News Science
Online ISSN: 2980-9274 Print ISSN: 2382-9788
Homepage: www.mjourcom.ir

International Legal Implications of AI-Driven Global Privacy Breaches by the U.S. Intelligence Community: A Comparative Analysis of Iran and Russia

Hasan Biarjomandi[1]✉ | **Mahmoud Alamolhoda**[2]

1. Corresponding Author: Department of Law, Faculty of Humanities and Social Sciences, Golestan University, Gorgan, Iran. E-mail: h.biarjomandi@gu.ac.ir
2 Assistant Professor, Department of Media Management, Comprehensive University of the Islamic Revolution, Tehran, Iran. E-mail: m.alamolhoda@cuir.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 16 October 2025
Received in revised form: 18 December 2025
Accepted: 21 April 2026
Published online: 30 May 2026

Keywords:
U.S. Intelligence Community,
Global Violation of Privacy,
Artificial Intelligence,
Iran,
Russia.

ABSTRACT

Objective: The purpose of this research is to examine the role of the United States intelligence community in the recent data-driven war against the Islamic Republic of Iran, drawing a comparison with similar targeted operations against Russian commanders in Ukraine. Specifically, the study investigates the global consequences of violating individuals' right to privacy from the perspective of international law.

Methods: This research employed a descriptive-analytical method, focusing on the right to privacy of individuals to examine the actions of the American intelligence community, particularly those leveraging artificial intelligence, in the global violation of this right. Primary sources related to CENTCOM's cooperation with the Israeli regime were reviewed, drawing upon credible scientific reports from think tanks and research centers, as well as official statements and declarations.

Results: The findings of this research indicate that over the past two decades, the United States has developed data-driven warfare by leveraging artificial intelligence technologies, leading to violations of individuals' privacy in multiple jurisdictions, including Russia and Iran.

Conclusions: The findings of this study suggest that, according to explicit statements made by the US President on November 6, 2025, CENTCOM, under the command of General Erik Kurilla, played a role in the direction and control of the conflict that began on June 13, 2025. This involvement extended to specific operations, including the targeting of several prominent university professors, senior military commanders, and their families in residential and civilian areas. Such actions constitute a flagrant violation of the right to privacy, given the long-term collection and continuous processing of these individuals' personal data.

Cite this article: Biarjomandi, H.& Alamolhoda, M. (2026). International Legal Implications of AI-Driven Global Privacy Breaches by the U.S. Intelligence Community: A Comparative Analysis of Iran and Russia, ***News Science***, 14 (1), 45-50.
DOI : http//doi.org/10.22034/lrsi.2026.553763.1458

DOI : http//doi.org/10.22034/lrsi.2026.553763.1458

The Journal of *News Science*
Vol. 15, No. 1, Ser.57, Spring 2026, P. 45- 50
Journal homepage: https://www.mjourcom.ir/
DOI: http//doi.org/10.22034/lrsi.2026.553763.1458

Open Access

ORIGINAL ARTICLE

International Legal Implications of AI-Driven Global Privacy Breaches by the U.S. Intelligence Community: A Comparative Analysis of Iran and Russia

Hasan Biarjomandi[1] | Mahmoud Alamolhoda[2]

[1] Corresponding Author: Department of Law, Faculty of Humanities and Social Sciences, Golestan University, Gorgan, Iran. E-mail: h.biarjomandi@gu.ac.ir
[2] Assistant Professor, Department of Media Management, Comprehensive University of the Islamic Revolution, Tehran, Iran. E-mail: m.alamolhoda@cuir.ac.ir

Received: October 16, 2025 Accepted: April 21, 2026

EXTENDED ABSTRACT

Introduction:

On June 13, 2025, the Zionist regime, in flagrant violation of Article 1(1) and Article 2(4) of the Charter of the United Nations, carried out the assassination of several prominent university professors, scientists, senior military commanders, and their families in residential and civilian areas during the initial wave of an armed aggression. This aggression persisted for twelve days, and owing to the Security Council's inaction, the assassinations continued unabated. Contrary to the official statement issued by U.S. Secretary of State Marco Rubio at the onset of this military aggression, President Donald Trump, on November 6, 2025, publicly claimed responsibility for both the armed aggression and the aforementioned assassinations - a claim that implies U.S. "direction and control" over these data-driven killings. This form of algorithmic warfare, enabled by artificial intelligence technologies, has a documented precedent in operations against senior Russian officials and commanders in Kharkiv, as well as against leaders and

commanders of the resistance front. Accordingly, this research aims to examine the role of the U.S. intelligence community in the direction and control of algorithmic warfare, and to assess the global consequences of violations of the right to privacy.

Method:

This study, with a focus on the right to privacy under international law, employs a descriptive-analytical and comparative method to examine the U.S. intelligence community's AI-based actions in the systematic global infringement of this right. Primary sources and documents concerning privacy violations in data-driven assassinations—specifically in Russia and Iran - were considered in light of the requirements of the comparative method. The analysis draws on credible scientific reports, publications from think tanks and research centers, and official statements and declarations regarding the strategic ties between the Zionist regime and CENTCOM from 2020 to 2025. Furthermore, to substantiate the U.S. intelligence community's role in directing and controlling these data-driven wars, the study reviews over four decades of this community's engagement in the development and application of AI technologies and data-driven warfare, based on the work of internationally recognized scholars and official pronouncements by relevant authorities. The issue of data-driven warfare is thus analyzed with due attention to its origins, credibility, legal implications, and the preservation of informational integrity, thereby ensuring that the principal findings and conclusions possess the requisite validity.

Findings:

The findings indicate that, over the past two decades, the United States has developed a new model of data-driven hybrid warfare through the strategic deployment of artificial intelligence technologies. Within this framework - characterized by effective "direction and control" in conflicts involving Ukraine (NATO) and Russia, as well as Israel and Iran - the United States has undertaken extensive and sustained actions aimed at violating the privacy of individuals in Russia, Iran, and their regional allies. This model is currently expanding within the Indo-Pacific Command, driven by the U.S. - China trade war over 5G and AI technologies, and is similarly manifesting within the Latin American and Caribbean Command. Consequently, we are witnessing an invisible, data-driven global war that various nations are developing under transnational alliances.

From a human rights perspective, the most serious threat posed by such data-driven warfare is the large-scale violation of individuals' right to privacy. Moreover, under the Charter of the United Nations, these activities constitute a threat to international peace and security. Given the existing legal and structural lacunae, coupled with the ineffectiveness of the United Nations - contrary to Article 1(4) of the Charter - the Organization's central role in coordinating collective action for common objectives is being progressively eroded. This trend risks undermining the vision articulated in the Preamble to the UN Charter in the contemporary era.

Conclusion:

The results of this study demonstrate that the development and application of artificial intelligence technologies within the American information society spans nearly half a century. Specifically, in the context of the Special Forces' data-driven overseas operations, the use of such technologies has persisted for almost two decades. Numerous documented cases of AI-based, data-driven operations in the West Asia region - particularly those corresponding to the first part of the second hypothesis - indicate that the joint operation conducted by the United States and Ukraine on May 1, 2022, against the Chief of Staff of the Russian Army and several senior Russian officers in Izyum, Kharkiv, constitutes a concrete example of these unlawful activities. In accordance with the second part of the second hypothesis, and in light of explicit statements made by the U.S. President on November 6, 2025, CENTCOM, under the command of General Erik Kurilla, played a decisive role in directing and controlling the imposed war of June 13, 2025, and

in the assassination of several prominent university professors, senior military commanders, and their families in residential and civilian areas. Given the long-standing collection and continuous processing of these individuals' personal data, such actions amount to a grave violation of the right to privacy. Finally, consistent with the third hypothesis, the findings reveal that the United States has engaged—persistently and with full knowledge—in the violation of the privacy rights of citizens of UN member states, through the systematic collection and processing of big data pertaining to military command structures, including CENTCOM.

Data Availability Statement
Data available on request from the authors.
Acknowledgements
The authors would like to thank anonymous reviewers.
Ethical considerations
Not applicable.
Funding
Not applicable.
Conflict of interest
The authors declare no conflict of interest.

References:

Abouzari, M. (2023). Law and artificial intelligence. Mizan Publishing. (in Persian)

Aidun, E. (2025). Data privacy in the digital age: A comparative analysis of U.S. and EU regulations. *University of Cincinnati Law Review*, 93. https://uclawreview.org/2025/03/05/data-privacy-in-the-digital-age-a-comparative-analysis-of-u-s-and-eu-regulations/

Al Jazeera. (2025, November 6). Trump says he was "very much in charge" of Israel's June 13 attack on Iran. https://www.aljazeera.com/news/2025/11/6/trump-says-he-was-very-much-in-charge-of-israels-june-13-attack-on-iran

American Privacy Rights Act of 2024, (2024) (APRA). https://www.govinfo.gov/app/details/BILLS-118hr8818ih

Angerhofer, M. D., Datta, S., Vishwakarma, A. K., Sharma, U. R., Singh, V., & Gautam, P. (2024). Privacy in the age of artificial intelligence: Addressing the ethical and legal implications. *Journal of Informatics Education and Research*, 4(3), 1399–1414. https://jier.org/index.php/journal/article/view/1465

Ansari, B. (2022). Mass communication law. Samt Publications. (in Persian)

Barnes, J. E., Cooper, H., & Schmitt, E. (2022, May 4). U.S. intelligence is helping Ukraine kill Russian generals, officials say. *The New York Times*. https://www.nytimes.com/2022/05/04/us/politics/russia-generals-killed-ukraine.html

Bharati, R. K. (2024). The right to privacy in the age of artificial intelligence: Challenges and legal frameworks. *Dastavej Research Journal*, 54(7), 27–38. https://dastavej.net/volume-54-issue-7/

Bondar, K. (2024). Understanding the military AI ecosystem of Ukraine. *Center for Strategic and International Studies (CSIS)*. https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine

Borchert, H., Schütz, T., & Verbovszky, J. (Eds.). (2025). *The very long game: 25 case studies on the global state of defense AI*. Springer Nature.

Chinmay. (2025). Privacy in the age of artificial intelligence. *NUJS Journal of Regulatory Studies*, 9(4), 71–88. https://journals.nujs.edu/index.php/njrs/article/view/338

Crawford, J. (2002). The ILC's articles on responsibility of states for internationally wrongful acts: A retrospect. *American Journal of International Law*, 96(4), 874–890. http://www.jstor.org/stable/3070683

Dadmehr, H. (2015). Reputations in international law and international relations. Majd Publications. (in Persian)

Dashti, T. S., & Motamednejad, R. (2024). The role of artificial intelligence in EU legislation. *News Science*, 11(3), 1–20. (in Persian)
Dekel, U., & Bar Or, Y. (2021). A breeze of change: Israel joins the US Central Command region. *Institute for National Security Studies (INSS)*, Tel Aviv University. https://www.inss.org.il/publication/centcom/
DLA Piper. (2024). Data protection laws of the world – United States edition. DLA Piper Global Data Protection Team. https://www.dlapiperdataprotection.com/?c=US
Ewbank, J. (2024). The role of artificial intelligence in the U.S. Intelligence Community: Current uses and future developments. Aspen Institute. https://www.aspeninstitute.org/wp-content/uploads/2024/10/Ewbank_Role-of-AI-in-USIC_Final.pdf
Faverio, M. (2023, October 18). Key findings about Americans and data privacy. Pew Research Center. https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/
Goncharuk, V. (2025). Survival of the smartest? Defense AI in Ukraine. In H. Borchert, T. Schütz, & J. Verbovszky (Eds.), The very long game: 25 case studies on the global state of defense AI (pp. 375–395). Springer Nature.
Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., & Scharre, P. (2018). Artificial intelligence and international security. Center for a New American Security (CNAS). https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS-AI-and-International-Security-July-2018_Final.pdf
Huberman, B., & Amaral, R. A. D. (2025). Hegemony and resistance: US imperial strategies in Latin America. *Journal of Latin American Political Economy*. https://www.tandfonline.com/doi/full/10.1080/19436149.2025.2578046
Ignatius, D. (2022, June 24). How the U.S. helped Ukraine inflict devastating losses on Russia. *The Washington Post*. https://www.washingtonpost.com/opinions/2022/06/24/us-intelligence-assistance-ukraine-russia-war
International Covenant on Civil and Political Rights. (1966). United Nations. https://iran.un.org/en/106018-international-covenant-civil-and-political-rights
Jewish Institute for National Security of America (JINSA). (2022, October 24). How a shift to CENTCOM enabled close U.S.-Israel coordination against Iran. https://jinsa.org/how-a-shift-to-centcom-enabled-close-us-israel-coordination-against-iran/
King, A. (2024). Digital targeting: Artificial intelligence, data, and military intelligence. *Journal of Global Security Studies*, 9(2), 1–16.
Kissinger, H. A., Schmidt, E., & Huttenlocher, D. (2023). The age of AI: And our human future (P. Hamooni, Trans.). Soroush Publishing. (in Persian)
Knights, M. (2021). Moving Israel to CENTCOM: Another step into the light. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/moving-israel-centcom-another-step-light
Lappin, Y. (2021). The US brings Israel into CENTCOM (BESA Center Perspectives Paper No. 1,940). Begin-Sadat Center for Strategic Studies. https://besacenter.org/us-israel-centcom/
Lee, J. (2022). Artificial intelligence and international law. Springer Nature.
Mahmodi Parchini, M., et al. (2025). Comparison of personal data protection laws: Unique general regulations under the European Union's General Data Protection Regulation (GDPR) and United States laws. *News Science*, 13(4), 31–35. (in Persian)
McClain, C., Faverio, M., Anderson, M., & Park, E. (2023, October 18). How Americans view data privacy. Pew Research Center. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/
Ministry of Foreign Affairs of the Islamic Republic of Iran. (2025). https://mfa.gov.ir/portal/newsview/777763
Mirmohamadi, M. (2007). Neoconservatives and the information security policies of the United States. *The Journal of Foreign Policy*, 21(1), 93–126. (in Persian)
Mirmohamadi, M. (2023). Approaches for managing the intelligence community. *Strategic Studies Quarterly (SSQ),* 100, 155–159. (in Persian)
Moran, C., Burton, J., & Christou, G. (2023). The US Intelligence Community, global security, and AI: From secret intelligence to smart spying. *Journal of Global Security Studies*, 8(2), 1–18.
Negrão, T., Gobbi, M. C., Silva, T. C., & Holouka, G. (2025). The trade war between China and the USA and the geopolitical impacts of the 5G. São Paulo State University. https://www.researchgate.net/publication/388757321_The_Trade_War_Between_China_And_The_USA_And_The_Geopolitical_Impacts_Of_The_5G
Nordic Conference on the Right to Privacy. (1967). Right to privacy seminar report and conclusions. International Commission of Jurists. https://www.icj.org/wp-content/uploads/2013/06/Right-to-privacy-seminar-report-conclusions-1967-eng.pdf

