DOI: 10.22124/jol.2026.29178.2544

Research Article

University of Guilan Iranian association of penal law

Criminal law Research
A Biannual Journal
Vol . 17, No.1, Spring & Summer 2026(Serial 33)

Responding to Threats from Terrorist Activities on Virtual Platforms through AI Governance Capacity

1. Peyman Namamian,
Associate Professor, Law Department, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran (E mail: p-namamian@araku.ac.ir)

Submit Date:2024/12/05	**Accept Date:2026/01/10**

Abstract:
Terrorist crimes on virtual platforms have become a serious threat to security. In this context, the use of artificial intelligence (AI) to identify and address these threats has become a key priority in the field of security. This technology plays an important role in identifying suspicious patterns and analyzing data, but it faces challenges such as privacy protection and accuracy in detection, which require responsible and balanced governance to overcome. Additionally, there are significant gaps in the legal frameworks and oversight mechanisms for AI governance, which need fundamental reforms. These gaps include the misalignment of laws with the rapid pace of technological advancement and the lack of legal frameworks for international cooperation. Therefore, the development of new laws in areas such as human rights, privacy protection, algorithmic transparency, and international collaboration is essential for effectively combating terrorist crimes, ensuring the appropriate use of AI, and safeguarding individual user rights. This paper emphasizes the importance of creating transparent governance structures based on human rights principles in the use of AI technologies and, through documentary and descriptive-analytical methods, analyzes the role of AI governance in identifying, preventing, and reducing terrorist crimes on virtual platforms. It seeks to answer the question "How can AI governance be effective in combating terrorist crimes on virtual platforms?"

Key Words: *Cyberspace, Terrorist Crimes on Virtual Platforms, AI Technology Governance, Prevention, Security on Virtual Platforms*

1. Introduction

In recent years, cyberspace has assumed a critical role in global security and international relations, as the widespread reliance of societies and organizations on modern technologies has transformed the distribution of power and methods of influence. Digital capabilities, based on access to technology and the skillful use of it, have diminished the exclusive authority of traditional power rooted in force, enabling individuals and groups to exert direct influence. These capabilities are exploited not only for peaceful purposes but also by terrorist groups for planning operations, infiltrating information networks, and conducting sabotage, highlighting the growing importance of cybersecurity.

The expansion of the internet and smart technologies has increased economic opportunities and access to services, yet it has simultaneously created a fertile ground for cross-border crimes and terrorist activities. The transnational, anonymous, and technically complex nature of these threats underscores the need to employ intelligent technologies for data analysis, detecting suspicious patterns, and responding rapidly to threats. Responsible use of artificial intelligence, combined with smart governance and proactive policy-making, can serve as an effective tool to counter cyber threats.

2. Methodology

This descriptive-analytical study examines the role of AI governance in preventing and combating cyberterrorism. Data were collected from library and documentary sources and analyzed using a critical and comparative approach. The findings emphasize the effectiveness of AI tools, ethical and legal considerations, regulatory limitations, and the importance of technology governance in managing terrorist threats, providing a framework for the effective use of this technology.

3. Results and Discussion

In recent years, the advancement of emerging technologies, particularly artificial intelligence and digital platforms, has posed complex threats to international security and human rights. Terrorist groups exploit digital tools to promote extremist activities, plan attacks, and evade surveillance. In this context, international cooperation is crucial, and global organizations such as the United Nations and the European Union can, by developing coordinated laws and conventions, both safeguard human rights and provide countries with the tools to counter digital threats. Governance of artificial intelligence should be based on transparency, accountability, and respect for fundamental human rights.

The Global Program to Combat Cyberterrorism (2020) is an example of international efforts to enhance capacities for addressing emerging technological threats. By strengthening critical infrastructure, reinforcing the criminal justice system, and collaborating with the private sector to collect digital evidence, the program enhances member states' abilities to confront digital threats. Furthermore, UN Security Council resolutions oblige countries to cooperate and coordinate to prevent terrorist groups from exploiting digital spaces.

The International Convention on Cybercrime (2010–2024) criminalizes offenses such as unauthorized access, illegal surveillance, data destruction, sexual exploitation of children, and digital money laundering. However, concerns remain regarding extensive governmental powers and insufficient privacy safeguards. Artificial intelligence can play an effective role in detecting and preventing terrorist activities, provided that a balance between security and human rights is maintained. Establishing coordinated frameworks, adhering to ethical principles, and strengthening international cooperation for information sharing are essential for effectively countering the threats posed by emerging technologies.

