجیتال و امنیت منطقه‌ای خود بهره‌برداری نماید.

هوش مصنوعی

هوش مصنوعی یکی از موضوعات کلیدی در بخش‌های تجاری در سال‌های اخیر بوده است و عامل اصلی نوآوری مخرب در سال‌های آینده دیده می‌شود. این اصطلاح، همانطور که توسط کمیسیون اروپا تعریف شده است، به سیستم هایی اشاره دارد که با تجزیه و تحلیل محیط خود و انجام اقدامات – با درجاتی از خودمختاری برای دستیابی به اهداف خاص، رفتار هوشمندانه ای از خود نشان می دهند. بنابراین، می‌توانیم هوش مصنوعی را به عنوان هر سیستمی که قادر به انجام کارهایی است که معمولاً در انسان‌ها هوشمند می‌دانیم، در نظر بگیریم. امروزه برای کاربردهای هوش مصنوعی، این معمولاً به شکل شناخت الگوها، استنتاج، تصمیم گیری مورد به مورد یا درگیر شدن در مکالمه است (Torki, 2024).

[1] Justo-Hanani

در واقع، مهم است که هوش مصنوعی را به عنوان یک اصطلاح کلی بشناسیم که فناوری‌های مختلفی را پوشش می‌دهد که هر کدام برای حل یک مشکل خاص طراحی شده‌اند. هوش مصنوعی به عنوان یک مفهوم و زمینه تحقیقاتی از دهه ۱۹۵۰ وجود داشته است. با این حال، چندین محرک کلیدی در تسریع پذیرش صنعت که امروزه مشاهده می شود، کمک می کنند. حجم داده‌های موجود برای مدل‌های هوش مصنوعی که می‌توانند از آن‌ها یاد بگیرند، بیش از هر زمان دیگری است و با سرعت در حال رشد است، در عین حال، دموکراسی‌سازی فزاینده الگوریتم‌ها و پلتفرم‌ها، اکوسیستمی را ایجاد کرده است که در آن راه‌حل‌های هوش مصنوعی می‌توانند با سهولت بیشتری توسط طیف وسیع‌تری از افراد و سازمان‌ها آزمایش و پیاده‌سازی شوند (Al Ridhaw et al., 2020).

واضح است که تأثیر هوش مصنوعی در سراسر جهان یکسان نیست. علاوه بر این، بازار محصولات و راه‌حل‌های هوش مصنوعی نسبتاً جدید است، و بنابراین در سراسر و درون اکثر کشورها تکه‌تکه باقی می‌ماند.

نحوه عملکرد هوش مصنوعی

از سال ۱۹۵۶، زمانی که اصطلاح هوش مصنوعی توسط جان مک کارتی، دانشمند کامپیوتر آمریکایی، به عنوان «علم و مهندسی ساخت ماشین‌های هوشمند، به‌ویژه برنامه‌های هوشمند» ابداع و تعریف شد، هوش مصنوعی پیشرفت چشمگیری داشته است. امروزه به عنوان «مجموعه‌ای از فناوری‌هایی که داده‌ها، الگوریتم‌ها و قدرت محاسباتی را ترکیب می‌کند» (European Commission, 2022) شناخته می‌شود و به شیوه‌ای مثالی وابستگی خود را به تعامل تکنیک‌ها، اکتشافات و ایده‌ها نشان می‌دهد. دانشمندان کامپیوتر روشی را برای تجزیه و تحلیل داده‌ها توسعه داده‌اند که ساخت مدل تحلیلی را خودکار می‌کند، که از الگوریتم‌هایی استفاده می‌کند که به طور مکرر از داده‌ها یاد می‌گیرند و به رایانه‌ها اجازه می‌دهد تا بینش‌های پنهان را بدون برنامه‌ریزی صریح به جایی که باید نگاه کنند، به نام یادگیری ماشین[1] پیدا کنند (Moroney, 2020).

دانشمندان کامپیوتر روش یادگیری عمیق را توسعه داده‌اند، شکلی از یادگیری ماشینی که رایانه‌ها را قادر می‌سازد از تجربه بیاموزند و جهان را بر اساس سلسله مراتبی از مفاهیم درک کنند. بنابراین، کامپیوتر دانش را از تجربه جمع آوری می کند. بنابراین نیازی به تعامل اپراتور انسانی با کامپیوتر نیست (Kuhi et al., 2022). استفاده از چنین روش‌هایی در ابررایانه‌هایی مانند Deep Blue شرکت آی‌بی‌ام با سرعت و ظرفیت ذخیره‌سازی فوق‌العاده‌اش به دومی در سال ۱۹۹۷ اجازه داد تا گری کاسپاروف قهرمان شطرنج جهان را شکست دهد و نشان‌دهنده ظهور اولین مرحله توسعه هوش مصنوعی، یعنی « Artificial Narrow» بود. اگرچه قدرت کامپیوتر برای عملکرد هوش مصنوعی ضروری است، حتی ابرکامپیوترهایی مانند Deep Blue یا حتی بسیار قدرتمندتر چینی Tianhe-۲ که می تواند ۳۴ کوادریلیون محاسبه در ثانیه انجام دهد و می تواند مسائل پیچیده را به سرعت حل کند، نسبت به اطلاعاتی که سازندگان آنها در اختیار آنها قرار می دهند، هیچ درکی از چیزهای دیگر ندارند (Babu et al., 2024).