Qhorbani, M., & Javaheri, M. (2023). United States Intelligence Community: Structures and functions. *Journal of Criminal Intelligence Researches*, 18(2), 145–176. (in Persian)

Sfetcu, N. (2024). Artificial intelligence in intelligence agencies, defense and national security. MultiMedia Publishing. https://www.telework.ro/en/e-books/artificial-intelligence-in-intelligence-agencies-defense-and-national-security/

Shokrollahi, S., & Motamednejad, R. (2025). The global governance of artificial intelligence in the service of humanity's interests and the key role of the UN. *News Science*, 14(1), 11–15. (in Persian)

Stone, C. (2021). The integration of artificial intelligence in the Intelligence Community: Necessary steps to scale efforts and speed progress (pp. 1–71). American University Washington College of Law.

The Jakarta Post. (2025, June 26). Mossad chief thanks CIA for help in Iran war. https://www.thejakartapost.com/world/2025/06/26/mossad-chief-thanks-cia-for-help-in-iran-war.html

United Nations. (1945). Charter of the United Nations. https://www.un.org/en/about-us/un-charter/chapter-1

United Nations General Assembly. (2001, December 12). Responsibility of states for internationally wrongful acts (A/RES/56/83). https://undocs.org/en/A/RES/56/83

United Nations International Law Commission. (2001). Articles on responsibility of states for internationally wrongful acts. United Nations Office of Legal Affairs. https://legal.un.org/avl/ha/rsiwa/rsiwa.html

United Nations. (1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights

U.S. Central Command (CENTCOM). (2024). Official image of a regional military exercise. https://www.centcom.mil/MEDIA/IMAGERY/igphoto/2003145032/

U.S. Department of State. (2025, June 12). Statement from Secretary of State Marco Rubio. https://www.whitehouse.gov/briefings-statements/2025/06/statement-from-secretary-of-state-marco-rubio/

Wooldridge, M. (2021). Artificial intelligence (A. Haghighi Qazvini, Trans.). Tamaddon Elmi. (in Persian)

Ziai Bigdeli, M. R. (2024). Public international law. Ganjedanesh Publications. (in Persian).

علوم خبری
شاپا چاپی: ۲۳۸۳-۹۷۸۸ شاپا الکترونیکی: ۹۲۷۴-۲۹۸۰

حقوق بین الملل و پیامدهای نقض جهانی حریم خصوصی با هوش مصنوعی توسط جامعه اطلاعاتی آمریکا (مطالعه مقایسه ای: ایران و روسیه)

حسن بیارجمندی[۱]✉ | محمود علم الهدی[۲]

۱. استادیار گروه حقوق، دانشکده علوم‌انسانی و اجتماعی، دانشگاه گلستان، گرگان، ایران. (نویسنده مسئول)، رایانامه: h.biarjomandi@gu.ac

۲ استادیار گروه مدیریت رسانه دانشگاه جامع انقلاب اسلامی، تهران، ایران. رایانامه: m.alamolhoda@cuir.ac.ir

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۴۰۴/۷/۲۴
تاریخ بازنگری: ۱۴۰۴/۹/۲۷
تاریخ پذیرش: ۱۴۰۵/۲/۱
تاریخ انتشار: ۱۴۰۵/۳/۹

کلیدواژه‌ها:
جامعه اطلاعاتی آمریکا،
هوش مصنوعی،
حریم خصوصی،
ایران،
روسیه.

چکیده

هدف: هدف این پژوهش بررسی نقش جامعه اطلاعاتی ایالات متحده آمریکا در جنگ داده محور اخیر علیه جمهوری اسلامی ایران با مقایسه ترورهای مشابه فرماندهان روسیه در اوکراین است و بطور خاص پیامدهای جهانی نقض حق حریم خصوصی افراد از منظر حقوق بین الملل مورد بررسی قرار می گیرد.

روش: در این پژوهش با تمرکز بر حق حریم خصوصی افراد ، اقدامات جامعه اطلاعاتی آمریکا مبتنی بر هوش مصنوعی در نقض جهانی این حق با روش توصیفی–تحلیلی بررسی شده است. منابع اصلی مربوط به همکاری ستتکام با رژیم صهیونیستی با در نظر گرفتن گزارش‌های علمی معتبر اندیشکده ها و مراکز تحقیقاتی، بیانیه‌ها و اعلامیه های رسمی مورد بررسی قرار گرفته‌اند.

یافته ها: یافته‌های این پژوهش نشان می‌دهد که در طول دو دهه گذشته، ایالات متحده با بهره‌گیری از فناوری‌های هوش مصنوعی، جنگ های داده محور را توسعه داده است که نقض حریم خصوصی افراد از جمله در روسیه و ایران را بدنبال داشته است.

نتیجه گیری: نتایج این پژوهش نشان می‌دهد که با توجه به اظهارات صریح رئیس جمهور ایالات متحده آمریکا در ۶ نوامبر ۲۰۲۵، ستتکام تحت فرماندهی ژنرال اریک کوریلا، در هدایت و کنترل جنگ تحمیلی ۱۳ ژوئن ۲۰۲۵ و بطور خاص ترور چندین استاد برجسته دانشگاه، فرماندهان ارشد نظامی و خانواده‌های آنها در مناطق مسکونی و غیرنظامی نقش آفرینی کرده است که با توجه به جمع‌آوری طولانی‌مدت و پردازش مستمر داده‌های شخصی این افراد، نقض فاحش حق حریم خصوصی محسوب می‌شود.

استناد: بیارجمندی، حسن و علم الهدی، محمود. (۱۴۰۵). حقوق بین الملل و پیامدهای نقض جهانی حریم خصوصی با هوش مصنوعی توسط جامعه اطلاعاتی آمریکا (مطالعه مقایسه ای: ایران و روسیه). *علوم خبری*، ۱۵ (۱)، ۲۵۳-۲۳۲.

DOI: http//doi.org/10.22034/lrsi.2026.553763.1458

مقدمه

رژیم صهیونیستی در ۱۳ ژوئن ۲۰۲۵ میلادی با نقض آشکار بند ۱ ماده ۱ و بند ۴ ماده ۲ منشور سازمان ملل متحد، در اولین موج تجاوز مسلحانه، اقدام به ترور تعدادی از اساتید برجسته دانشگاه، دانشمندان، فرماندهان ارشد نظامی و خانواده‌های آنان در اماکن مسکونی و غیرنظامی نمود. این تجاوز در طول ۱۲ روز ادامه یافت و با بی‌عملی شورای امنیت، ترورها ادامه داشت.

اما بر خلاف بیانیه رسمی مارکو روبیو، وزیر خارجه ایالات متحده، در آغاز این تجاوز نظامی اعلام کرد که اسرائیل به طور یک‌جانبه علیه ایران اقدام کرده است و ما در این حملات مشارکت نداریم و اولویت اصلی ما حفاظت از نیروهای آمریکایی است (بیانیه، ۱۲ ژوئن ۲۰۲۵) ؛ دیوید بارنیا رئیس موساد، در پیامی ویدئویی از سازمان اطلاعات مرکزی آمریکا (سیا) به عنوان شریک اصلی و به‌خاطر اقدام مشترک و موفقیت‌آمیز، قدردانی و تشکر کرد(جاکارتا پست، ۲۶ ژوئن ۲۰۲۵). همچنین دونالد ترامپ رئیس‌جمهور ایالات متحده، در ۶ نوامبر ۲۰۲۵ (۱۵ آبان ۱۴۰۴) مسئولیت این تجاوز مسلحانه و ترورهای یاد شده را بر عهده گرفت (الجزیره، ۲۰۲۵).

این اظهارات صریح که با واکنش وزارت خارجه ایران مواجه شد (وزارت امور خارجه جمهوری اسلامی ایران، ۱۴۰۴)، بر اساس بازتاب‌های عرفی تدوین مسئولیت دولت‌ها در قبال اعمال متخلفانه بین‌المللی در کمیسیون حقوق بین‌الملل (کمیسیون حقوق بین‌الملل، ۲۰۰۱) و گزارش آن (کرافورد، ۲۰۰۲) و شناسایی و تأیید ضمنی مفاد آن طی تصویب قطعنامه‌ای مجمع‌عمومی به شماره *A/RES/56/83* مورخ ۲۰۰۱ و قطعنامه‌های بعدی و استنادات دیوان بین‌المللی دادگستری (کمیسیون حقوق بین‌الملل، ۲۰۰۱)؛ دلالت بر «هدایت و کنترل»[1] ایالات متحده در این تجاوز نظامی و ترورهای داده‌محور دارد. همچنین، عملیات‌هایی با بهره‌گیری از فناوری‌های هوش مصنوعی علیه مقامات و فرماندهان ارشد روسیه در خارکیف و رهبران و فرماندهان جبهه مقاومت انجام شده است.

سرهنگ نیروی دریایی ایالات متحده، آندرو کوکور که نقش مهمی در پروژه ماون[2] داشت، اعلام کرد که ایالات متحده در یک «مسابقه تسلیحاتی هوش مصنوعی» قرار دارد (کینگ، ۲۰۲۴). فرانک کندال، وزیر نیروی هوایی ایالات متحده، در سپتامبر ۲۰۲۱ بخشی از این مسابقه تسلیحاتی را فاش کرد (موران، برتون و کریستو، ۲۰۲۳). همچنین، مدیر مرکز مشترک هوش مصنوعی در پنتاگون می‌گوید که شبکه‌های ما سلاح هستند و باید با آنها مانند سلاح رفتار کنیم. باید برای حفاظت و مقاوم‌سازی این شبکه‌ها برنامه‌ریزی کنیم، زیرا هر اقدامی که بر پایه هوش مصنوعی یا داده انجام می‌شود، به امنیت این شبکه‌ها بستگی دارد (موران، برتون و کریستو، ۲۰۲۳).

بنابراین، توسعه و کاربرد هوش مصنوعی در بستر ساختارهای جهانی ایالات متحده آمریکا، برخلاف فرصت‌هایی که به طور عمومی و فراگیر در اختیار مردم جهان قرار می‌دهد، به دلیل ماهیت اطلاعاتی و نظامی آن‌ها، تهدیدات جدی علیه حریم خصوصی افراد و حقوق بشر محسوب می‌شود. علاوه بر این، زمانی که جامعه اطلاعاتی ایالات متحده[3] برای نظارت جهانی (جاسوسی) اقدام به ذخیره‌سازی داده‌های کلان و پردازش آن‌ها می‌کند، این امر نقض حریم خصوصی اتباع دیگر کشورها را به دنبال دارد. بهره‌گیری تسلیحاتی از هوش مصنوعی در بستر ساختارهای جهانی، تحت حکمرانی اطلاعاتی و نظامی، منجر به نقض جهانی و فراگیر حریم خصوصی می‌شود که بعضی از اصول و مقاصد اساسی منشور سازمان ملل را نقض می‌کند.

هدایت و کنترل ایالات متحده در ترور دانشمندان و فرماندهان ایرانی و فرماندهان ارشد روسیه، نمونه‌های بارزی از این اقدامات است. براین‌اساس، باید به سؤالات مهمی پاسخ داد: جنگ‌های اطلاعاتی و نظامی داده‌محور در جامعه اطلاعاتی آمریکا چه پیشینه و ابعادی دارند؟ چگونه جامعه اطلاعاتی ایالات متحده اقدام به نقض حریم خصوصی اتباع دیگر کشورهای عضو سازمان ملل می‌کند؟ چه دلایل و مستنداتی در خصوص هدایت و کنترل جامعه اطلاعاتی آمریکا بر عملیات‌های ترور مقامات و فرماندهان ارشد روسیه و دانشمندان و فرماندهان ایرانی و خانواده‌های آنان در اماکن مسکونی و غیرنظامی وجود دارد؟ در این

---

[1] . Direction and control
[2] . Project Maven
[3] . The United States Intelligence Community IC

پژوهش، باتوجه‌به اهمیت موضوع و منابع علمی، ابتدا مروری بر پیشینه تخصصی آن انجام شد، سپس روش‌شناسی و فرضیه‌های اصلی ارائه گردید، و در ادامه، چارچوب مفهومی – نظری مطرح و بر اساس آن یافته‌ها و نتایج بررسی شد.