4. Conclusions

Cyberspace, with its strategic importance in economic, political, and security domains, has become a fertile ground for terrorist activities. These threats include propaganda, recruitment, espionage, and the sabotage of information infrastructures, which are amplified by advanced technologies such as encryption and sophisticated surveillance tools, requiring multi-level and technological countermeasures. Artificial intelligence is both a threat and an opportunity; it can make terrorist tools smarter and automate human tasks, while simultaneously enhancing the capabilities of law enforcement in detecting and preventing cybercrimes. Proposed solutions include training and equipping judicial and security personnel, reforming cyber laws, expanding international cooperation, and leveraging technology in compliance with legal and ethical standards. Effective countering of

digital threats necessitates a comprehensive, multi-sectoral approach based on ethical governance and global standards.

5. Selection of References

Ahmad, Nafees (2024), The Draft UN Cybercrime Convention: A Threat to Human Rights, fair observer, March 23, https://www.fairobserver.com/world-news/the-draft-un-cybercrime-convention-a-threat-to-human-rights/#

Bhushan, Tripti (2024), Artificial Intelligence, Cyberspace and International Law Artificial Intelligence, Cyberspace and International Law, *Indonesian Journal of International Law*, 21(2): 281-314. https://www.doi.org/10.17304/ijil.vol21.2.3

Davis, Aaron L (2021), Artificial Intelligence and the Fight Against International Terrorism, *American Intelligence Journal*, 38(2): 63-73.

Etaki, Abdelghany, et al. (2024). Justifying the Criminalization of Disseminating of Misleading Information in Cyberspace in Light of Criminalization Criteria. *Criminal Law Research*, 15(1), 147–162. https://www.doi.org/10.22124/jol.2024.26338.2436 [In Persian]

Namamian, Peyman (2024). Countering and Preventing Terrorist Crimes in the Virtual Social Networks. *Law of Emerging Technologies*, 5(10): 215–233. https://www.doi.org/10.22133/mtlj.2024.410930.1236 [In Persian]

Namamian, Peyman. (2025). The Scope of Documents of Global and Regional Organizations in Strengthening the Legal Capacity to Deal with Terrorist Crimes. *Criminal Law Research*, 15(2), 173–189. https://www.doi.org/10.22124/jol.2024.26384.2442 [In Persian]

Pournejafi, L., et al. (2023). Filtering the cyberspace as a crime or a way for its prevention? Criminal Law Research, 13(2), 163–187. https://www.doi.org/10.22124/jol.2022.20840.2214 [In Persian]

Wall, C. (2025). The ghost in the machine: Counterterrorism in the age of artificial intelligence. https://www.tandfonline.com/doi/full/10.1080/1057610X.2025.2475850#d1e108

Citation:
Namamian,P (2026), "Responding to Threats from Terrorist Activities on Virtual Platforms through AI Governance Capacity", **Criminal Law Research,** 17(33), pp. 179-192. DOI: 10.22124/jol.2026.29178.2544

DOI: 10.22124/jol.2026.29178.2544

نشریه علمی

پژوهشنامه حقوق کیفری

سال هفدهم، شماره اول، بهار و تابستان ۱۴۰۵، پیاپی ۳۳

مقاله پژوهشی

صفحات مقاله: ۱۷۹-۱۹۲

واکنش به تهدیدهای ناشی از ارتکاب جرایم تروریستی در سکوهای مجازی با بهره‌گیری از ظرفیت حکمرانی هوش مصنوعی

پیمان نمامیان

دانشیار گروه حقوق، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران

✉ p-namamian@araku.ac.ir

تاریخ ارسال: ۱۴۰۳ /۰۹/۱۵	تاریخ پذیرش : ۱۴۰۴/۱۰/۲۰

چکیده:

جرایم تروریستی در سکوهای مجازی به یک تهدید جدی برای امنیت تبدیل شده است. در این راستا، به‌کارگیری هوش مصنوعی برای شناسایی و مقابله با این تهدیدات به یکی از اولویت‌های کلیدی در حوزه امنیت تبدیل گشته است. این فناوری با توانمندی در شناسایی الگوهای مشکوک و تحلیل داده‌ها نقش مهمی ایفا می‌کند، ولی با چالش‌هایی نظیر حفظ حریم خصوصی و دقت در شناسایی مواجه است که برای رفع آن‌ها نیازمند حکمرانی مسئولانه و متوازن می‌باشد. همچنین، در زمینه حکمرانی هوش مصنوعی، کمبودهای قابل توجهی در قوانین و نظارت‌ها وجود دارد که نیازمند اصلاحات اساسی است. این کمبودها شامل عدم هم‌راستایی قوانین با سرعت پیشرفت فناوری و فقدان چارچوب‌های قانونی برای همکاری‌های بین‌المللی می‌باشد. بنابراین، تدوین قوانین جدید در حوزه حقوق بشر، حفظ حریم خصوصی، شفافیت الگوریتم‌ها و تعاملات بین‌المللی برای مقابله مؤثر با جرایم تروریستی ضروری به نظر می‌رسد، به‌طوری‌که هم از بهره‌برداری مناسب از هوش مصنوعی حمایت کند و هم حقوق فردی کاربران حفظ گردد.

واژگان کلیدی: سکوهای مجازی، جرایم تروریستی در سکوهای مجازی، حکمرانی هوش مصنوعی، پیشگیری، امنیت در سکوهای مجازی.

مقدمه

فضای مجازی در نظام بین‌المللی از اهمیت قابل ملاحظه‌ای برخوردار شده است، زیرا ماهیت آن سامانه را پس از اتکای فزاینده به فناوری تحت‌تأثیر قرار می‌دهد. علاوه بر این، از طریق ظهور نوع جدیدی از قدرت، که قدرت الکترونیکی است، به پایان دادن به انحصار قدرت به معنای سنتی قدرت سخت کمک کرد. علاوه بر این، این قدرت در اختیار هر شخصی قرار گرفته است که از دانش فناورانه برخوردار بوده و توانایی بهره‌گیری از آن را برای تحقق اهداف خود داردبا این حال، نه‌تنها به صورت مسالمت‌آمیز، بلکه توسط گروه‌های تروریستی برای انجام حملات خود استفاده می‌شود. علاوه بر این، توسط افراد و بازیگران غیردولتی برای نفوذ به شبکه‌های اطلاعاتی یا جاسوسی و سایر اهداف توهین آمیز استفاده می‌شود. [۱] با توجه به اینکه دیجیتالی شدن یک پدیدهٔ جهانی است، امنیت در سکوهای مجازی نقش مهمی در سطح بین‌المللی ایفا می‌کند و تراکنش‌های ایمن را بین بازیگران مختلف تضمین می‌کند.[۲] به این ترتیب، هوش مصنوعی ممکن است به تروریست‌ها و سایر گروه‌ها در توسعهٔ جرایم تروریستی[۳] در سکوهای مجازی پیچیده‌تر و خطرناک‌تر کمک کند، که احتمالاً پیامدهای جهانی را به همراه دارد(Nikolic, 2024: 1).

جرایم تروریستی در سکوهای مجازی با توسعه جامعه تکامل می یابد و خطرناک‌تر از جرایم معمولی می‌شود. به خصوص با گسترش فناوری مدرن و وابستگی روزافزون جهان به رایانه و اینترنت، تروریست تنها به رایانه نیاز دارد و ارتباط خود را با شرکت اینترنتی برای انجام اقدامات تروریستی ایمن می‌کند. از اینرو، روش مدیریت جرایم تروریستی پیچیده تر شده است؛ زیرا گروه های تروریستی از فضای مجازی برای انجام حملات با استفاده از اینترنت و برنامه‌های پیچیده استفاده می‌کنند. بنابراین، جرایم تروریستی از سنتی مبتنی بر قدرت سخت به جرایم تروریستی در سکوهای مجازی مبتنی بر قدرت نرم تبدیل شده است.[۴] بر این اساس، در چارچوب تعریف جرایم تروریستی ارتکابی در سکوهای مجازی اذعان می‌شود این دسته از جرایم از طریق اینترنت و فضای مجازی به‌منظور ترویج یا ارتکاب فعالیت‌های تروریستی ارتکاب می‌یابند که به‌طور معمول مشتمل بر بهره‌گیری از سکوهای برخط برای تبلیغ اندیشه‌های تروریستی، جذب و آموزش اعضای جدید، برنامه‌ریزی و هماهنگی عملیات تروریستی، و حمله به اهداف خاص از طریق فناوری‌های دیجیتال است. این نوع جرایم اغلب از طریق وب‌گاه‌ها و شبکه‌های اجتماعی، ارتکاب می‌یابند(Namamian, 2024: 221).