در حال حاضر، هوش مصنوعی به مرحله بعدی توسعه خود، یعنی «هوش عمومی مصنوعی[2]» نزدیک می شود. هوش عمومی مصنوعی نشان دهنده «هوش مصنوعی سطح انسانی» خواهد بود، به این معنی که رایانه‌ها «از هر نظر به اندازه انسان‌ها باهوش خواهند بود و قادر به انجام تمام وظایف فکری انسان‌ها خواهند بود». در مرحله پایانی خود، به نام «فوق هوش

[1] Machine Learning
[2] AGI

مصنوعی[1]»، هوش مصنوعی «بسیار باهوش‌تر از بهترین مغزهای انسان در عمل در هر زمینه‌ای از جمله خلاقیت علمی، خرد عمومی و مهارت‌های اجتماعی» خواهد بود (Farhad et al., 2024). یک راهگشای بسیار مهم در برنامه های جدید هوش مصنوعی، استفاده از «شبکه های عصبی مصنوعی[2]»، یک «پارادایم پردازش اطلاعات است که از روشی که سیستم های بیولوژیکی مانند مغز، اطلاعات را پردازش می کنند» الهام گرفته شده است. شیمون اولمن شبکه‌های عصبی هوش مصنوعی را «رویکردی بسیار تقلیل‌گرایانه برای مدل‌سازی مدارهای قشر مغز» توصیف می‌کند و مشاهده می‌کند که «این مدل الهام‌گرفته از مغز از لایه‌های متوالی نورون در شکل اصلی فعلی خود که به عنوان معماری «شبکه عمیق» شناخته می‌شود، ساخته شده است. عناصری مانند، که توسط وزن‌های قابل تنظیم به هم متصل شده‌اند، به نام همتایان بیولوژیکی خود «سیناپس» نامیده می‌شوند و مانند انسان ها با مثال یاد می گیرند. شبکه‌های عصبی مصنوعی توانایی استخراج معنی از داده‌های پیچیده یا غیردقیق را دارند، می‌توانند برای استخراج الگوها و تشخیص روندهایی استفاده شوند که بسیار پیچیده‌تر از آن هستند که توسط انسان یا سایر تکنیک‌های رایانه‌ای مورد توجه قرار گیرند. یک شبکه عصبی آموزش دیده را می توان به عنوان یک "متخصص" در دسته اطلاعاتی که برای تجزیه و تحلیل داده شده است در نظر گرفت (Agatonovic-Kustrin & Beresford, 2000).

هوش مصنوعی در اروپا

کمیسیون اروپا همچنین به ضرورت اتخاذ تدابیری برای مقابله مناسب با تغییرات تکنولوژیکی ایجاد شده توسط فناوری هوش مصنوعی پی برد. در بیانیه‌ای درباره «هوش مصنوعی برای اروپا» در ۲۵ آوریل ۲۰۱۸، پی‌نوشت ۱، اعلام کرد که ۱.۵ میلیارد یورو را تا سال ۲۰۲۰ به بودجه تحقیقاتی هوش مصنوعی اختصاص داده است. اتحادیه اروپا به‌عنوان یک کل (بخش‌های دولتی و خصوصی ترکیبی) باید تا پایان سال ۲۰۳۰ حداقل ۲۰ میلیارد یورو در تحقیق و توسعه هوش مصنوعی و سپس ۲۰ میلیارد یورو در سال برای دهه بعد سرمایه‌گذاری کند (Gianluca Misuraca, 2022 &van Noordt). کمیسیون همچنین نوعی «موجودی» از دستاوردها و قابلیت‌های مرتبط با هوش مصنوعی اروپا ارائه کرد و برنامه‌هایی را برای طیف وسیعی از اقدامات لازم برای اطمینان از اینکه اتحادیه اروپا می‌تواند تغییر ایجاد کند – و قهرمان رویکردی باشد که به نفع مردم و جامعه باشد، اعلام کرد. در کل.' برای دستیابی به این هدف، کمیسیون اعلام کرد که زمان آن رسیده است که تلاش های قابل توجهی انجام دهیم تا اطمینان حاصل شود که:

اروپا در چشم انداز هوش مصنوعی با سرمایه گذاری های جسورانه که با وزن اقتصادی آن مطابقت دارد، رقابتی است. این در مورد حمایت از تحقیق و نوآوری برای توسعه نسل بعدی فناوری‌های هوش مصنوعی و استقرار برای اطمینان از اینکه شرکت‌ها – به ویژه شرکت‌های کوچک و متوسط که ۹۹ درصد تجارت در اتحادیه اروپا را تشکیل می‌دهند – می‌توانند هوش مصنوعی را اتخاذ کنند، است. هیچ کس از تحول دیجیتال عقب نمانده است. هوش مصنوعی ماهیت کار را تغییر می‌دهد: مشاغل ایجاد می‌شوند، سایرین ناپدید می‌شوند و بیشتر آنها دگرگون می‌شوند. نوسازی آموزش در همه سطوح باید در اولویت دولت ها باشد.