پیشینه پژوهش

پیشینه پژوهشی مربوط به جوامع اطلاعاتی و هوش مصنوعی هنوز در مراحل اولیه خود است. چنین وضعیتی متأثر از دیوار بلند دوقلوی محرمانگی آن است. دیوار اول توسط خود جوامع اطلاعاتی ساخته شده است که از افشای منابع و روش‌های آسیب‌پذیر و هوشیارکننده رقیبان و دشمنان جلوگیری می‌کند و دیوار دوم از همکاران حوزه فناوری این جوامع است که قراردادهای محرمانگی با آنان امضا می‌کنند، اما همچنین می‌خواهند از محصولات پیشرفته خود در برابر شبیه‌سازی یا سرقت توسط رقبای تجاری محافظت کنند (موران، برتون و کریستو، ۲۰۲۳). بنابراین، باتوجه‌به محدودیت‌های یادشده، به آثار کمی در حوزه اطلاعاتی دسترسی داریم. برخی از آثار که در این پژوهش مورد بررسی قرار گرفتند عبارت‌اند از؛

پژوهش معتبری توسط مک کلین و همکاران از پژوهشگران حوزه اینترنت و فناوری در مرکز پیو (۲۰۲۳) به‌صورت پیمایشی انجام شده است که نگرش‌ها و ادراک شهروندان ایالات متحده آمریکا را دربارهٔ حفاظت از داده‌های شخصی افراد، احساس امنیت دراین‌خصوص و اعتماد به صیانت از آن از سوی دستگاه‌های دولتی و شرکت‌های خصوصی مورد بررسی و تحلیل قرار داده‌اند. یافته‌های کلیدی این پژوهش توسط فاوریو ارائه شده است. این یافته‌ها نشان می‌دهد؛ علاوه بر اینکه ناخشنودی و بی‌اعتمادی گسترده‌ای نسبت به حکمرانی کنونی یادشده نسبت به حفاظت از داده‌های شخصی افراد وجود دارد، بلکه خواستار اصلاح قوانین و ایجاد یک چارچوب استاندارد و یکپارچه فدرال هستند.

گزارش تحلیلی – مقایسه‌ای معتبر از سوی مؤسسه بین‌المللی حقوقی دلا پایپر[1] (۲۰۲۴) به‌عنوان یکی از بزرگ‌ترین شرکت‌های حقوقی چندملیتی جهان؛ قوانین حفاظت از داده‌ها در ایالات متحده را ترکیبی پیچیده از قوانین و مقررات ملی، ایالتی و محلی معرفی می‌کند و اینکه این کشور فاقد یک قانون جامع قدرتمند است و باوجود اینکه در سال‌های اخیر، با اقدام کالیفرنیا (۲۰۱۸) دیگر ایالت‌ها اقداماتی را در این خصوص آغاز کرده‌اند و همچنین پیش‌نویس قانون جامع فدرال در سال ۲۰۲۴[2] ارائه شده است، اما تغییراتی در فضای سیاسی، پیچیدگی فزاینده و رفع نگرانی‌های مربوط به حریم خصوصی، ایجاد نشده است.

در پژوهشی دیگر توسط آیدون (۲۰۲۵) حفاظت از داده‌های شخصی افراد در عصر دیجیتال را به‌صورت تحلیل تطبیقی از مقررات ایالات متحده آمریکا و اتحادیه اروپا ارائه داده است. این پژوهشگر با پرداختن به پیشرفت‌های مستمر فناوری‌های دیجیتال، چشم‌انداز قانونی پیرامون حفاظت از داده‌های شخصی افراد را همچنان در حال تغییر می‌داند و با بررسی مقررات اتحادیه اروپا، به طور مستند اشاره می‌کند که ایالات متحده همچنان به یک مجموعه قوانین خاص و مقررات پراکنده و فزاینده ایالتی متکی است که بسیاری از مصرف‌کنندگان آمریکایی را با حفاظت‌های متناقض و فاقد یک استاندارد فدرال یکپارچه رها نموده است؛ بنابراین، موضوع حفاظت از داده‌های شخصی افراد در ایالات متحده در سال‌های آینده همچنان یک مسئله کلیدی است.

بهاراتی (۲۰۲۴) در پژوهشی حق حریم خصوصی در عصر هوش مصنوعی را به‌عنوان یک مسئله‌محوری و پیچیده مطرح می‌کند که با فناوری، حقوق و اخلاق تلاقی دارد. با ادامه توسعه فناوری‌های هوش مصنوعی و تبدیل آن به بخشی جدایی‌ناپذیر از بخش‌های مختلف زندگی بشری، حریم خصوصی افراد به طور فزاینده‌ای در معرض تهدید و تجاوز قرار می‌گیرد. این امر نگرانی‌های قابل‌توجهی در مورد نظارت گسترده، تضعیف حقوق حریم خصوصی و استفاده اخلاقی از هوش مصنوعی ایجاد کرده است. به‌ویژه اینکه، پیچیدگی و نامرئی‌بودن روش‌های جمع‌آوری داده‌ها که توسط فناوری‌های هوش مصنوعی صورت می‌گیرد، رفع چنین نگرانی‌هایی را دشوار نموده است.

---

1 . DLA Piper LLP

2 . American Privacy Rights Act of 2024(APRA)

انگر هوفر و همکاران (۲۰۲۴) در پژوهشی ضمن پرداختن به جنبه‌های مثبت فناوری‌های هوش مصنوعی در زندگی بشری، به یکی از جنبه‌های بسیار تاریک و ترسناک آن می‌پردازند و آن ازبین‌بردن مفهوم سنتی از حق حریم خصوصی است که به طور خاص با جمع‌آوری داده‌ها، نظارت و تصمیم‌گیری و چالش‌های آن گره‌خورده است.

چینمای (۲۰۲۵) در پژوهشی با رویکردی کیفی، پیامدهای حقوقی ناشی از تلاقی فناوری و نگرانی‌های مربوط به حریم خصوصی در جهان را بررسی می‌کند. این پژوهش این مفهوم را در پرتو آموزه‌های مختلف و رویه‌های قضایی پیشرو مورد بررسی قرار می‌دهد تا به مخاطب دیدگاهی جامع و فراگیر پیرامون آن و روابط آن با سایر حوزه‌ها، یعنی مالکیت معنوی، هوش مصنوعی، نگرانی‌های مربوط به حریم خصوصی و غیره ارائه دهد.

در پژوهشی توسط اسفتکو (۲۰۲۴) بهره‌گیری از هوش مصنوعی در آژانس‌های اطلاعاتی و نقش حیاتی آن در پردازش داده‌ها و تحلیل اطلاعات، و همچنین مسائل مرتبط با حوزه‌های دفاع و امنیت ملی بررسی شده است. پژوهشگر به کاربردهای مختلف این فناوری در آژانس‌های اطلاعاتی، پیامدها و چالش‌ها و نیز رعایت ملاحظات اخلاقی پرداخته است.

در پژوهشی توسط موران، برتون و کریستو (۲۰۲۳) باتوجه‌به پیشینه بهره‌گیری جامعه اطلاعاتی آمریکا از هوش مصنوعی در دهه‌های گذشته، به مزیت پیش‌گامی ایالات متحده در این عرصه از یک سو و اینکه سایر بازیگران جهانی باید با آن‌ها هماهنگ باشند، اشاره می‌کنند. آنان استدلال می‌کنند که جامعه اطلاعاتی ایالات متحده به دلیل قوانین ملی و بین‌المللی در خصوص جمع‌آوری و حفاظت از داده‌ها نخواهد توانست از تمام ظرفیت‌های این سیستم‌ها بهره‌برداری کند.

در پژوهشی دیگر توسط کینگ (۲۰۲۴) به‌صورت مستند، بر اساس یک پرونده از جنگ روسیه و اوکراین، پاسخ می‌دهد که ایالات متحده آمریکا چگونه از هوش مصنوعی برای هدف‌گیری دیجیتال بهره می‌برد.

در پژوهشی دیگر توسط میرمحمدی (۱۳۸۶) به بررسی تفکر حاکم بر جامعه اطلاعاتی آمریکا از مقطع وقایع ۱۱ سپتامبر و تأثیرات آن بر اصلاحات ساختاری این جامعه پرداخته است و ریشه‌های نظری آن را در چارچوب دو رویکرد فکری الگو محور و تهاجمی بررسی و تحلیل کرده است.

باوجود این آثار، این پژوهش با تأکید بر ترور داده‌محور دانشمندان و فرماندهان ایرانی و خانواده‌های آنان، برای پژوهشگران حقوق بشر و هوش مصنوعی، مقامات و مدیران عالی جمهوری اسلامی ایران یکی از مهم‌ترین موضوعات جدید محسوب می‌شود.

روش پژوهش

در این پژوهش، با تمرکز بر حق حریم خصوصی افراد در حقوق بین‌الملل، اقدامات جامعه اطلاعاتی آمریکا مبتنی بر هوش مصنوعی در نقض جهانی این حق، با روشی توصیفی – تحلیلی و به‌صورت مقایسه‌ای مورد بررسی قرار گرفته است.

منابع و مستندات اصلی مربوط به نقض حریم خصوصی در ترورهای داده‌محور (روسیه و ایران)، باتوجه‌به ضرورت‌های روش مقایسه تطبیقی، تحلیل گزارش‌های معتبر علمی، اندیشکده‌ها و مراکز مطالعاتی، بیانیه‌ها و اظهارات رسمی ناظر بر پیوندهای راهبردی رژیم صهیونیستی با سنتکام در دوره زمانی ۲۰۲۰ تا ۲۰۲۵ میلادی، موردتوجه قرار گرفته است. همچنین، باتوجه‌به ضرورت اثبات نقش‌آفرینی جامعه اطلاعاتی ایالات متحده آمریکا در هدایت و کنترل این جنگ‌های داده‌محور، پیشینه بیش از چهار دهه فعالیت این جامعه در توسعه و کاربرد فناوری‌های هوش مصنوعی و جنگ‌های داده‌محور، بر اساس مقالات نویسندگان شناخته شده بین‌المللی و اظهارات رسمی مقامات ذی‌ربط، مورد بررسی قرار گرفته است؛ بنابراین، موضوع جنگ‌های داده‌محور، باتوجه‌به منشأ، اعتبار، آثار حقوقی و حفظ انسجام اطلاعات، مورد تحلیل و بررسی قرار گرفته است، به‌گونه‌ای که این روند، اطمینان می‌دهد که یافته‌ها و نتایج اصلی، از اعتبار لازم برخوردارند.

فرضیه‌های اصلی این پژوهش، بر اساس سؤالات مطرح‌شده در مقدمه، عبارت‌اند از:

الف. توسعه و کاربرد هوش مصنوعی در جامعه اطلاعاتی آمریکا و ادغام فناوری‌های متنوع آن برای جنگ‌های داده‌محور علیه دیگر کشورها، پیشینه قابل‌توجهی دارد.

ب. جامعه اطلاعاتی آمریکا در هدایت و کنترل ترور مقامات و فرماندهان ارشد روسیه، دانشمندان و فرماندهان ایرانی و خانواده‌های آنان در اماکن مسکونی، با بهره‌گیری از هوش مصنوعی، نقش مؤثری ایفا می‌کند.
ج. جامعه اطلاعاتی ایالات متحده آمریکا، به طور مستمر، با جمع‌آوری و پردازش داده‌های کلان مربوط به مراکز فرماندهی‌های نظامی، از جمله سنتکام، آگاهانه اقدام به نقض حریم خصوصی اتباع دیگر کشورها می‌نماید.

چارچوب مفهومی و نظری

این قسمت، پایه و تعیین‌کننده سمت‌وسوی مسئله اصلی هر پژوهش است و به پژوهشگر جهت اصلی یافتن پاسخ سؤالات اصلی و ارائه یافته‌های پژوهش کمک می‌کند.

نقش هوش مصنوعی در معماری اطلاعات نظامی نوین

ایده ابتدایی و بخشی از توسعه اولیه و فلسفه هوش مصنوعی از رمزگشایان کد انیگمای آلمان در جنگ جهانی دوم نشأت گرفته است (موران، برتون و کریستو، ۲۰۲۳). این ایده که آلن تورینگ[1]، مخترع کامپیوتر در دهه ۱۹۳۰ و بعدها مدیر تیم موسوم به بِلچلی پارک[2]، تصور می‌کرد ممکن است روزی کامپیوتر هوشمند شود، طرح وولدرج (۱۴۰۰) و با ساخت و رمزگشایی آن، پیاده‌سازی کرد (موران، برتون و کریستو، ۲۰۲۳). این زمینه جذب و علاقه بازیگران عرصه اطلاعات نظامی (بریتانیا و ایالات متحده آمریکا) را فراهم نمود و پس از پایان جنگ، ایده آن در مقاله‌ای تحت عنوان آزمایش تورینگ در سال ۱۹۵۰ منتشر شد (وولدرج، ۱۴۰۰). در سال ۱۹۵۶، جان مک‌کارتی[3]، دانشمند جوان آمریکایی، با راه‌اندازی مدرسه‌ای تابستانه به نام «هوش مصنوعی» در کالج دارتموث نیوهمپشایر، همگان را با این نام و آغاز عصر طلایی آن آشنا نمود که تا نیمه دهه ۱۹۷۰ ادامه یافت (وولدرج، ۱۴۰۰).