هوش مصنوعی به بخشی جدایی‌ناپذیر از دنیای مدرن تبدیل شده است و در ابعاد گوناگون حیات بشر مانند مراقبت‌های بهداشتی، مالی، حمل و نقل و سرگرمی نفوذ کرده است. در حوزه فضای مجازی، هوش مصنوعی نقشی محوری در افزایش امنیت سکوهای مجازی، خودکارسازی وظایف و بهینه سازی فرآیندهای تصمیم گیری ایفا می‌کند(Ashley, 2017: 171). با این حال، هم‌چون هر پیشرفت فناوری‌ها، قابلیت کاربرد هوش مصنوعی در زمینه فضای مجازی با مجموعه‌ای از محدودیت‌ها و چالش‌های خاص خود همراه است. هوش مصنوعی با ارائه ابزارهای پیشرفته برای شناسایی، پیشگیری و کاهش تهدیدهای موجود در سکوها، امنیت را متحول کرده است(Marra and McNeil, 2013: 1140).

---

۱. امروزه هوش مصنوعی در کالبد ربات های ساخت بشر دمیده شده و نقش ربات ها با کاربردهای مختلف نظامی، درمانی و غیره در زندگی انسان‌ها رو به افزایش است. همین مسئله سبب شده تا مسائل و مشکلاتی در حوزه حقوق کیفری کشورها به‌وجود آید(Atazadeh & Ansari, 2019: 55).

۲. با توجه به ماهیت فراملیتی حکمرانی و توسعه هوش مصنوعی و تأثیری که دارد، باید یک واکنش قوی‌تر و نهادی در سطح جهانی وجود داشته باشد که توسعه آن را تنظیم کرده و از دست سازمان‌های تروریستی دور نگه دارد. در نهایت، ظرفیت حکمرانی هوش مصنوعی برای ایجاد بی‌ثباتی و تخریب بسیار زیاد است و نیاز به تنظیم بهتر آن در سطح ملی و بین‌المللی وجود دارد.

۳ .جرایم تروریستی تهدیدی جدی برای امنیت و جان مردم محسوب می‌شوند و مقابله با آن‌ها چالش‌های امنیتی گسترده‌ای ایجاد می‌کند. اقدامات و مقررات ضدتروریستی، گرچه ضروری هستند، می‌توانند محدودیت‌هایی بر حقوق بنیادین افراد و جامعه تحمیل کنند. سازمان‌های بین‌المللی و منطقه‌ای با ایجاد فضای گفت‌وگو و تبادل اطلاعات، نقش اساسی در هماهنگی و هم‌گرایی دیدگاه دولت‌ها دارند و به آن‌ها کمک می‌کنند تا با درک متقابل، استفاده مؤثرتری از ابزارهای مقابله با تروریسم داشته باشند(Namamian, 2025: 173).

۴. با گسترش استفاده از رایانه و اینترنت در زندگی روزمره، جرایم مرتبط با فضای مجازی نیز افزایش یافته‌اند. این امر نشان‌دهنده اهمیت تطبیق قوانین و مقررات حقوقی با تکنولوژی و واقعیت‌های جدید است. همین امر ممکن است باعث چالش‌های حقوقی شود(Kaveh & Barani, 2024: 51).

در مدت کمی بیش از دو دهه، رشد سریع اینترنت و فناوری‌های اطلاعاتی و ارتباطی باعث رشد اقتصادی و گسترش دسترسی به خدمات حیاتی شده است. با این حال، فرصت های جدیدی برای فعالیت‌های مجرمانه نیز ایجاد کرد. از آنجایی که مجرمان به ذینفعان ناخواسته فناوری جدید و جهانی شدن تبدیل شده اند؛ زیرا این تحولات آنها را قادر می‌سازد تا با بهره برداری از فعالیت های فراملی مرتکب جنایات شده و از آن سود ببرند و همچنین فعالیت‌ها و اقدامات غیرقانونی خود را از طریق سکوهای مجازی به گونه ای گسترش دهند که ارتکاب جرم توسط تروریست‌ها کاهش یابد. از سوی دیگر، فناوری‌های کنونی فرصت‌های جدیدی را برای اجرای قانون، تحقیقات جنایی و تعقیب کیفری و مبارزه با جرایم تروریستی در سکوهای مجازی ارائه می‌کند تا امنیت عمومی را بهبود بخشد و آژانس‌های مجری قانون و عدالت کیفری را قادر به پیشگیری و مبارزه با جرایم از طریق فن‌آوری کنند. پیشرفت و فناوری و همچنین هوش مصنوعی که تأثیر مثبتی در پیشگیری یا مقابله با این جرایم دارد(Kumar Saini, 2023: 28-29).