فناوری های جدید بر اساس ارزش ها است. مقررات عمومی حفاظت از داده ها گامی مهم برای ایجاد اعتماد بود که در بلندمدت برای افراد و شرکت ها ضروری است. اینجاست که رویکرد پایدار اتحادیه اروپا به فناوری‌ها با پذیرش تغییرات مبتنی بر ارزش‌های اتحادیه مندرج در ماده ۲ معاهده اتحادیه اروپا، یعنی احترام به کرامت انسانی، آزادی، دموکراسی، برابری، حاکمیت

[1] ASI
[2] ANN

قانون و احترام، مزیت رقابتی ایجاد می‌کند. برای حقوق بشر، از جمله حقوق افراد متعلق به اقلیت ها. مانند هر فناوری دگرگون‌کننده، برخی از برنامه‌های کاربردی هوش مصنوعی ممکن است سؤالات اخلاقی و حقوقی جدیدی را مطرح کنند، برای مثال مربوط به مسئولیت یا تصمیم‌گیری بالقوه مغرضانه. بنابراین اتحادیه اروپا باید اطمینان حاصل کند که هوش مصنوعی در چارچوبی مناسب توسعه یافته و به کار گرفته شده است، که نوآوری را ترویج می کند و به ارزش ها و حقوق اساسی اتحادیه و همچنین اصول اخلاقی مانند پاسخگویی و شفافیت احترام می گذارد. اتحادیه اروپا این بحث را در صحنه جهانی رهبری خواهد کرد (European Commission, 2021).

در ۱۹ فوریه ۲۰۲۰، کمیسیون اتحادیه اروپا "کاغذ سفید در مورد هوش مصنوعی – رویکرد اروپایی به تعالی و اعتماد" را با هدف تعیین گزینه های سیاست در مورد چگونگی دستیابی به اهداف دوگانه ارتقاء جذب هوش مصنوعی و پرداختن به خطرات مرتبط با کاربردهای خاص این فناوری جدید منتشر کرد . طبق کتاب سفید، قابل اعتماد بودن یک پیش نیاز برای جذب هوش مصنوعی است زیرا هوش مصنوعی به عنوان یک فناوری دیجیتال، بخش مرکزی هر جنبه از زندگی مردم است. مردم باید بتوانند به آن اعتماد کنند. کمیسیون اتحادیه اروپا تاکید می کند که یک رویکرد مشترک اروپایی برای هوش مصنوعی برای رسیدن به مقیاس کافی و جلوگیری از تکه تکه شدن بازار واحد ضروری است. برای این هدف، کتاب سفید حاوی دو «بلوک سازنده» اصلی است: یک چارچوب سیاستی که اقدامات مشترک اتحادیه اروپا لازم برای بسیج منابع عمومی و خصوصی برای دستیابی به یک «اکوسیستم برتری» در طول کل زنجیره ارزش، با شروع تحقیق و نوآوری را تعیین می‌کند. و ایجاد انگیزه های مناسب برای تسریع در پذیرش راه حل های مبتنی بر هوش مصنوعی، از جمله توسط شرکت های کوچک و متوسط؛ و یک چارچوب نظارتی با عناصر کلیدی که یک «اکوسیستم اعتماد» منحصر به فرد ایجاد می‌کند و از انطباق با قوانین اتحادیه اروپا، از جمله قوانین حمایت از حقوق اساسی و حقوق مصرف‌کنندگان، به‌ویژه برای سیستم‌های هوش مصنوعی فعال در اتحادیه اروپا که خطر بالایی دارند، اطمینان حاصل می‌کند (European Commission, 2020).

اروپا در زمینه هوش مصنوعی جهانی

قبل از پرداختن به «چارچوب اخلاقی و قانونی مناسب» پیش‌بینی‌شده توسط کمیسیون، نگاهی اجمالی به ارزیابی سال ۲۰۱۸ کمیسیون از موقعیت اتحادیه اروپا در چشم‌انداز بین‌المللی رقابتی ضروری به نظر می‌رسد. در حالی که کمیسیون اعتراف کرد که اروپا در سرمایه گذاری خصوصی در هوش مصنوعی (۲.۴ تا ۳.۲ میلیارد یورو در سال ۲۰۱۶)، در مقایسه با آسیا (۶.۵–۹.۷ میلیارد یورو) و آمریکای شمالی (۱۲.۱ تا ۱۸.۶ میلیارد یورو) عقب است، اما ادعا کرد که اروپا «خانه است» به یک جامعه تحقیقاتی پیشرو در زمینه هوش مصنوعی و همچنین کارآفرینان نوآور و استارت‌آپ‌های فناوری عمیق. این مؤسسه تأکید کرد که اروپا بیشترین سهم را از ۱۰۰ مؤسسه تحقیقاتی برتر هوش مصنوعی در سراسر جهان به خود اختصاص داده است و ۳۲ مؤسسه در بین ۱۰۰ مؤسسه برتر جهانی از نظر استناد به مقالات تحقیقاتی مرتبط با هوش مصنوعی (در مقابل ۳۰ مؤسسه از ایالات متحده و ۱۵ مؤسسه از چین) دارند. در ادامه با اشاره به صنعت قوی اروپا، «تولید بیش از یک چهارم ربات‌های خدمات صنعتی و حرفه‌ای جهان (به عنوان مثال برای کشاورزی دقیق، امنیت، بهداشت، تدارکات)» و پیشرو در تولید، مراقبت‌های بهداشتی، حمل‌ونقل و فناوری‌های فضایی، ادامه داد. که همه به طور فزاینده ای به هوش مصنوعی متکی هستند (EU Commission, 2018).

هیچ یک از شرکت‌های اروپایی در بین شرکت‌های دیجیتال پیشرو در جهان قرار ندارد – که انباشته‌ای از پول نقد بی‌سابقه (اپل، گوگل، آمازون، مایکروسافت و فیس‌بوک معادل ۱۰ درصد تولید ناخالص داخلی) هستند. ایالات متحده و ژاپن، ارزش بازار و حجم اطلاعات حتی برای افراد عادی، و به طور فزاینده ای زیرساخت های اقتصاد اطلاعات را کنترل می کنند. حتی مایکروسافت اخیراً از دولت‌ها و شرکت‌های سراسر جهان خواسته است تا داده‌های بیشتری را با سایر سازمان‌ها به اشتراک بگذارند تا از تمرکز قدرت دیجیتال در دست ایالات متحده، چین و تعداد کمی از شرکت‌های بزرگ فناوری جلوگیری کنند. (Economist, 2024).