اما علی‌رغم ورود کوتاه‌مدت به «زمستان هوش مصنوعی» به دلیل کاهش بودجه تحقیقاتی از سوی ادارات دولتی و سرمایه‌گذاران خصوصی، از اوایل دهه ۱۹۸۰ با ایجاد سیستم‌های خبره، گامی امیدوارکننده به سوی بهار هوش مصنوعی برداشته شد (ابوذری، ۱۴۰۲: ۲۷). باتوجه‌به پیشینه تاریخی یاد شده، نگاه بازیگران اصلی عرصه اطلاعاتی کشورهای صاحب فناوری‌های نوین از حساسیت مفرط بازدارنده به توسعه و کاربرد پیش‌برنده تغییر یافت. در این چهار دهه گذشته، پیشرفت‌های گسترده‌ای رخ داده است که ویژگی بارز آن، همه‌جا بودن و برای همه بودن است، باتوجه‌به کاربردهای متنوع آن و به‌طور خاص جمع‌آوری اطلاعات لحظه‌ای. بر همین اساس، این فناوری با حیات جامعه بشری و سرنوشت آن پیوند خورده است (وولدرج، ۱۴۰۰).

به‌طورکلی، امروزه هوش مصنوعی به‌عنوان مجموعه‌ای از سیستم‌ها و فناوری‌های مختلف، از جمله دستگاه‌ها، نرم‌افزارها و برنامه‌ها، شناخته می‌شود که تقریباً مانند انسان توانایی یادگیری و تصمیم‌گیری دارند. همچنین، این فناوری‌ها به آن‌ها اجازه می‌دهد بر اساس وظایف و شرایط موجود، به روشی معقول عمل کنند (ابوذری، ۱۴۰۲). بر پایه پردازش داده‌های کلان و مقایسه روندهای گذشته و حال، بهترین تحلیل‌ها، برآوردها و پیش‌بینی‌ها ارائه می‌شود.

ویژگی‌ها و کارکردهای مذکور، سازمان‌های اطلاعاتی کشورهای عضو سازمان ملل متحد را در متن این تحولات قرار داده است و هیچ راهی برای چشم‌پوشی از اصل آن وجود ندارد ؛ بنابراین، رهبران کشورهای مختلف در سراسر جهان باید مسئولیت‌های سنگین خود در کاربردهای جهانی این فناوری‌ها را درک کنند (کیسینجر، اشمیت، هوتنلانگر، ۱۴۰۳). در وهله اول نیز ، تحت یک دیپلماسی و چارچوب گذاری جهانی ، می توانند هدایت و کنترل مثبت(شکرالهی ومعتمدنژاد،۱۴۰۳) شرکت‌های فراملیتی و چندملیتی را بدست بگیرند. این شرکت‌ها و نهادها که از تابعین منفعل حقوق بین‌الملل به سمت تابعین فعال در عرصه جهانی در حال حرکت هستند(ضیایی بیگدلی،۱۴۰۳)، باید مسئولانه در توسعه و بهره‌برداری از فناوری‌های هوش مصنوعی مشارکت فعال داشته باشند.

حق بر حریم خصوصی در جامعه داده‌محور

[1] . Alan Turing
[2] . Bletchley Park
[3]. John MaCarthy

حق بر حریم خصوصی بر اساس مقدمه اعلامیه جهانی حقوق بشر مصوب مجمع‌عمومی سازمان ملل متحد پیوند خورده است. ماده ۱۲ این اعلامیه به طور خاص مقرر می‌دارد: «هیچ‌کس در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات خود نباید مورد مداخلات خودسرانه قرار گیرد و شرافت و نام و رسم او نباید مورد حمله قرار گیرد. هر فرد حق دارد در مقابل اینگونه مداخلات و حملات، تحت حمایت قانون قرار گیرد.» همچنین بندهای ۱ و ۲ ماده ۱۷ میثاق مدنی و سیاسی تصریح می‌کنند: «هیچ‌کس نباید در زندگی خصوصی، خانواده، اقامتگاه یا مکاتبات خود مورد مداخلات خودسرانه یا خلاف قانون قرار گیرد و شرافت و حیثیت او نباید مورد تعرض غیرقانونی قرار گیرد. هر فرد حق دارد در مقابل این نوع مداخلات یا تعرض‌ها، از حمایت قانون بهره‌مند شود.»

این حق، باتوجه‌به تحولات جهانی و تأثیرپذیری از توسعه و کاربرد هوش مصنوعی و شکل‌گیری جوامع داده‌محور، به مرحله‌ای بسیار حساس رسیده است. اما چشم‌انداز قانونی پیرامون آن، با تأکید بر حفاظت از داده‌های شخصی افراد، همچنان در حال تغییر است (آیدون، ۲۰۲۵). به‌ویژه اینکه چنین حقی، با حرکت جامعه بین‌المللی به سمت روابط و مناسبات تحت نفوذ هوش مصنوعی و پردازش داده‌های کلان جهانی، مرزهای سیاسی کشورهای عضو سازمان ملل را درنوردیده و به یک حق جهانی در این عصر تبدیل شده است. ازاین‌رو، برخلاف گذشته و با تغییر مفهوم سنتی این حق، ما با وضعیتی بسیار تاریک، ترسناک (انگرهوفر و همکاران، ۲۰۲۴) و پیچیده جهانی مواجه هستیم که با فناوری، حقوق و اخلاق تلاقی دارد. با ادامه توسعه فناوری‌های هوش مصنوعی و تبدیل آن به بخش جدایی‌ناپذیر زندگی بشر، حریم خصوصی افراد به طور فزاینده‌ای در معرض تهدید و تجاوز قرار می‌گیرد (بهاراتی، ۲۰۲۴).

بنابراین، می‌توان حریم خصوصی افراد در ارتباطات و تعاملات بین‌المللی، در بستر سکوهای خارجی و ابزارهای مخابراتی بهره‌مند از هوش مصنوعی، را به این صورت تعریف کرد که قلمرو زندگی افراد و اشخاص یک دولت است که آن افراد، معمولاً و یا با اعلام قبلی، انتظار دارند دیگران بدون رضایت آنان به داده‌ها و اطلاعات مربوط به آن قلمرو دسترسی نداشته باشند، وارد نشوند، نظارت نکنند یا درهرصورت دیگری، آنان را در آن قلمرو مورد تعرض قرار ندهند. دراین‌ارتباط، داده‌ها و اطلاعات مربوط به منازل و اماکن مسکونی، جسم افراد، و اطلاعات شخصی ناشی از رفت‌وآمدها و ارتباطات خصوصی، از مهم‌ترین مصادیق این حق هستند؛ بنابراین، جمع‌آوری داده‌های مربوط به این مصادیق و پردازش غیرقانونی آن‌ها، با هر هدف و مقصودی، مهم‌ترین نمونه‌های نقض حریم خصوصی محسوب می‌شود (انصاری، ۱۴۰۱).باوجود این، نباید از نظر دور داشت که پیچیدگی و نامرئی‌بودن روش‌های جمع‌آوری داده‌ها که توسط فناوری‌های هوش مصنوعی انجام می‌شود، تشخیص این موضوع را دشوار ساخته است (بهاراتی، ۲۰۲۴).

جامعه اطلاعاتی آمریکا و جنگ‌های داده‌محور

جامعه اطلاعاتی آمریکا مجموعه‌ای از وزارتخانه‌ها، آژانس‌ها، سازمان‌های مستقل، دفاتر و مدیریت‌های اطلاعات نظامی و غیرنظامی و همچنین ادارات تحلیل در دپارتمان اجرایی فدرال است که بر اساس وظایف و اهداف مشخص، در راستای اجرای امنیت ملی و روابط خارجی کشور با یکدیگر همکاری می‌کنند (قربانی و جواهری، ۱۴۰۲).

این جامعه به طور خاص، باتوجه‌به رقابت قدرت‌های بزرگ، دسترسی جهانی به فناوری‌های نوین و ضرورت‌های پاسخ مؤثر به تهدیدهای نوظهور، از حدود ۴۵ سال پیش بهره‌گیری از هوش مصنوعی را در دستور کار خود قرار داده و آن را توسعه داده است. بدون بهره‌گیری از هوش مصنوعی، این جامعه اطلاعاتی ممکن است ناکارآمد و منسوخ شود (ایوبنک، ۲۰۲۴). بر اساس برآوردهای داخلی، ایالات متحده در معرض تهدیدات جدی خارجی قرار دارد. کمیسیون امنیت ملی هوش مصنوعی[1] در گزارشی اعلام کرد که باید هوش مصنوعی را برای تغییر روش‌های دفاع از آمریکا، بازداشتن دشمنان، استفاده از اطلاعات برای درک جهان و پیروزی در جنگ‌ها به کار گرفت (استون، ۲۰۲۴).

اولین سرمایه‌گذاری‌های رسمی جامعه اطلاعاتی آمریکا در حوزه هوش مصنوعی به جان مک ماهون، معاون مدیر سازمان اطلاعات مرکزی[2]، در آوریل ۱۹۸۲ نسبت داده می‌شود. او باتوجه‌به ۳۰ سال مسئولیت‌های مدیریتی در پروژه‌های ویژه و فناوری‌های

[1] . The National Security Commission on Artificial Intelligence (NSCAI)
[2] . The deputy director of the Central Intelligence Agency (DD/CIA)

اطلاعاتی، منشأ تغییرات و تحولات گسترده در این جامعه شد. سوابق و شهرت جان مک ماهون به‌عنوان «شاخه کیو» در آژانس اطلاعات مرکزی [1]و آشنایی گسترده او با «جادوگران لنگلی»، درک کارکردهای هوش مصنوعی را که می‌تواند با داده‌های بیشتر، الگوریتم‌های بهبود یافته و قدرت پردازش بیشتر، جاسوسی را متحول کند، پیش‌تر از زمان خود برد (موران، برتون و کریستو، ۲۰۲۳).

در سال ۱۹۸۳، فرماندهی سیا در اولین گام، مدیران و کارکنان این سازمان را با فناوری‌های اولیه هوش مصنوعی آشنا کرد. اسناد سیا تا سال ۱۹۸۷ نشان می‌دهند که جان مک ماهون، علاوه بر نقش مؤثر در اصلاح نگرش جامعه اطلاعاتی آمریکا درباره هوش مصنوعی، با اقدامات و برنامه‌های قابل‌توجه، برخی فناوری‌های هوش مصنوعی را با سازمان و نهادهای مرتبط در تعامل با دانشگاه‌ها و شرکت‌های خصوصی ادغام و نهادینه کرد. ازاین‌رو، او را می‌توان پدر هوش مصنوعی در جامعه اطلاعاتی دانست (موران، برتون و کریستو، ۲۰۲۳).

بعدها، جامعه اطلاعاتی تحت سیاست‌های حمایت دفاعی دولت رونالد ریگان علیه اتحاد جماهیر شوروی قرار گرفت. با اهداف برون‌مرزی آن، در دهه‌های ۱۹۸۰ و ۱۹۹۰ میلادی در فضای جنگ سرد و آغاز کاربرد هوش مصنوعی توسط آژانس‌های اطلاعاتی از ابتدای آن (اسفتکو، ۲۰۲۴)، موفقیت‌های متوسطی در توسعه فناوری‌های نظارتی و مدیریت حجم انبوه تماس‌های تلفنی شوروی به دست آمد که ممکن است در تغییر و تحولات اجتماعی و سیاسی منتهی به فروپاشی شوروی نقش داشته باشد. این دستاوردهای جهانی، زمینه‌ساز شکل‌گیری دیدگاه‌های رسوب یافته درباره هوش مصنوعی به‌عنوان دارایی اصلی حفظ نظام تک‌قطبی شدند. امروز، جامعه اطلاعاتی آمریکا با پروژه‌های متعددی، از جمله پیشگامان بهره‌برداری تسلیحاتی و اطلاعاتی از هوش مصنوعی در جهان است. در اجلاس اطلاعات و امنیت ملی ۲۰۱۸، داون مایریکس، مدیر علم و فناوری سیا، فاش کرد که این سازمان ۱۳۷ پروژه هوش مصنوعی دارد. در سال ۲۰۲۱، کمیسیون امنیت ملی آمریکا، چشم‌اندازی تا سال ۲۰۳۰ برای توسعه هوش مصنوعی ترسیم کرد (موران، برتون و کریستو، ۲۰۲۳).

رویکردهای جهانی آمریکا در کاربردهای هوش مصنوعی

پیشینه توسعه و کاربرد هوش مصنوعی در جامعه اطلاعاتی آمریکا، مزیت پیش‌گامی جهانی آن را تضمین نموده است و این خود یکی از چالش‌برانگیزترین موضوعات جهانی محسوب می‌شود؛ چراکه ایالات متحده سوابق و پیشینه‌هایی را ایجاد نموده است که سایر کشورهای جهان می‌بایست یا تحت یک جبرگرایی با آنها هماهنگی و از استانداردهای آنان تبعیت کنند، یا مذاکره نمایند؛ تا به یک پیمان امنیتی دو یا چندجانبه دست یابند، یا با مقاومت و تکیه بر فناوری‌های بومی خود، این تهدیدات را مدیریت و مرتفع سازند (موران، برتون و کریستو، ۲۰۲۳).