همگرایی جرایم تروریستی و فضای مجازی، مفهوم صریح جرایم تروریستی در سکوهای مجازی را به وجود آورده است. پیش‌بینی می‌شود که این پدیده هشداردهنده‌ترین تحول جنایی در سال‌های آتی باشد، با ظرفیت سوءاستفاده تروریست‌ها از اینترنت برای مقاصد مخرب و در نتیجه عواقب شدیدتری در مقایسه با روش‌های سنتی(Davis, 2021: 68). از این‌رو، در چارچوب تقویت همکاری بین‌المللی علیه تروریست‌ها، اگرچه تروریست‌ها در دستکاری اینترنت و سایر فناوری‌های نوین مهارت پیدا کرده‌اند، حکمرانی هوش مصنوعی ابزار قدرتمندی در مبارزه با آن‌ها است.[1] بنابراین، سیاست ضدتروریستی بین حفظ امنیت یک جمعیت و احترام به حقوق فردی برای حفظ حریم خصوصی و آزادی‌هایی مانند آزادی بیان، انجمن و مذهب تعادل ایجاد می‌کند (Brokenshire, 2013: 1). تحولات فناوری‌های نوین می‌تواند اجرای این سیاست‌ها را با وادار کردن مقامات به بررسی مجدد نحوه مبارزه با جرایم تروریستی به چالش بکشد. اقدامات انجام می‌شود (Cornish, 2010: 888). هوش مصنوعی یکی از این فناوری‌ها است.[2]

با توجه به سطرهای بالا، هدف اصلی این مطالعه، بررسی نحوه بهره‌گیری از فنون و سازوکارهای فنی موجود در فناوری هوش مصنوعی در مقابله با جرایم تروریستی در سکوی مجازی است. این پژوهش با استفاده از روش توصیفی-تحلیلی و گردآوری داده‌ها از طریق بررسی نتایج مطالعات و تقریرات موجود، به این پرسش که «حکمرانی هوش مصنوعی چه ظرفیت‌هایی را برای مقابله با جرایم تروریستی در سکوی مجازی فراهم کرده است؟» خواهد داد.

۱. ویژگی‌ها و چالش‌های جرایم تروریستی در سکوهای مجازی

جرایم تروریستی در سکوهای مجازی به چالش‌های پیچیده‌ای در حوزه‌های حقوقی و امنیتی تبدیل شده‌اند. ویژگی‌های این جرایم، از جمله فرامرزی بودن، تهدیدات جهانی و استفاده از فناوری‌های دیجیتال، ضرورت اتخاذ راهکارهای نوین حقوقی و نظارتی را ایجاب می‌کند که در این راستا حکمرانی هوش مصنوعی می‌تواند نقشی کلیدی ایفا نماید. این جرایم به دلیل عبور از محدودیت‌های جغرافیایی و استفاده از اینترنت، پیچیدگی‌هایی در تعقیب قانونی ایجاد می‌کنند. حکمرانی هوش مصنوعی با تحلیل داده‌ها و شناسایی الگوهای مشکوک می‌تواند به تسهیل نظارت بین‌المللی و مقابله با این تهدیدات کمک کند. این تهدیدات نه‌تنها امنیت ملی کشورها را تهدید می‌کنند، بلکه به‌طور جهانی شامل تبلیغ خشونت، انتشار اطلاعات گمراه‌کننده (Etaki, et al, 2024: 154-156) و حملات سایبری نیز می‌شود.