پیامدهای حقوقی و اخلاقی هوش مصنوعی اتحادیه اروپا

کمیسیون اتحادیه اروپا در بیانیه ۲۰۱۸ خود توجه زیادی به اطمینان از چارچوب قانونی و اخلاقی مناسب هوش مصنوعی کرد. در رابطه با چارچوب قانونی، این ارتباطات مقررات حفاظت از داده های عمومی (GDPR) اشاره کرد که از قبل استاندارد بالایی از حفاظت از داده های شخصی را تضمین می کند. از جمله، به طور خاص به ماده ۲۲ اشاره کرد که «موضوع داده‌ها» را با این حق که «مشمول تصمیم‌گیری صرفاً مبتنی بر پردازش خودکار، از جمله نمایه‌سازی نباشد» (EU Commission, 2018).

یک «سند کاری کارکنان» در مورد مسئولیت برای فناوری‌های دیجیتال نوظهور از جمله مروری بر قوانین ایمنی مربوط به فناوری‌های دیجیتال نوظهور در سطح اتحادیه اروپا ارائه می‌کند و به اصول قوانین مسئولیت قراردادی اضافی قابل اجرا در همین زمینه می‌پردازد. همچنین شامل مطالعات موردی مربوط به دستگاه‌ها و سیستم‌های قدرت هوش مصنوعی (هواپیماهای بدون سرنشین [پهپادها] و اتومبیل‌های خودران) و اینترنت اشیا (سیستم‌های خانه‌های هوشمند و حملات سایبری) بود و به جنبه‌هایی از دستورالعمل مسئولیت محصولات ۱۹۸۵ اشاره کرد. تجزیه و تحلیل بیشتر.

ضمیمه "فهرست قوانین اتحادیه اروپا" نشان می دهد که اتحادیه اروپا در حال حاضر دارای ۶۴ دستورالعمل و مقررات مربوط به مسئولیت، ایمنی و غیره است! کتاب سفید به خطرات جدیدی می‌پردازد که فناوری‌های هوش مصنوعی زمانی که فناوری‌ها در محصولات و خدمات تعبیه شده‌اند، برای کاربران ایجاد می‌کند، به‌عنوان مثال در نتیجه نقص‌هایی در فناوری تشخیص شی نصب شده در یک خودروی خودمختار، و یک چارچوب قانونی بهبودیافته می‌تواند به آنها رسیدگی کند (European Commission, 2020).

حاکمیت دیجیتال اتحادیه اروپا در امنیت: رهبری جهانی یا قدرت هنجاری؟

فقدان صنعت فناوری دیجیتال و سایر شکل‌های سرمایه‌گذاری از بخش دفاعی، اتحادیه اروپا را از ایفای نقش فعالانه در تعجیل به برتری فناوری جهانی باز می‌دارد. به طور خاص، اتحادیه اروپا در حوزه هوش مصنوعی عقب مانده است، در حالی که رقبای اصلی به طور مداوم از مرزهای فن آوری در داده کاوی، پیچیدگی الگوریتم ها و ظرفیت محاسباتی که توسط توسعه رایانه های کوانت هدایت می شود، جلوتر می روند. در سناریوی کنونی، پیش‌بینی اینکه اتحادیه اروپا در آینده نزدیک به عقب خواهد افتاد دشوار است. با توجه به پیامدهای اقتصادی، امنیتی و ژئوپلیتیکی این وضعیت، باید این نکته را نیز در نظر گرفت که در حوزه‌ای که فناوری سریع‌تر از ظرفیت توسعه هنجارها، سیاست‌ها و مقررات تکامل می‌یابد، کشورهایی که پیشتاز تحولات تکنولوژیکی کنونی هستند نیز در این حوزه قرار خواهند گرفت. یک موقعیت مزیت برای تعیین استانداردها در مورد استفاده و تأثیر این فناوری ها. در نتیجه، اتحادیه اروپا ممکن است در آینده با سناریوهای کاهش کنترل و خودمختاری در این زمینه مواجه شود (Broeders et al., 2023)