علاوه بر چالش یاد شده، باتوجه‌به اینکه نظم حاکم بر جامعه اطلاعاتی آمریکا، تابعی از بنیان‌های نظری لیبرال از یک سو و نظم حقوقی داخلی متأثر از بنیان‌های یادشده با ترجیح بر تعهدات بین‌المللی آنان است (دادمهر، ۱۳۹۴)؛ این پیشگامی از لحاظ سیاسی و حقوقی نیز این تهدیدات را نهادینه و تعمیق بخشیده است. چراکه ریشه‌ها و بنیان‌های چنین نظمی را باید در آیینه هویت سیاسی ملی این کشور که در درجه نخست از راه انگاره «باور به استثنایی بودن»[2] ابراز می‌شود، شناخت. چراکه الگوی ذهنی – تاریخی این دولت کشور از خود همواره به‌عنوان موجودیتی استثنایی و «ملتی برگزیده» بوده است که یک اراده مافوق بشری آن را راهبری می‌کند و همین بر اراده و مأموریت‌های ادواری رهبران سیاسی آن از جمله مأموریت ویژه آنان برای پیشبرد ارزش‌ها و نهادهای لیبرال دموکراتیک در خارج از آمریکا تأثیر عمیقی داشته است. ازاین‌رو، راهبرد توسعه لیبرالیسم و دموکراسی (ارزش‌های آمریکایی) در سطح بین‌الملل یک جریان مداوم در تاریخ دیپلماسی آمریکا است. براین‌اساس، دو رویکرد فکری در میان رهبران

[1] . Central Intelligence Agency (CIA)
[2] . Ecxeptionalism

سیاسی و اندیشمندان آن شکل‌گرفته است؛ رویکرد فکری الگو بودن و تهاجمی بودن که هم‌زمان و در تعامل با هم در بسیاری از تحولات داخلی و بین‌المللی ایالات متحده آمریکا نقش داشته‌اند (میرمحمدی، ۱۳۸۶).

بنابراین، باتوجه‌به بنیان‌های نظری و رویکردهای فکری متأثر از آن، از جمله رویکرد تهاجمی در طول چهار دهه گذشته و به‌ویژه پس از وقایع یازدهم سپتامبر، تأثیر مستقیمی بر فلسفه بهره‌گیری از هوش مصنوعی در رهبری نظام تک‌قطبی داشته است. هدف از این بهره‌گیری، پیش‌بینی تصویری از جهان‌نما و شناسایی تهدیدات همه‌جانبه آینده علیه ایالات متحده است. بر خلاف تصور رایج در جوامع اطلاعاتی که «تصور آیینه‌ای»[1] نامیده می‌شود، تولید «اطلاعات ترکیبی و استراتژیک زنده» نقش کلیدی در این فرایند دارد. این نوع اطلاعات، کارکرد اصلی آن، تصویرسازی عینی تهدیدات بر اساس شناخت ماهیت سیاسی، ادراک نیات واقعی و اهداف اصلی رقبا و دشمنان است. هدف نهایی، انطباق با مطلوبیت موردانتظار است که ممکن است شامل بازگوکردن حقایق یا توجیه دقیق (اطلاعات مطلوب) درباره دستور کارهای سیاسی رهبران باشد. این فرایند نیازمند جمع‌آوری و پردازش داده‌های کلان و دقیق از تمامی ابعاد زندگی فردی و اجتماعی است، همچنین شامل افکار جاری در کشور یا کشورهای هدف که تحت یک شبکه و ساختارهای جهانی با ترکیبی از سیستم‌های هوش مصنوعی قرار دارند. این سیستم‌ها می‌توانند شاخص‌های پیش‌گامی اطلاعاتی در عصر حاضر را تأمین کنند. این فرایند شامل تمرکززدایی از عملیات‌های اطلاعاتی سازمان سیا، تحلیل اطلاعات برای ساختن آینده موردانتظار، نه صرفاً پیش‌بینی آن، و ترکیب عملیات‌های پنهانی با زندگی روزمره مردم کشور است. همچنین، نفوذ و کنترل مستمر در لایه‌های مختلف جامعه، از جمله اهداف این رویکرد است (میرمحمدی، ۱۳۸۶).

بر اساس همین رویکرد تهاجمی جهانی و نیز ملاحظات فنی، جامعه اطلاعاتی ایالات متحده از همان ابتدا، پروژه‌های هوش مصنوعی را به طور کامل به داخل و قلمرو ملی خود محدود نکرده است (ایوبنک، ۲۰۲۴) و به همین دلیل صنعت فناوری‌های ایالات متحده متنوع و پراکنده است، با طیف گسترده‌ای از ایدئولوژی‌ها و منافع، نه‌تنها در سیلیکون‌ولی[2] بلکه در جنوب غربی، ساحل شرقی و دفاتری در سراسر جهان واقع شده‌اند (موران، برتون و کریستو، ۲۰۲۳). این حکمرانی جهانی مبتنی بر هوش مصنوعی ایدئولوژیک آمریکایی، اولاً، اقدامات ساختارشکنانه جامعه اطلاعاتی آمریکا برای بهره‌گیری از پتانسیل کامل سیستم‌ها و فناوری‌های هوش مصنوعی، از طریق مقابله با قوانین محدودکننده استفاده از داده‌های خصوصی در سطح بین‌المللی، را به دنبال داشته است و ثانیاً دورزدن شرکت‌های خصوصی همکار فناوری آنان که به آنان اجازه نمی‌دهند فناوری‌هایشان را به روش‌هایی که با منافع و ایدئولوژی خودشان همسو نیست، استفاده کنند، منجر به سلاح مخفی‌شدن آنها در سراسر جهان شده است. نمونه‌هایی از این موارد شامل اختلاف بین اپل و اداره تحقیقات فدرال[3] بر سر رمزگذاری و حق دسترسی اداره به ارتباطات امن ذخیره‌شده در آیفون‌های افراد مظنون (موران، برتون و کریستو، ۲۰۲۳) و یا قابلیت داده‌های پیش‌بینی‌کننده است که با سنجش دمای جمعیت کشورها در سازه‌های جهانی، رویدادهای اجتماعی مانند ناآرامی در مکزیک و پاراگوئه در سال ۲۰۱۲ را از طریق بررسی خودکار داده‌های عمومی، محتواهای خبری و گزارش‌های اقلیمی، ارائه می‌دهند و امکان پیش‌بینی رویدادهایی مانند بهار اسلامی و سرکوب نرم آنها را فراهم می‌کنند که مخاطرات جدی برای امنیت جهانی و امنیت بین‌الملل است؛ بنابراین، بخش عمده‌ای از انگیزه برای کار باهوش مصنوعی، نه‌تنها از نخبگان کامپیوتر در آژانس امنیت ملی[4] بلکه از دفاتر اجرایی طبقه هفتم سازمان سیا که بیشتر به دلیل اطلاعات جمع‌آوری‌شده منابع انسانی و انجام عملیات مخفی شناخته می‌شوند، نشأت می‌گیرد (موران، برتون و کریستو، ۲۰۲۳). این دفاتر ریشه‌های عمیقی در پروژه‌های ادغامی سازمان سیا با هوش مصنوعی دارند و ترکیبی از منابع اطلاعاتی متنوع، با رفع آسیب‌های پیشین مانند «مه داده»[5] و «استوپایپینگ»[6] را رقم زده‌اند، و بدون آن‌ها باید پیش‌گامی چین و پایان تاریخ لیبرال دموکراسی را بپذیرند.

---

1 . Mirror Imaging
2 . Silicon Valley
3 . Federal Bureau of Investigation(FBI)
4 . The National Security Agency (NSA)
5 . Data smog
6 . Stovepiping

مرکز علوم و امور بین‌الملل بلفر[1] گزارشی به سفارش دفتر مدیر اطلاعات ملی[2] تهیه کرد که در آن اعلام شد؛ هوش مصنوعی به همان روشی که هواپیماها و سلاح‌های هسته‌ای جنگ‌های مدرن را متحول کردند، متحول خواهد کرد و جهانی از هژمون‌های هوش مصنوعی را پیش‌بینی کرد که مشابه قدرت‌های هسته‌ای قرن بیستم هستند (موران، برتون و کریستو، ۲۰۲۳). بنابراین، همچنان در مقدمه اشاره شد، کارکرد تسلیحاتی هوش مصنوعی و بنیان‌های جهانی آن، از جمله در جنگ‌های اطلاعاتی، ضد اطلاعاتی و «جاسوسی نسل چهارم» (موران، برتون و کریستو، ۲۰۲۳) و ترور، از سوی جامعه اطلاعاتی ایالات متحده، موضوعی ناشناخته نیست.

تحلیل مسئولیت ایالات متحده در نقض حریم خصوصی

جامعه اطلاعاتی آمریکا پس از دوره زمستان هوش مصنوعی و از آغاز دهه ۱۹۸۰، هوش مصنوعی را در متن اجرای طرح‌ها و برنامه‌های فناورانه خود قرار داده است و برای بهره‌گیری از ظرفیت‌های آن، اقدامات عملی قابل‌توجهی انجام داده است. بنابراین، جایگاه هوش مصنوعی در جامعه اطلاعاتی آمریکا تابعی از پیشینه تاریخی آن در حدود ۴۵ سال گذشته است. به‌نحوی‌که باوجود دو دیوار دوقلوی محرمانگی، تصویری قابل‌توجه از زوایای این ادغام ترسیم می‌شود. این وضعیت، علاوه بر شناساندن اجمالی ساختارها، در اختیار داشتن بن‌سازه‌های جهانی و پراکنده در سراسر جهان، بنا بر اقتضائات و سیاست‌های ایالات متحده، »دسترسی پیچیده و نامرئی» (بهاراتی، ۲۰۲۴) به داده‌های تولیدی مستمر اتباع دیگر کشورها و نیز کارکردهای متنوع مورد بهره‌برداری آن؛ تصویر واقعی از یک حکمرانی اطلاعاتی و نظامی جهانی ترسیم می‌کند.

در همین ارتباط به طور خاص، جامعه اطلاعاتی ایالات متحده تحت حکمرانی یاد شده و باوجود بازتوزیع صلاحیت‌ها و مأموریت‌های آن بالاخص بعد از ۱۱ سپتامبر، با بهره گیری از شرکت‌های فراملی و چند ملیتی دارای بن سازه های جهانی در بستر اینترنت، بطور مستمر نسبت به جمع آوری فراگیر و پردازش داده‌های کلان مردم ملل متحد اقدام و حریم خصوصی آنان را با نقض گسترده ای مواجه نموده است و با وجود مساله بنیادی چگونگی مدیریت تضاد میان فعالیتهای نامرئی فناورانه جامعه اطلاعاتی با مجموعه ای از هنجارها و نظارت بر پردازش داده ها و تولید اطلاعات در چارچوب هنجارهای حقوقی ملی و بین المللی با تاکید بر بنیان های حقوق بشری (میرمحمدی ،۱۴۰۲)؛ مکانیزم قانونی جامع و شفاف فدرالی در حال حاضر وجود ندارد و با ترکیبی پیچیده از قوانین حفاظت از داده ها در سطح ملی، ایالتی و محلی روبرو هستیم (دلا پاپیر،۲۰۲۴) تا جایی که چنین وضعیتی ناخشنودی و بی‌اعتمادی گسترده مردم این کشور را نسبت به حکمرانی در حفاظت از داده های شخصی افراد را بدنبال داشته است(مک کلین و همکاران، ۲۰۲۳). بنابراین نمی توان گفت که ایالات متحده همچون اتحادیه اروپا و قانونگذاری آن (دشتی و معتمدنژاد،۱۴۰۳) در حفاظت از داده های عمومی از یک سازوکاری جهانی برای تضمین حاکمیت قانون و تعهدات بنیادین حقوق بشری بهره می برد(محمودی پرچینی ، ریاضی و پورابراهیمی، ۱۴۰۳).

بررسی اسناد و گزارش‌های رسمی نشان می‌دهد که به طور خاص، قریب به دو دهه از کارکرد تسلیحاتی هوش مصنوعی و بن سازه‌های جهانی آن توسط جامعه اطلاعاتی آمریکا می‌گذرد و مقامات آمریکایی به این موضوع اذعان کرده‌اند و در به‌کارگیری این فناوری‌ها، به‌ویژه در جریان فروپاشی اتحاد جماهیر شوروی و پس از آن، تا کنون، این فناوری‌ها به‌عنوان دارایی استراتژیک جهان تک‌قطبی و حافظ آن شناخته شده‌اند (موران، برتون و کریستو، ۲۰۲۳).

اسناد و گزارش‌های رسمی نشان می‌دهد که یکی از مهم‌ترین پروژه‌های هوش مصنوعی با کارکرد تسلیحاتی، همکاری سازمان سیا با شرکت نرم‌افزاری پالانتیر تکنولوژی است؛ نرم‌افزاری که اطلاعات موقعیت‌یاب را از انبوهی پیام‌های بدون ساختار، داده‌های شبکه، تلفن و اسناد سرقتی در قالب نقشه‌ها، هیستوگرام‌ها و نمودارهای ارتباطی به دست می‌آورد. ژنرال دیوید پترائوس، رئیس سابق سیا، به ماهیت این نرم‌افزار برای داده‌کاوی مجموعه‌های داده‌های کلان به‌منظور کاربردهای اطلاعاتی و نظامی اذعان نموده بود (موران، برتون و کریستو، ۲۰۲۳)؛ بنابراین یکی از مهم‌ترین کاربردهای هوش مصنوعی در جامعه اطلاعاتی آمریکا در

[1] . The Belfer Center for Science and International Affairs
[2] . The director of national intelligence (DNI)

اطلاعات نظامی است (کینگ، ۲۰۲٤). هدایت و کنترل مؤثر ایالات متحده در ترور فرماندهان ارشد روسیه و دانشمندان و فرماندهان ایرانی دو نمونه بارز این عملیات‌هاست که دلالت بر نقض حق حریم خصوصی افراد دارد.

۱. هدایت و کنترل در ترور فرماندهان روسیه

در ارتباط با پرونده جنگ روسیه و اوکراین که فناوری‌های هوش مصنوعی در آن نقش‌محوری از جمله در دفاع سایبری، حملات نظامی، عملیات‌های اطلاعاتی و هدف‌گیری‌های دیجیتال دارد (کینگ، ۲۰۲٤)، پیشینه مستندی از ابعاد هدایت و کنترل جامعه اطلاعاتی آمریکا در ترور فرماندهان روسیه ارائه می‌دهد.

به‌طورکلی تا پیش از فوریه ۲۰۲۲، اوکراین دارای یک اکوسیستم پیشرفته برای توسعه و کاربرد هوش مصنوعی در حوزه تجاری بود و در بخش صنعت دفاعی بر سخت‌افزارهای سنتی متمرکز بود (گنچاروک، ۲۰۲۵). اما جنگ اوکراین و روسیه، به اولین جنگی تبدیل شد که هر دو طرف در هوش مصنوعی و با آن رقابت‌ها را آغاز کردند و به یک جزء حیاتی پیروزی مبدل شد. بالاخص اینکه توسعه‌دهندگان فناوری‌های هوش مصنوعی خارجی (ناتو) از جنگ به‌عنوان بستری آزمایشی برای ارزیابی کارکردهای آن در میدان جنگ استفاده می‌کنند.

ازاین‌رو، یکی از جنبه‌های منحصربه‌فرد این جنگ در اوکراین، پشتیبانی بی‌سابقه توسط شرکت‌های خارجی و به طور خاص ایالات متحده است (گنچاروک، ۲۰۲۵؛ بُندار، ۲۰۲٤)؛ همچون «اسپیس‌اکس» برای دسترسی آنی به انتقال داده‌ها، «جنرال اَتامیکس» در سامانه‌های هوایی بدون سرنشین، «اِروواِیرنِمنت» در پهپادهای تاکتیکی سبک و شبکه‌های هوشمند میدان جنگ، و نیز تعامل با سیستم‌های دلتا و کروپووا در اوکراین؛ «کراوداسترایک» در تشخیص و واکنش به تهدیدات سایبری در زمان واقعی؛ «فایِرآی» در تحلیل تهاجم‌های پیشرفته. اما در این میان، «پالانتیر»[1] (بُندار، ۲۰۲٤) با ارائه قابلیت‌های گسترده اشتراک‌گذاری داده‌ها به فرماندهی نظامی، نقش‌محوری ایفا کرده است و از طریق متاکانستلیشن خود شبکه‌ای از تمام منابع داده‌ای عملیاتی در سطوح مختلف زمین، هوا، فضا و سایبر یکپارچه‌سازی داده‌های تجاری تا اطلاعات طبقه‌بندی‌شده از سرویس‌های اطلاعاتی خارجی را در مقیاس کلان تسهیل کرد.

نکته قابل‌توجه این است که در طول آزادسازی خرسون، ارتش اوکراین از اطلاعات دقیقی در مورد حرکات نیروهای روسی بهره‌مند شد و امکان حملات دقیق دوربرد را فراهم کرد (ایگناتیوس، ۲۰۲۲). همچنین شرکت‌های آمریکایی مانند «پِلَنت لَبز»، «بِلَک اسکای تِکنالِجی» و «مَکسار تِکنالِجی»، با تولید تصاویر ماهواره‌ای از عملیات‌های جنگی جاری و به اشتراک‌گذاری داده‌ها با دولت و نیروهای مسلح اوکراین (گنچاروک، ۲۰۲۵)، سهم قابل‌توجهی در هدایت و کنترل این جنگ داده‌محور دارند.

در همین چارچوب، در عملیات مشترک ایالات متحده و اوکراین در اول ماه مه ۲۰۲۲، والری گراسیموف، رئیس ستاد ارتش روسیه و مقام مسئول عملیات نظامی ویژه در اوکراین، به همراه جمعی از افسران ارشد روسیه، به طور غافلگیرانه‌ای در حال بازدید از مرکز فرماندهی ارتش روسیه در شهر ایزیوم در منطقه خارکیف، با سامانه موشکی هیمارس آمریکایی که از هدایت ماهواره‌ای برخوردار هستند مورد هدف‌گیری دیجیتال قرار گرفتند. در این حمله، تعدادی از افسران ستاد کشته شدند و خود رئیس ستاد ارتش روسیه نیز مجروح شد. این عملیات‌های مشترک، الگوی جدید جنگ داده‌محور را تحت هدایت و کنترل ایالات متحده ارائه می‌کند (بارنز، کوپر و اشمیت، ۲۰۲۲).

طراحی و پیاده‌سازی این عملیات‌های مشترک از سوی تیم منتسب به فرماندهی هجدهم هوابرد ایالات متحده آمریکا[2] صورت‌گرفته است. این فرماندهی که در ویسبادن[3] آلمان از سال ۲۰۱۵ آموزش نیروهای اوکراینی را هماهنگ می‌کرد، با شروع جنگ روسیه و اوکراین، نقش پشتیبانی عملیات فوری از نیروهای اوکراینی، از جمله هدف‌گیری داده‌محور را ارائه داده است. این یگان از سال ۲۰۱۹ تا ۲۰۲۲ تحت فرماندهی ژنرال اریک کوریلا[4] که به‌عنوان یکی از فرماندهان نیروهای عملیات ویژه ایالات متحده در

---

1 . The software company Palantir Technologies

2 . The XVIII Air- borne Corps

3 . Weisbaden

4 . General Erik Kurilla

افغانستان تحت پروژه ماون وزارت دفاع آموزش‌دیده و آن را به این یگان منتقل نموده بود دارای توان هدایت و کنترل چنین جنگ‌هایی بوده است. کوریلا بعد از خود، فرماندهی را به جانشین خود، ژنرال کریستوفر دونوهو[1] سپرد؛ فرماندهی که همچون کوریلا در نیروهای عملیات ویژه در عراق و افغانستان، عملیات‌های داده‌محور را در عمل و به‌عنوان اپراتور نیروهای ویژه آموخته بود و سپس به‌عنوان فرمانده لشکر ۸۲ هوابرد ارتش آمریکا به کار گرفته شده بود.

کوریلا و دونوهو با تکیه بر چنین تجربه‌ای در ستاد فرماندهی هجدهم هوابرد، با انتصاب یک مدیر ارشد فنی غیرنظامی و استخدام متخصصان داده‌های غیرنظامی و نظامی، تغییر و تحولات لازم را ایجاد کردند و با انتصاب دونوهو به فرماندهی متعاقباً در سال ۲۰۲۲، یک کارآفرین و مدیر اجرایی مشهور را استخدام کردند تا اطمینان حاصل شود که این یگان به یک سازمان داده‌محور تبدیل می‌شود. همین سازمان توانست یکی از مهم‌ترین هدف‌گیری‌ها را مبتنی بر ردپای دیجیتالی در فضای مجازی به نام خود ثبت کند.

بر اساس مستندات موجود، این یگان برای توسعه و اصلاح نرم‌افزار هدف‌گیری به پشتیبانی فنی و همکاری شرکت پالانتیر تکنولوژی متکی بوده است؛ شرکتی که در سال ۲۰۰۳ تأسیس و با ارائه پشتیبانی نرم‌افزاری به وزارت دفاع، مستقیماً در تأمین امنیت ملی ایالات متحده مشارکت داشته است و در سال ۲۰۰۹ شروع به فروش مستقیم آن به واحدهای مختلف آمریکایی در عملیات‌های عراق و افغانستان کرد. در سال ۲۰۱۱، کوریلا و دونوهو برای اولین‌بار با نرم‌افزار این شرکت مواجه شدند و با هدف‌گیری اسامه بن‌لادن در ماه مه ۲۰۱۱ میلادی با ابعاد ویژه این «سلاح مخفی» به تعبیر هفته‌نامه بیزینس ویک، آشنا شدند. واشنگتن‌پست در مقاله‌ای، محتاطانه و باتوجه‌به طبقه‌بندی فرایند هدف‌گیری، این عملیات را با جزئیات شرح داده است (ایگناتیوس، ۲۰۲۲). همین الگوی عملیات داده‌محور در سال ۲۰۲۱ علیه اهداف حماس در غزه به‌عنوان اولین جنگ دیجیتال (کینگ، ۲۰۲٤) و پس از ۷ اکتبر ۲۰۲۳ تاکنون در کل حوزه فرماندهی سنتکام پیاده‌سازی شده است.

۲. هدایت و کنترل در ترور دانشمندان و فرماندهان ایران

در ارتباط با مسئولیت هدایت و کنترل ایالات متحده در ترور دانشمندان و فرماندهان ایران در جنگ ۱۲ روزه؛ باتوجه‌به پیشینه قابل‌استناد یاد شده و دیگر مستندات و گزارش‌های ذیل، بالاخص در چارچوب اظهارات صریح ۶ نوامبر ۲۰۲۵ رئیس‌جمهور ایالات متحده، این موضوع قابل‌اثبات است.

الف. در ۱۵ ژانویه ۲۰۲۱، در آستانه تغییر دولت ترامپ، رژیم صهیونیستی از منطقه فرماندهی اروپایی ایالات متحده[2] به فرماندهی مرکزی سنتکام[3] منتقل شد. این انتقال نشانگر یک چرخش راهبردی در هدایت و کنترل امنیتی و نظامی آمریکا در همکاری با رژیم صهیونیستی در منطقه غرب آسیا محسوب می‌شود. بر اساس یادداشتی که توسط مرکز مطالعات امنیت ملی اسرائیل، وابسته به دانشگاه تل‌آویو، منتشر شده است، این تصمیم ترامپ منجر به ارتقای ترتیبات امنیتی منطقه‌ای، به‌ویژه در مواجهه با ایران، خواهد شد. در این یادداشت تصریح شده است که روابط اسرائیل با سنتکام اخیراً پدیدار نشده است، بلکه این روابط پس از سال‌ها توسعه و تدریجی شکل‌گرفته است. همچنین، بازدیدها و جلسات با فرماندهان سنتکام و ستادهای آن‌ها از اوایل دهه گذشته آغاز شده است. در اوایل سال ۲۰۱۶، گزارش شد که یک کانال گفتگوی سه‌جانبه بین ارتش اسرائیل و دو فرماندهی اروپا و سنتکام، به ریاست معاون رئیس ستاد کل ارتش اسرائیل، وجود دارد. این کانال مخفیانه حدود یک دهه قبل آغاز شده و از آن زمان، با جلسات فرماندهان و افسران ستاد، عمدتاً در اسرائیل و در مقر فرماندهی اروپایی در آلمان، ادامه یافته است. پیامد اصلی این ساختار جدید، کمک به ایالات متحده در ایجاد یک ائتلاف منطقه‌ای با مشارکت کشورهای عربی و اسرائیل علیه تهدیدات ایران است. این ائتلاف بستری برای ارتقای روابط امنیتی بین متحدان ایالات متحده و همچنین ترتیبات امنیتی منطقه‌ای تحت حمایت آمریکا فراهم می‌کند، از جمله هشدارهای اولیه و اطلاعاتی، مبارزه با تروریسم، دفاع هوایی، دفاع ضد موشکی، آموزش و ذخایر. موضوعاتی که

---

1 . General Christopher Donohue

2 . The United States European Command (EUCOM)

3 . The United States Central Command (CENTCOM)

از سوی پژوهشگر ارشد حوزه امنیت خلیج‌فارس در مؤسسه واشنگتن برای سیاست خاور نزدیک[1] در ۱۵ ژانویه ۲۰۲۱، با جزئیات مشابه، مورد بررسی قرار گرفته است.

ب. انتقال رژیم صهیونیستی از فرماندهی اروپایی ارتش آمریکا به حوزه مسئولیت سنتکام؛ همان‌طور که در یادداشتی که در تاریخ ۲۲ فوریه ۲۰۲۱ توسط مرکز مطالعات راهبردی بگین – سادات[2] منتشر شده است، اشاره شده است که این رژیم در حال تبدیل‌شدن به عضو مرکزی یک اتحاد منطقه‌ای ضدایرانی است. این اقدام در نهایت به‌عنوان یک اقدام جمعی منطقه‌ای برای کاهش حضور ایران در حوزه سنتکام تفسیر می‌شود و همچنین برای جنگ احتمالی قریب‌الوقوع آماده‌سازی می‌کند و همکاری‌های عملیاتی روزمره را تسهیل می‌نماید (لاپین، ۲۰۲۱).