مشابه ابتکارات اتخاذ شده برای محافظت از بازار دیجیتال و شهروندان اتحادیه اروپا، با نگاهی به اجرای مرتبط هوش مصنوعی در بخش نظامی، اتحادیه اروپا موضع مشترکی را در مورد کنترل انسانی بر سیستم های مجهز به هوش مصنوعی در بحث سازمان ملل در مورد قوانین ارائه کرده است (Bellanova, 2022). به دنبال افزایش نگرانی جهانی در رابطه با پذیرش هوش مصنوعی در صنایع دفاعی و در نتیجه استفاده از چنین تسلیحاتی، سازمان ملل در سال ۲۰۱۷ گروهی از کارشناسان دولتی (UNGGE) را در زمینه فناوری های نوظهور در حوزه قوانین ایجاد کرد. با هدف شناسایی اصول و هنجارهای رسمی شده در چارچوب سازمان ملل متحد، همچنین به دلیل نقش فعال کشورهای عضو اتحادیه اروپا، UNGGE اصول بشردوستانه را در استفاده از قوانین شناسایی کرده است (Sinha, 2021). در راستای این قطعنامه، در اوایل سال ۲۰۲۱، پارلمان اروپا متنی را در مورد دستورالعمل‌های غیرالزام‌آور برای استفاده نظامی و غیرنظامی از هوش مصنوعی به تصویب رساند و هوش مصنوعی را مانند استفاده از سلاح‌های متعارف در درگیری‌ها تابع قوانین عمومی بین‌المللی قرار داد. این قطعنامه جدید استفاده مشروع از هوش مصنوعی در بخش نظامی را مشخص می کند (Agarwal, 2018). قابل ذکر است که کاربرد هوش مصنوعی از طریق پردازش انبوه نظارت بر سلامت و پیش بینی خطرات زیست محیطی و همچنین امکان ماندن پرسنل نظامی در عملیات در محیط های پرخطر، برای پاکسازی مین و دفاع در برابر ازدحام پهپادها را تشخیص می دهد. این قطعنامه به دنبال اجماع اولیه ای است که پارلمان اروپا در سال ۲۰۱۸ به دست آورد و خواستار ممنوعیت قوانین شد (European Parliament, 2020) شد. اگرچه این نتیجه الزام آور نبود، اما دیدگاه اتحادیه اروپا را در مورد پذیرش هوش مصنوعی در قلمرو نظامی ارائه کرد. با این وجود، این ممنوعیت با راه‌اندازی EDF در سال ۲۰۱۹ عملی شد. به همین مناسبت، بودجه EDF به شرط عدم تخصیص بودجه برای تحقیق و توسعه در قوانین مربوط به سال ۲۰۱۸ قطعنامه ممنوعیت پذیرش آنها به تصویب نمایندگان مجلس رسید (Bellanova, 2022).

دیدگاه اتحادیه اروپا در مورد مقررات و حمایت از حقوق فردی به عنوان مانع از توسعه هوش مصنوعی در نظر گرفته شده است زیرا نوآوری و جمع آوری داده ها را سخت می کند (Wagner, 2021).

در راستای دیدگاه‌های ارائه شده توسط NPE و Brussels Effects، که به ما کمک می‌کند تا اتحادیه اروپا را در تلاش برای غلبه بر فقدان رهبری خود در صنعت هوش مصنوعی و بخش امنیتی مرتبط با آن، با ترویج ایده‌ها، هنجارها و مقررات تفسیر کنیم. به طور فزاینده ای بر اهمیت همکاری با سایر بازیگران همفکر در پاسخ به جنبه های نظامی و امنیتی هوش مصنوعی تأکید می کند(European Commission, 2020). این امر به ویژه در حوزه امنیت سایبری مشهود است، جایی که اتحادیه اروپا در حال افزایش جاه طلبی خود برای ایفای نقش محوری در همکاری های بین المللی است. در نتیجه، اتحادیه اروپا با گسترش رویکرد دیپلماتیک سایبری خود فراتر از حوزه امنیت، ایجاد مشارکت ها را تشدید می کند (Chiappetta, 2023). یکی از آنها همکاری تقویت شده با برزیل در زمینه اقتصاد دیجیتال از طریق گفتگوی اقتصاد دیجیتال است که باید در مورد هوش مصنوعی نیز بحث کند. مشارکت مشابهی نیز با سنگاپور تقویت شده است که چارچوبی برای همکاری های آتی در مناطق نوظهور با پتانسیل اقتصادی متحول کننده، از جمله هوش مصنوعی فراهم می کند. در نهایت، اولین مشارکت دیجیتال رسمی که اتحادیه اروپا با یک کشور شریک امضا کرده است، در اجلاس سران اتحادیه اروپا–ژاپن در ماه مه ۲۰۲۲ با ژاپن بود. در زمینه هوش مصنوعی، همکاری بین دو بازیگر باید بر کاربردهای ایمن و اخلاقی این فناوری متمرکز شود.

در حوزه دیجیتال، اتحادیه اروپا گزینه‌های کمی دارد. برخلاف توسعه هوش مصنوعی مبتنی بر بازار آزاد ایالات متحده و عجله چینی ها برای به دست آوردن تسلط نظامی در بخش هوش مصنوعی، بدون ابزاری برای بازی در این حوزه، اتحادیه اروپا مجبور است رویکردی اخلاقی برای هوش مصنوعی اتخاذ کند. با انجام این کار، نقش خود را در بحث جهانی در مورد تحولات دیجیتال پایدار مشخص می کند و از خود در برابر غول های دیجیتال خارجی محافظت می کند. با این حال، اینکه آیا با جاه طلبی برای به دست آوردن حاکمیت دیجیتال سازگار است یا خیر، کمتر مشهود است.

بحث

هوش مصنوعی در دنیای معاصر به یکی از مهم‌ترین فناوری‌های تحول‌آفرین تبدیل شده است که تأثیرات گسترده‌ای بر ابعاد مختلف جامعه، اقتصاد و امنیت دارد. اتحادیه اروپا، به‌ویژه در زمینه تقویت امنیت سایبری و حاکمیت دیجیتال، در حال انجام تلاش‌های گسترده‌ای برای بهره‌برداری از این فناوری است. با این حال، استفاده از هوش مصنوعی در این زمینه با چالش‌های متعددی مواجه است که نیازمند دقت و بررسی دقیق هستند. این چالش‌ها و فرصت‌ها به‌ویژه در قالب قانون هوش مصنوعی اتحادیه اروپا که در سال ۲۰۲۴ تصویب شد، نمود پیدا کرده است و هدف آن تنظیم استفاده از این فناوری در جهت حفظ حقوق بشر، امنیت و حاکمیت دیجیتال اروپا است. این بخش از تحلیل با نتایج مطالعات Verma (۲۰۱۹) همخوانی دارد که به چالش‌های سوگیری الگوریتمی و مشکلات اخلاقی ناشی از استفاده از هوش مصنوعی اشاره کرده‌اند.

چالش‌های اصلی و فرصت‌ها در استفاده از هوش مصنوعی در اتحادیه اروپا

یکی از چالش‌های عمده‌ای که اتحادیه اروپا با آن مواجه است، سوگیری الگوریتمی است. در تحقیقات پیشین به این نکته اشاره شده است که سوگیری‌های موجود در الگوریتم‌های هوش مصنوعی می‌تواند منجر به تبعیض و نقض حقوق بشر شود (Azin et al., 2024). این مسأله به‌ویژه در اتحادیه اروپا که در تلاش برای ایجاد یک سیستم نظارتی شفاف و منصفانه است، تبدیل به چالشی پیچیده شده است. قانون هوش مصنوعی اتحادیه اروپا، با تنظیم استفاده از الگوریتم‌ها و ارائه دستورالعمل‌های مشخص برای کاربردهای با ریسک بالا، قصد دارد تا این چالش‌ها را کاهش دهد و همزمان از رشد و نوآوری در این حوزه حمایت کند. این تحلیل با نتایج تحقیقات Brynjolfsson & McAfee (۲۰۱۷) که بر ضرورت نظارت و تنظیم استفاده از الگوریتم‌ها در جهت جلوگیری از سوگیری و تبعیض تأکید دارند، هم‌راستا است.

مقررات و استانداردهای موجود در اتحادیه اروپا

تحقیقات مختلف (Rodrigues, 2020; European Commission, 2020) نشان می‌دهند که اتحادیه اروپا با چالش‌های نظارتی متعددی در زمینه هوش مصنوعی روبه‌رو است. در حالی که اتحادیه اروپا پیشگام در زمینه مقررات حفاظت از داده‌ها و ایجاد استانداردهای حقوق بشری در فناوری‌های نوظهور است، هنوز در زمینه ایجاد زیرساخت‌های لازم برای پیاده‌سازی این استانداردها در بخش‌های خصوصی و دولتی با مشکلاتی مواجه است. به‌ویژه، در بخش‌هایی مانند حریم خصوصی و امنیت سایبری، نگرانی‌های زیادی درباره امکان دستکاری داده‌ها و نقض امنیت افراد و دولت‌ها وجود دارد. این در حالی است که در مقایسه با چین و ایالات متحده، که مقررات سختگیرانه‌ای ندارند، اتحادیه اروپا با مقررات پیچیده‌تری روبه‌روست که ممکن است سرعت نوآوری در این زمینه را کاهش دهد (Birkstedt et al., 2023). این یافته‌ها مشابه با

نتایج تحقیقات Birkstedt et al. (۲۰۲۳) است که تأکید دارند قوانین و مقررات سنگین ممکن است مانع نوآوری در اتحادیه اروپا شوند.

رقابت جهانی و موقعیت اتحادیه اروپا

در سطح جهانی، رقابت‌های شدیدی میان قدرت‌های بزرگ در زمینه هوش مصنوعی به‌ویژه در حوزه‌های نظامی و اقتصادی وجود دارد. ایالات متحده و چین به‌عنوان دو بازیگر اصلی در این رقابت‌ها با سرمایه‌گذاری‌های عظیم در فناوری‌های هوش مصنوعی، در حال پیشی گرفتن از اتحادیه اروپا هستند. این موضوع به‌ویژه پس از بحران اوکراین که رقابت‌های ژئوپلیتیکی به اوج خود رسید، شدت بیشتری یافته است. اتحادیه اروپا، در حالی که دارای ظرفیت‌های تحقیقاتی و نوآورانه قدرتمندی است، هنوز در جذب سرمایه‌گذاری‌های کلان و پیشرو بودن در صنعت هوش مصنوعی نسبت به رقبای خود عقب‌تر است (Mokry & Gurol, 2024). بنابراین، برای اینکه اتحادیه اروپا بتواند به‌عنوان یک قدرت پیشرو در حوزه هوش مصنوعی مطرح شود، نیازمند سرمایه‌گذاری بیشتر در زیرساخت‌های دیجیتال، پشتیبانی از استارت‌آپ‌ها و شرکت‌های کوچک و متوسط (SMEs) و همچنین ارتقای همکاری‌های بین‌المللی با دیگر قدرت‌های جهانی است (European Commission, 2024). این تحلیل با نتایج تحقیقات Mokry & Gurol (۲۰۲۴) که بر ضرورت سرمایه‌گذاری کلان در زمینه هوش مصنوعی و توسعه زیرساخت‌های دیجیتال تأکید دارند، هم‌راستا است.

در کنار چالش‌ها، هوش مصنوعی برای اتحادیه اروپا فرصت‌های زیادی نیز به ارمغان می‌آورد. توسعه زیرساخت‌های دیجیتال و پیشرفت‌های نوآورانه در زمینه هوش مصنوعی می‌تواند به بهبود امنیت سایبری و مدیریت بحران‌ها کمک کند. به‌ویژه، هوش مصنوعی می‌تواند در مقابله با تهدیدات سایبری به ابزارهای مؤثری تبدیل شود و در این زمینه اتحادیه اروپا می‌تواند با همکاری‌های بین‌المللی نظیر مشارکت‌های خود با برزیل و سنگاپور، موقعیت خود را تقویت کند (Chiappetta, 2023). این همکاری‌ها می‌تواند به توسعه استانداردهای جهانی برای استفاده از هوش مصنوعی در بخش‌های نظامی، اقتصادی و امنیتی کمک کند و به اتحادیه اروپا این امکان را دهد که در مذاکرات بین‌المللی در مورد حاکمیت دیجیتال و مقررات جهانی هوش مصنوعی نقش مؤثری ایفا کند. این تحلیل با نتایج تحقیق Chiappetta (۲۰۲۳) که به اهمیت همکاری‌های بین‌المللی در زمینه هوش مصنوعی برای تقویت امنیت سایبری و مدیریت تهدیدات اشاره کرده است، هم‌راستا می‌باشد.