ج. بر اساس گزارش مؤسسه یهودی برای امنیت ملی آمریکا[3] در خصوص حمایت از طرح انتقال رژیم صهیونیستی به حوزه فرماندهی سنتکام که از آوریل و اکتبر ۲۰۲٤ آشکارتر گردید، همچنان‌که مایکل ماکوفسکی، رئیس و مدیرعامل مؤسسه یادشده اظهار نموده است، این تغییر بازی با تمرکز سنتکام بر ایران و همچنین رویکرد تهاجمی فرمانده آن، ژنرال اریک کوریلا، علیه ایران صورت گرفته و هماهنگی بسیار نزدیکی را بین آنها به‌عنوان «یک دارایی استراتژیک مهم» رقم زده است (سنتکام، ۲۰۲۴). موضوعی که یک مقام نظامی رژیم صهیونیستی در آغاز تجاوز نظامی علیه ایران و ترور دانشمندان و فرماندهان نظامی بدان اذعان نمود؛ اینکه ارتش ایالات متحده از روز اول این جنگ شریک اصلی بود و این اغراق نیست (جینسا، ۲۰۲۲).

براین‌اساس، اظهارات رئیس‌جمهور آمریکا در هدایت و کنترل تجاوز ۱۳ ژوئن ۲۰۲۵ به ایران نه‌تنها تأیید می‌شود؛ بلکه هماهنگی‌های لازم آن با تغییر ساختارها و مأموریت‌های یاد شده از سال ۲۰۲۱ به طور رسمی و علنی اعلام شده است؛ بنابراین، ایالات متحده علاوه بر نقض منشور ملل متحد، باتوجه‌به نقش‌آفرینی «هدایت و کنترل»، مسئولیت این تجاوز نظامی و ترورهای داده‌محور متوجه آن است.

به طور خاص در ارتباط با نقض حریم خصوصی اتباع دیگر کشورها، باوجود وضعیت پیچیده و ترکیبی از قوانین و مقررات ملی، ایالتی و محلی، و وضع برخی قوانین محدودکننده داخلی پس از افشاگری‌ها درباره نحوه جمع‌آوری داده‌ها توسط سازمان‌ها و مدت زمانی که می‌توانند آن را برای اهداف تحلیلی نگه دارند، نظارت (جاسوسی) الکترونیکی بر افراد غیرآمریکایی در خارج از ایالات متحده بر اساس بخش ۷۰۲ قانون نظارت بر اطلاعات خارجی[4] و با اجازه دادگاه اعمال می‌شود. جامعه اطلاعاتی آمریکا نسبت به دور زدن قوانین تحت معافیت‌های خاص اقدام می‌کند. تا جایی که در اوایل سال ۲۰۲۲، دو تن از اعضای کمیته اطلاعات سنا ادعا کردند که سیا با انجام جمع‌آوری انبوه داده‌ها و اطلاعات تحت مجوز فرمان اجرایی ۱۲,۳۳۳ دوران ریگان (۱۹۸۱)، نظارت قضایی و کنگره را دور می‌زند (موران، برتون و کریستو، ۲۰۲۳). با جمع‌بندی مطالب مطروحه، اکنون می‌توان مهم‌ترین یافته‌های این پژوهش را به شرح ذیل ارائه نمود.

الف. ایالات متحده آمریکا، الگوی جدید جنگ‌های ترکیبی داده‌محور را در دو دهه اخیر با بهره‌گیری از فناوری‌های هوش مصنوعی توسعه داده است. در برخی از جنگ‌های منطقه‌ای، این الگو پیاده‌سازی و توسعه‌یافته است که اثر بارز آن، از منظر حقوق بشر، نقض مستمر حق حریم خصوصی افراد است.

ب. ایالات متحده آمریکا تحت الگوی جنگ‌های ترکیبی داده‌محور و نقش‌آفرینی «هدایت و کنترل» مؤثر در جنگ‌های اوکراین (ناتو) و روسیه و اسرائیل، ایران، نسبت به نقض حریم خصوصی افراد در کشورهای روسیه و ایران و همچنین متحدین منطقه‌ای آنان، اقدامات گسترده و مستمری را انجام داده است و همچنان ادامه دارد. این الگو در حوزه فرماندهی در هند و اقیانوس آرام، باتوجه‌به جنگ تجاری آمریکا با چین در خصوص فناوری ۵ G(نگرائو و همکاران، ۲۰۲۵) و فناوری‌های هوش مصنوعی در سطح جهانی (لی، ۲۰۲۲) و همچنین فرماندهی آمریکای لاتین و کارائیب، باتوجه‌به تهدیدات نظامی علیه این منطقه، از جمله ونزوئلا

[1] . The Washington Institute for Near East Policy
[2] . The Begin–Sadat Center for Strategic Studies (BESA Center)
[3] . The Jewish Institute for National Security of America (JINSA)
[4] . The Foreign Intelligence Surveillance Act (FISA)

(هوبرمن و آمارال، ۲۰۲۵)، در حال گسترش است. در نتیجه، ما با یک جنگ جهانی نامرئی داده‌محور مواجه هستیم که کشورهای مختلف تحت ائتلاف‌های جهانی درحال توسعه آن هستند (بورچرت، شوتز و وربووزکی، ۲۰۲۵).

ج. بزرگ‌ترین تهدید چنین جنگ داده‌محوری از منظر حقوق بشر، نقض جهانی حق حریم خصوصی افراد در سراسر جهان و نیز بر اساس منشور ملل متحد، تهدید جهانی علیه صلح و امنیت بین‌الملل است؛ چراکه اولاً بهره‌گیری از چنین قدرت محاسباتی جهانی، علیه تمامیت ارضی و استقلال سیاسی کشورهای عضو سازمان ملل متحد است و بر اساس ویژگی‌های کاربردی این فناوری‌ها با تأکید بر جمع‌آوری مستمر داده‌های کلان و پردازش آنها برای اشراف بر کشورها، دخالت در امور داخلی کشورهای یادشده محسوب می‌گردد.

ثانیاً بااطلاع یافتن کشورها و اتباع آنان از چنین تجاوزی به حریم خصوصی خود و همکاری بعضی دولت‌ها با آنان، در وهله اول برخلاف بندهای ۲ و ۳ ماده ۱ منشور، مقاصد ملل متحد ناظر بر توسعه روابط دوستانه بین ملل بر مبنای احترام به اصل خودمختاری ملل و نیز حصول همکاری‌های بین‌المللی در حل مسائلی که دارای جنبه‌های اقتصادی، اجتماعی و فرهنگی یا بشردوستی است، تحت‌تأثیر قرار می‌گیرد و دچار مخاطرات جدی (هرج‌ومرج) داخلی و منطقه‌ای خواهد گردید.

ثالثاً، باتوجه‌به خلأهای حقوقی و ساختاری کنونی و عدم کارآمدی سازمان ملل متحد، برخلاف بند ۴ ماده ۱ منشور ملل متحد، مرکزیت آن برای هماهنگ‌کردن اقداماتی که ملل متحد جهت هدف‌های مشترک معمول می‌دارند، تضعیف می‌گردد و این خود می‌تواند چشم‌اندازی را که در مقدمه منشور ملل متحد ترسیم شده است، در این عصر تیره‌وتار نماید.

نتیجه‌گیری

در این پژوهش، نقش جامعه اطلاعاتی آمریکا در نقض حقوق حریم خصوصی جهانی با بهره‌گیری از فناوری‌های هوش مصنوعی، به رویکرد توصیفی و تحلیلی مورد بررسی قرار گرفت. به طور خاص، برای اثبات چنین رویه‌ای، دو پرونده ترور فرماندهان روسیه و دانشمندان و فرماندهان ایران در تجاوز مسلحانه ۲۳ خرداد ۱۴۰۴ مورد تحلیل قرار گرفت. نتایج این پژوهش نشان داد که اولاً، توسعه و کاربرد فناوری‌های هوش مصنوعی در جامعه اطلاعاتی آمریکا از پیشینه‌ای قریب نیم قرن برخوردار است و به طور خاص، در جنگ‌های داده‌محور و برون‌مرزی نیروهای ویژه آن، قریب دو دهه است که ادامه دارد. ثانیاً، سوابق متعدد عملیات‌های داده‌محور مبتنی بر هوش مصنوعی در منطقه غرب آسیا، به ویژه در چارچوب بخش اول فرضیه دوم، نشان می‌دهد که عملیات مشترک ایالات متحده و اوکراین در اول ماه مه ۲۰۲۲، علیه رئیس ستاد ارتش روسیه و جمعی از افسران ارشد روسیه در شهر ایزیوم خارکیف، نمونه‌ای عینی از این فعالیت‌ها است. هرچند، به دلیل طبقه‌بندی خاص اطلاعاتی و محرمانگی روش‌های پیاده‌سازی آن، تمامی ابعاد این عملیات‌ها فاش نشده است.

همچنین در چارچوب بخش دوم فرضیه دوم و باتوجه‌به اظهارات صریح رئیس‌جمهور آمریکا در ۶ نوامبر ۲۰۲۵، سنتکام به فرماندهی ژنرال اریک کوریلا در هدایت و کنترل جنگ تحمیلی ۱۳ ژوئن ۲۰۲۵ و ترور چندین استاد برجسته دانشگاه، فرماندهان ارشد نظامی و خانواده‌های آنان در اماکن مسکونی و غیرنظامی نقش‌آفرینی نموده است که به دلیل پیشینه جمع‌آوری مستمر داده‌های شخصی افراد یادشده و پردازش مداوم آن‌ها، نقض فاحش حق بر حریم خصوصی است.

نتایج نهایی این پژوهش، بر اساس فرضیه سوم، نشان می‌دهد که ایالات متحده آمریکا به طور مستمر با جمع‌آوری و پردازش داده‌های کلان مربوط به مراکز فرماندهی نظامی، از جمله سنتکام، آگاهانه اقدام به نقض حریم خصوصی اتباع کشورهای عضو سازمان ملل متحد می‌کند. این اقدامات تجاوزکارانه و متخلفانه بین‌المللی، پرونده‌ای مستند و قابل‌استناد در مجامع بین‌المللی و منطقه‌ای برای اثبات نقض گسترده حریم خصوصی است. ادامه چنین اقداماتی می‌تواند منجر به تضعیف نظام حقوق بین‌الملل معاصر و در نتیجه سلب روح همکاری و حسن‌نیت حاکم بر جامعه بین‌المللی گردد. در سال‌های آینده، شاهد تشدید اختلافات سیاسی، تنش‌های امنیتی و نظامی در مناطق مختلف جهان خواهیم بود، و سازمان ملل متحد از مرکزیت هماهنگی و همکاری

بین‌المللی خود تهی خواهد شد. این وضعیت، نظم و امنیت بین‌المللی را متزلزل می‌سازد و در رقابت‌های جدی قدرت‌های جهانی، روابط و مناسبات دوستانه و مسالمت‌آمیز اعضای سازمان ملل آسیب جدی خواهد دید.

این نتایج جدید می‌تواند در توسعه نظریه‌های موجود در حوزه حفاظت از حقوق حریم خصوصی در عصر هوش مصنوعی مؤثر باشد. همچنین، باتوجه‌به محدودیت‌های این پژوهش، پیشنهاد می‌شود در زمینه موضوعاتی مانند تحلیل سیاست‌ها و استراتژی‌های بین‌المللی هوش مصنوعی ایالات متحده آمریکا، تأثیر آن بر رویکردهای جدید سنتکام، و همچنین پیش‌بینی روندهای آینده بر اساس مدل همکاری‌های راهبردی این کشور با رژیم صهیونیستی در دوره زمانی ۲۰۲۲ تا ۲۰۲۵، تحقیقات لازم انجام شود. این تحقیقات باید اثرات امنیتی این سیاست‌ها و همکاری‌ها بر صلح و امنیت منطقه غرب آسیا را مورد بررسی قرار دهند. علاوه بر این، نقش دفاتر منطقه‌ای (غرب آسیا) شرکت‌های خصوصی فراملی و چندملیتی فعال در حوزه هوش مصنوعی در تعمیق حکمرانی جهانی اطلاعات و تأثیر آن بر صلح و امنیت بین‌الملل نیز باید موردمطالعه قرار گیرد. به‌عنوان راهکارهای پیشنهادی، این موضوعات در دو سطح قابل‌بررسی است که می‌تواند به بهبود سیاست‌گذاری‌ها و استراتژی‌های منطقه‌ای و بین‌المللی کمک کند.

سطح داخلی

الف. جمهوری اسلامی ایران، باتوجه‌به اقتضائات عصر هوش مصنوعی و تهدیدات مذکور، نسبت به نوسازی شورای هماهنگی اطلاعات جمهوری اسلامی، تحت یک جامعه اطلاعاتی نوین و حکمرانی مطلوب در حوزه اطلاعات و نظامی، با تأکید بر اصول و ارزش‌های جهانی اسلام، اقدام لازم را انجام دهد.

ب. جمهوری اسلامی ایران، تقویت شبکه ملی اطلاعات و زیرساخت‌های بومی آن در سطح داخلی، با تأکید بر توسعه و کاربرد مدل‌های بومی سیستم‌ها و فناوری‌های هوش مصنوعی، را در دستور کار قرار دهد.