نتیجه‌گیری

هوش مصنوعی به‌عنوان یکی از تحولات بزرگ فناوری در دنیای معاصر، تأثیرات فراوانی بر تمامی ابعاد زندگی بشر گذاشته است. در حالی که بسیاری از کشورها و بازیگران جهانی در تلاشند تا از این فناوری به‌عنوان ابزاری برای پیشبرد اهداف امنیتی، اقتصادی و اجتماعی خود بهره‌برداری کنند، اتحادیه اروپا نیز به‌عنوان یکی از قدرت‌های مهم جهانی، چالش‌ها و فرصت‌های بسیاری را در این مسیر پیش رو دارد. این تحقیق با هدف تحلیل چالش‌ها و فرصت‌های استفاده از هوش مصنوعی در تقویت امنیت سایبری و حاکمیت دیجیتال اتحادیه اروپا انجام شد. نتایج این مطالعه نشان داد که در حالی که اتحادیه اروپا توانسته است با تصویب قوانین نوآورانه همچون قانون هوش مصنوعی در سال ۲۰۲۴، قدم‌هایی بزرگ در جهت تقویت نظارت و حفظ حاکمیت دیجیتال بردارد، اما همچنان با چالش‌های مهمی در زمینه نظارت بر استفاده از هوش مصنوعی، هماهنگی بین‌المللی و حفظ حقوق بشر مواجه است.

یکی از مهم‌ترین چالش‌های اتحادیه اروپا، سوگیری الگوریتمی و مشکلات اخلاقی است که ممکن است منجر به نقض حقوق افراد و کاهش اعتماد عمومی به این فناوری‌ها شود. از سوی دیگر، اتحادیه اروپا با نگرانی‌هایی جدی درباره عدم وجود یک صنعت پیشرو در هوش مصنوعی مواجه است که این مسأله توانایی آن را برای رقابت با کشورهای پیشرفته‌ای چون ایالات متحده و چین محدود می‌کند. در حالی که اتحادیه اروپا در زمینه تحقیق و نوآوری در هوش مصنوعی ظرفیت‌های بسیاری دارد، نبود سرمایه‌گذاری‌های کلان در این صنعت و همچنین پیچیدگی‌های مقرراتی باعث شده است که این منطقه نتواند به‌طور کامل از فرصت‌های این فناوری بهره‌برداری کند. با این حال، فرصت‌هایی همچون توسعه همکاری‌های بین‌المللی با کشورهای دیگر، به‌ویژه در زمینه‌های امنیت سایبری و مدیریت بحران‌ها، می‌تواند جایگاه اتحادیه اروپا را در زمینه هوش مصنوعی تقویت کند. در این راستا، اتحادیه اروپا باید به تقویت زیرساخت‌های دیجیتال و ایجاد محیط‌های مناسب برای پذیرش هوش مصنوعی توسط بخش‌های خصوصی و دولتی بپردازد. همچنین، برای رقابت با رقبای جهانی خود، نیاز به افزایش سرمایه‌گذاری در صنعت هوش مصنوعی و حمایت از استارت‌آپ‌ها و شرکت‌های کوچک و متوسط (SMEs) دارد. این رویکرد می‌تواند به اتحادیه اروپا کمک کند تا به‌عنوان یک بازیگر پیشرو در عرصه جهانی هوش مصنوعی شناخته شود.

با توجه به نتایج این تحقیق، پیشنهاد می‌شود که پژوهش‌های آینده بر تحلیل تأثیرات دقیق‌تر هوش مصنوعی بر سیاست‌های امنیتی اتحادیه اروپا تمرکز داشته باشند و به ویژه به بررسی چگونگی ارتقای همکاری‌های بین‌المللی در این زمینه پرداخته شود. همچنین، نیاز به مطالعات بیشتر در خصوص اثرات بلندمدت استفاده از هوش مصنوعی در مقابله با تهدیدات سایبری و نحوه تنظیم مقررات مناسب برای حفظ حقوق بشر و امنیت دیجیتال احساس می‌شود. به‌ویژه پژوهش‌هایی که به مقایسه رویکردهای مختلف کشورها در تنظیم مقررات هوش مصنوعی پرداخته و نتایج آن‌ها را با رویکرد اتحادیه اروپا مقایسه کنند، می‌تواند به ارائه راهکارهای مؤثرتر برای مدیریت چالش‌های جهانی هوش مصنوعی کمک کند. همچنین، تحقیقات آینده می‌توانند به بررسی اثرات استفاده از هوش مصنوعی در بخش‌های دفاعی و نظامی اتحادیه اروپا پرداخته و چگونگی ایجاد یک چارچوب قانونی و اخلاقی برای استفاده از این فناوری در عرصه‌های جنگی و امنیتی را بررسی نمایند. این پژوهش‌ها می‌توانند به تحلیل و توسعه سیاست‌های مشترک در سطح جهانی برای استفاده امن و اخلاقی از هوش مصنوعی کمک کنند.

References

Agarwal, S. (2018). Normative Challenges in the Cyber Domain-Limits of the UNGGE-OEWG Process. *-19 ISIL YB Int'l Human. & Refugee L.*, *18*, 270.

Agatonovic-Kustrin, S., & Beresford, R. (2000). Basic concepts of artificial neural network (ANN) modeling and its application in pharmaceutical research. *Journal of pharmaceutical and biomedical analysis*, *22*(5), 717-727.

Al Ridhawi, I., Otoum, S., Aloqaily, M., & Boukerche, A. (2020). Generalizing AI: Challenges and opportunities for plug and play AI solutions. *IEEE Network*, *35*(1), 372-379.

Azin, S., Hedayati Shahidani, M., & Jansiz, A. (2024). Artificial intelligence and strategic stability; A cognitive lesson on the development of military dimensions of artificial intelligence in the United States and Russia. American Strategic Studies, 4(15), 95-120. [In Persian]

Babu, M. V. S., & Banana, K. R. I. S. H. N. A. (2024). A study on narrow artificial intelligence—An overview. *Int. J. Eng. Sci. Adv. Technol*, *24*, 210-219.

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: an introduction. *European security*, *31*(3), 337-355.

Birkstedt, T., Minkkinen, M., Tandon, A., & Mäntymäki, M. (2023). AI governance: themes, knowledge gaps and future agendas. *Internet Research*, *33*(7), 133-167.

Boulanin, V., Goussac, N., Brunn, L., & Richards, L. (2020). Responsible Military Use of Artificial Intelligence: Can the European Union Lead the Way in Developing Best Practice?.

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. JCMS: Journal of Common Market Studies, 61(5), 1261-1280.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, *31*(3), 415-434.

Chiappetta, A. (2023). Navigating the AI frontier: European parliamentary insights on bias and regulation, preceding the AI Act. Internet Policy Review, 12(4), 1-26.

Economist. (2024). The EU is worried about sensitive exports to competitors and foes. Retrieved from: https://www.economist.com/europe/2025/01/30/the-eu-is-worried-about-sensitive-exports-to-competitors-and-foes

European Commission (2020). White Paper on Artificial Intelligence: Public consultation towards a European approach for excellence and trusts. http://ec.europa.eu/digital-single-market/en/news/white-paper-artificialintelligence-public-consultation-towards-european-approach-excellence. [Online; accessed May 24, 2021].

European Commission (2021). Proposal for a Regulation of the European Parliament and the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. http://digital-strategy.ec.europa.eu/en/library/proposal-regulation-layingdown-harmonised-rules-artificial-intelligence-artificial-intelligence. [Online; accessed May 17, 2021].

European Commission. (2024). *AI Act: The European Approach to AI Regulation.*

European Parliament. (2020). Setting up a special committee on artificial intelligence in a digital age, and defining its responsibilities, numerical strength and term of office [Decision]. https://www.europar l.europa.eu/doceo/document/TA-9-2020-0162_EN.html

European Union. (2018). A EUROPEAN APPROACH TO ARTIFICIAL INTELLIGENCE. Retrieved from:https://www.eitdigital.eu/fileadmin/2022/ecosystem/makers-shapers/reports/EIT-Digital-Artificial-Intelligence-Report.pdf

Fahad, M., Basri, T., Hamza, M. A., Faisal, S., Akbar, A., Haider, U., & Hajjami, S. E. (2024). The benefits and risks of artificial general intelligence (agi). In *Artificial General Intelligence (AGI) Security: Smart Applications and Sustainable Technologies* (pp. 27-52). Singapore: Springer Nature Singapore.

Ferguson, N. (2021). *Doom: The politics of catastrophe*. Penguin UK.

Justo-Hanani, R. (2022). The politics of Artificial Intelligence regulation and governance reform in the European Union. *Policy Sciences*, *55*(1), 137-159.

Kühl, N., Schemmer, M., Goutier, M., & Satzger, G. (2022). Artificial intelligence and machine learning. *Electronic Markets*, *32*(4), 2235-2244.

Mohammadi, S., Barzegar, K., Malek, E., & Makramipour, M. B. (2024). Artificial intelligence and transformation in the political-social domain (Case study: 2024 U.S. elections). American Strategic Studies, 3(12), 143-164. [In Persian]

Mokry, S., & Gurol, J. (2024). Competing ambitions regarding the global governance of artificial intelligence: China, the US, and the EU. *Global Policy*, *15*(5), 955-968.

Moroney, L. (2020). *AI and Machine Learning for coders*. O'Reilly Media.

Müller, V. C. (2020). Ethics of artificial intelligence and robotics.

Oseni, A., Moustafa, N., Janicke, H., Liu, P., Tari, Z., & Vasilakos, A. (2021). Security and privacy for artificial intelligence: Opportunities and challenges. *arXiv preprint arXiv:2102.04661*.

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, *4*, 100005.

Sinha, S. (2021). Technology: A Path Towards A More Collaborative World Order?. *Fletcher F. World Aff.*, *45*, 5.

Torki, H. (2024). A new approach to AI-based power (Case study: The U.S.-China competition from 2010 to 2023). American Strategic Studies, 4(14), 91-114. [In Persian]

Van Noordt, C., & Misuraca, G. (2022). Artificial intelligence for the public sector: results of landscaping the use of AI in government across the European Union. *Government information quarterly*, *39*(3), 101714.

Verma, S. (2019). Weapons of math destruction: how big data increases inequality and threatens democracy. *Vikalpa*, *44*(2), 97-98.

Wagner, G. (2021). Liability for artificial intelligence: A proposal of the European Parliament. *Available at SSRN 3886294*.