سطح بین‌المللی

الف. جمهوری اسلامی ایران باید همکاری‌های دو و چندجانبه با کشورهای دارای قوانین سخت‌گیرانه در حفاظت از داده‌ها و حریم خصوصی افراد را موردتوجه جدی قرار دهد. این اقدامات می‌تواند نقش مؤثری در کاهش تهدیدات امنیتی و حفظ حریم خصوصی ایفا کند و همچنین نیازهای ارتباطات و تبادلات بین‌المللی را تسهیل نماید.

ب. جمهوری اسلامی ایران باید دررابطه‌با پرونده تجاوز مسلحانه رژیم صهیونیستی و ایالات متحده آمریکا، این پرونده را با ابعاد نقض حقوق بشر و تهدیدهای جدی علیه اهداف منشور سازمان ملل متحد ثبت و اسناد آن را منتشر کند. این اقدام می‌تواند نقش مهمی در آگاهی‌بخشی جهانی و حمایت از حقوق بشر ایفا کند.

ج. جمهوری اسلامی ایران باید با همکاری دیگر کشورهای قربانی، در قالب دیپلماسی فعال رسمی و عمومی، ماهیت نقض حقوق بشر آمریکا در حریم خصوصی اتباع دیگر کشورهای عضو سازمان ملل را افشا کند. همچنین، پیگیری رسمی این پرونده در مجامع بین‌المللی می‌تواند منجر به صدور قطعنامه‌های مؤثر شده و افکار عمومی جهانی را بیدار کند. این اقدامات می‌تواند زمینه‌ساز پیشگیری از بحران‌های فزاینده علیه صلح و امنیت بین‌المللی باشد.

تعارض منافع

بر اساس اظهار نویسندگان این مقاله، تعارض منافع وجود ندارد.

منابع

ابوذری، مهرنوش (۱۴۰۲). **حقوق و هوش مصنوعی**، تهران: نشر میزان.

انصاری، باقری (۱۴۰۱). **حقوق ارتباطات جمعی**، تهران: انتشارات سمت.

دادمهر، هادی (۱۳۹۴). **اعتبارسازی در حقوق بین‌الملل و روابط بین‌الملل**، چاپ اول، تهران: انتشارات مجد.

دشتی، طاهره‌سادات و معتمدنژاد، رویا. (۱۴۰۳)،« جایگاه هوش مصنوعی در قانون‌گذاری اتحادیه اروپا»، علوم خبری، ۱۲(۱)، ۱–۲۰.

ضیایی بیگدلی، محمدرضا (۱۴۰۳). **حقوق بین‌الملل عمومی**، تهران: انتشارات گنج دانش.

شکرالهی، شیوا و معتمدنژاد، رویا.(۱۴۰۳)،« حکمرانی جهانی هوش مصنوعی در خدمت منافع بشریت و نقش سازمان ملل» ، علوم خبری،۱۴(۱)، ۵۰-۷۵.

قربانی، محمد و جواهری، مهدی. (۱۴۰۲)،«**جامعه اطلاعاتی ایالات متحده آمریکا؛ ساختار و کارکردها**»، فصلنامه پژوهش‌های اطلاعاتی و جنایی، ۱۸(۲)، ۱۷۶-۱۴۵.

کیسینجر، هنری، اشمیت، اریک و هوتنلانگر، دانیل (۱۴۰۳). **عصر هوش مصنوعی و آینده انسان**، ترجمه پوریا هامونی، تهران: نشر سروش.

محمودی پرچینی، محمود.، ریاضی، لادن و پورابراهیمی، علیرضا .(۱۴۰۳)،« مقایسه قوانین حفاظت از داده‌های شخصی: مقررات عمومی منحصربه‌فرد تحت مقررات حفاظت از داده‌های عمومی اتحادیه اروپا (GDPR) و قوانین ایالات متحده»، علوم خبری، ۱۳(۴)، ۳۱-۳۵.

میرمحمدی، مهدی. (۱۳۸۶)،«**نومحافظه‌کاران و سیاست‌های اطلاعاتی-امنیتی ایالات متحده آمریکا**»، نشریه سیاست خارجی، ۲۱(۱)، ۹۳-۱۲۶.

میرمحمدی، مهدی. (۱۴۰۲)،« **رهیافت‌های مدیریت جامعه اطلاعاتی**»، نشریه مطالعات راهبردی، ۱۰۰، ۱۵۵-۱۵۹.

ولدرج، مایکل (۱۴۰۰). **هوش مصنوعی**. ترجمه ابوالفضل حقیری قزوینی. تهران: انتشارات تمدن علمی.

References:

Abouzari, M. (2023). Law and artificial intelligence. Mizan Publishing. (in Persian)

Aidun, E. (2025). Data privacy in the digital age: A comparative analysis of U.S. and EU regulations. *University of Cincinnati Law Review*, 93. https://uclawreview.org/2025/03/05/data-privacy-in-the-digital-age-a-comparative-analysis-of-u-s-and-eu-regulations/

Al Jazeera. (2025, November 6). Trump says he was "very much in charge" of Israel's June 13 attack on Iran. https://www.aljazeera.com/news/2025/11/6/trump-says-he-was-very-much-in-charge-of-israels-june-13-attack-on-iran

American Privacy Rights Act of 2024, (2024) (APRA). https://www.govinfo.gov/app/details/BILLS-118hr8818ih

Angerhofer, M. D., Datta, S., Vishwakarma, A. K., Sharma, U. R., Singh, V., & Gautam, P. (2024). Privacy in the age of artificial intelligence: Addressing the ethical and legal implications. *Journal of Informatics Education and Research*, 4(3), 1399–1414. https://jier.org/index.php/journal/article/view/1465

Ansari, B. (2022). Mass communication law. Samt Publications. (in Persian)

Barnes, J. E., Cooper, H., & Schmitt, E. (2022, May 4). U.S. intelligence is helping Ukraine kill Russian generals, officials say. *The New York Times*. https://www.nytimes.com/2022/05/04/us/politics/russia-generals-killed-ukraine.html

Bharati, R. K. (2024). The right to privacy in the age of artificial intelligence: Challenges and legal frameworks. *Dastavej Research Journal*, 54(7), 27–38. https://dastavej.net/volume-54-issue-7/

Bondar, K. (2024). Understanding the military AI ecosystem of Ukraine. *Center for Strategic and International Studies (CSIS)*. https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine

Borchert, H., Schütz, T., & Verbovszky, J. (Eds.). (2025). *The very long game: 25 case studies on the global state of defense AI*. Springer Nature.

Chinmay. (2025). Privacy in the age of artificial intelligence. *NUJS Journal of Regulatory Studies*, 9(4), 71–88. https://journals.nujs.edu/index.php/njrs/article/view/338

Crawford, J. (2002). The ILC's articles on responsibility of states for internationally wrongful acts: A retrospect. *American Journal of International Law*, 96(4), 874–890. http://www.jstor.org/stable/3070683

Dadmehr, H. (2015). Reputations in international law and international relations. Majd Publications. (in Persian)

Dashti, T. S., & Motamednejad, R. (2024). The role of artificial intelligence in EU legislation. *News Science*, 11(3), 1–20. (in Persian)

Dekel, U., & Bar Or, Y. (2021). A breeze of change: Israel joins the US Central Command region. *Institute for National Security Studies (INSS)*, Tel Aviv University. https://www.inss.org.il/publication/centcom/

DLA Piper. (2024). Data protection laws of the world – United States edition. DLA Piper Global Data Protection Team. https://www.dlapiperdataprotection.com/?c=US

Ewbank, J. (2024). The role of artificial intelligence in the U.S. Intelligence Community: Current uses and future developments. Aspen Institute. https://www.aspeninstitute.org/wp-content/uploads/2024/10/Ewbank_Role-of-AI-in-USIC_Final.pdf

Faverio, M. (2023, October 18). Key findings about Americans and data privacy. Pew Research Center. https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/

Goncharuk, V. (2025). Survival of the smartest? Defense AI in Ukraine. In H. Borchert, T. Schütz, & J. Verbovszky (Eds.), The very long game: 25 case studies on the global state of defense AI (pp. 375–395). Springer Nature.

Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., & Scharre, P. (2018). Artificial intelligence and international security. Center for a New American Security (CNAS). https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/CNAS-AI-and-International-Security-July-2018_Final.pdf

Huberman, B., & Amaral, R. A. D. (2025). Hegemony and resistance: US imperial strategies in Latin America. *Journal of Latin American Political Economy*. https://www.tandfonline.com/doi/full/10.1080/19436149.2025.2578046

Ignatius, D. (2022, June 24). How the U.S. helped Ukraine inflict devastating losses on Russia. *The Washington Post*. https://www.washingtonpost.com/opinions/2022/06/24/us-intelligence-assistance-ukraine-russia-war

International Covenant on Civil and Political Rights. (1966). United Nations. https://iran.un.org/en/106018-international-covenant-civil-and-political-rights

Jewish Institute for National Security of America (JINSA). (2022, October 24). How a shift to CENTCOM enabled close U.S.-Israel coordination against Iran. https://jinsa.org/how-a-shift-to-centcom-enabled-close-us-israel-coordination-against-iran/

King, A. (2024). Digital targeting: Artificial intelligence, data, and military intelligence. *Journal of Global Security Studies*, 9(2), 1–16.

Kissinger, H. A., Schmidt, E., & Huttenlocher, D. (2023). The age of AI: And our human future (P. Hamooni, Trans.). Soroush Publishing. (in Persian)

Knights, M. (2021). Moving Israel to CENTCOM: Another step into the light. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/moving-israel-centcom-another-step-light

Lappin, Y. (2021). The US brings Israel into CENTCOM (BESA Center Perspectives Paper No. 1,940). Begin-Sadat Center for Strategic Studies. https://besacenter.org/us-israel-centcom/

Lee, J. (2022). Artificial intelligence and international law. Springer Nature.

Mahmodi Parchini, M., et al. (2025). Comparison of personal data protection laws: Unique general regulations under the European Union's General Data Protection Regulation (GDPR) and United States laws. *News Science*, 13(4), 31–35. (in Persian)

McClain, C., Faverio, M., Anderson, M., & Park, E. (2023, October 18). How Americans view data privacy. Pew Research Center. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Ministry of Foreign Affairs of the Islamic Republic of Iran. (2025). https://mfa.gov.ir/portal/newsview/777763

Mirmohamadi, M. (2007). Neoconservatives and the information security policies of the United States. *The Journal of Foreign Policy*, 21(1), 93–126. (in Persian)

Mirmohamadi, M. (2023). Approaches for managing the intelligence community. *Strategic Studies Quarterly (SSQ),* 100, 155–159. (in Persian)

Moran, C., Burton, J., & Christou, G. (2023). The US Intelligence Community, global security, and AI: From secret intelligence to smart spying. *Journal of Global Security Studies*, 8(2), 1–18.

Negrão, T., Gobbi, M. C., Silva, T. C., & Holouka, G. (2025). The trade war between China and the USA and the geopolitical impacts of the 5G. São Paulo State University. https://www.researchgate.net/publication/388757321_The_Trade_War_Between_China_And_The_USA_And_The_Geopolitical_Impacts_Of_The_5G

Nordic Conference on the Right to Privacy. (1967). Right to privacy seminar report and conclusions. International Commission of Jurists. https://www.icj.org/wp-content/uploads/2013/06/Right-to-privacy-seminar-report-conclusions-1967-eng.pdf

Qhorbani, M., & Javaheri, M. (2023). United States Intelligence Community: Structures and functions. *Journal of Criminal Intelligence Researches*, 18(2), 145–176. (in Persian)

Sfetcu, N. (2024). Artificial intelligence in intelligence agencies, defense and national security. MultiMedia Publishing. https://www.telework.ro/en/e-books/artificial-intelligence-in-intelligence-agencies-defense-and-national-security/

Shokrollahi, S., & Motamednejad, R. (2025). The global governance of artificial intelligence in the service of humanity's interests and the key role of the UN. *News Science*, 14(1), 11–15. (in Persian)

Stone, C. (2021). The integration of artificial intelligence in the Intelligence Community: Necessary steps to scale efforts and speed progress (pp. 1–71). American University Washington College of Law.

The Jakarta Post. (2025, June 26). Mossad chief thanks CIA for help in Iran war. https://www.thejakartapost.com/world/2025/06/26/mossad-chief-thanks-cia-for-help-in-iran-war.html
United Nations. (1945). Charter of the United Nations. https://www.un.org/en/about-us/un-charter/chapter-1
United Nations General Assembly. (2001, December 12). Responsibility of states for internationally wrongful acts (A/RES/56/83). https://undocs.org/en/A/RES/56/83
United Nations International Law Commission. (2001). Articles on responsibility of states for internationally wrongful acts. United Nations Office of Legal Affairs. https://legal.un.org/avl/ha/rsiwa/rsiwa.html
United Nations. (1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights
U.S. Central Command (CENTCOM). (2024). Official image of a regional military exercise. https://www.centcom.mil/MEDIA/IMAGERY/igphoto/2003145032/
U.S. Department of State. (2025, June 12). Statement from Secretary of State Marco Rubio. https://www.whitehouse.gov/briefings-statements/2025/06/statement-from-secretary-of-state-marco-rubio/
Wooldridge, M. (2021). Artificial intelligence (A. Haghighi Qazvini, Trans.). Tamaddon Elmi. (in Persian)
Ziai Bigdeli, M. R. (2024). Public international law. Ganjedanesh Publications. (in Persian).