---

1. https://operationalsupport.un.org/en/new-technologies-artificial-intelligence-aid-fight-against-global-terrorism

۲ . مفهوم استفاده از فناوری‌های پیش‌بینی دقیق مبتنی بر هوش مصنوعی برای مقاصد ضد جرایم تروریستی، حدس و گمان است اما امکان‌پذیر است. در نظر گرفتن احتمالات و هزینه‌های چنین رویکردی و چگونگی تنظیم این حوزه نوپا از قبل مفید است (Monaco, 2017: 25). لذا یکی از اقداماتی که می‌توان از هوش مصنوعی برای دفع تروریسم استفاده کرد، «پیش‌بینی رفتار افراد» از طریق ارائه داده‌ها به نرم‌افزارهای هوش مصنوعی است تا با تحلیل اطلاعات افراد که برگرفته از فضای مجازی و حقیقی است، بتواند رفتارهای احتمالی آنها در راستای اعمال تروریستی را پیش‌بینی نماید و از پیشروی بیشتر آن پیشگیری کند. همچنان که کنترل ارتباط‌گیری‌ها و کشف روابط شاخه‌های شبکه تروریستی در فضاهای ارتباطی مجازی است که می‌تواند نقشه تروریست‌ها در اعمال جنایی خنثی کرد.

هوش مصـــنوعی، از طریق تجزیه و تحلیل داده‌های کلان و شـــناســـایی تهدیدات در زمان واقعی، ابزار مؤثری برای مقابله با این تهدیدات و پیشـگیری از تأثیرات منفی بر امنیت ملی به‌شـمار می‌رود. اسـتفاده از این فناوری می‌تواند به‌طور چشـمگیری سـرعت پاسخ‌دهی به حملات سایبری و محتوای تروریستی را افزایش داده و از گسترش تهدیدات پیشگیری کند.

ویژگی دیگر جرایم تروریسـتی در سـکوهای مجازی، اسـتفاده گسـترده از فناوری‌های دیجیتال، از جمله شـبکه‌های اجتماعی، وب‌سایت‌ها و سکوهای برخط برای برنامه‌ریزی، جذب نیرو و تأمین مالی است.[1] از آنجا که این اقدامات اغلب به‌صورت ناشناس و با ابزارهای پیچیده انجام می‌شود، شناسایی و پیگیری این جرایم نیازمند ابزارهای نوین نظارتی و امنیتی است. در این راستا، حکمرانی هوش مصنوعی می‌تواند با به‌کارگیری الگوریتم‌های پیشرفته برای شناسایی رفتارهای مشکوک، شفاف‌سازی فرآیندها و مقابله با نقض حقوق بشر و آزادی‌های فردی در کنار حفظ امنیت، ایفای نقش کند.

یکی از چالش‌های اصـلی مقابله با جرایم تروریسـتی در سـکوهای مجازی، ضـرورت همکاری بین‌المللی اسـت. حکمرانی هوش مصنوعی می‌تواند این همکاری‌ها را تسهیل کرده و با تحلیل داده‌ها، شفاف‌سازی و ارائه اطلاعات به کشورهای مختلف، راهکارهای مؤثری برای پیشـــگیری و مقابله با جرایم ارائه دهد. تدوین معاهدات بین‌المللی و ایجاد چارچوب‌های قانونی هماهنگ در ســـطح جهانی باید هم‌زمان با حفاظت از حقوق فردی و مقابله با تهدیدات دیجیتال انجام شـــود تا امنیت و عدالت حفظ گردد. برای مقابله مؤثر با جرایم تروریستی در سکوهای مجازی، اصلاح و بروزرسانی قوانین در زمینه حقوق بشر، حریم خصوصی و شفافیت الگوریتم‌ها ضـروری اسـت. حکمرانی هوش مصـنوعی باید به‌گونه‌ای باشـد که اسـتفاده از این فناوری‌ها برای شـناسـایی و پیشـگیری از جرایم تروریستی به‌طور مؤثر و مسئولانه صورت گیرد، بدون آنکه موجب نقض حقوق فردی و آزادی‌های مدنی گردد. ویژگی‌های فرامرزی، تهدیدات جهانی و اســـتفاده از فناوری‌های دیجیتال در جرایم تروریســـتی ســـکوهای مجازی، نیاز به حکمرانی هوش مصـــنوعی را به‌عنوان یک ابزار کلیدی برای مقابله با این جرایم ایجاب می‌کند.[2] به منظور پاســـخ‌گویی مؤثر به این تهدیدات، باید ســـاختارهای حقوقی و نظارتی جدید و هماهنگ در سـطح بین‌المللی ایجاد شـوند که هم تهدیدات امنیتی را پوشـش دهند و هم حقوق فردی و آزادی‌های بشـــری را حفظ کننـد. حکمرانی هوش مصـــنوعی می‌توانـد نقش حیـاتی در تحقق این اهـداف ایفـا کرده و از طریق شفاف‌سازی و نظارت هوشمندانه بر فضای مجازی، به مقابله با این نوع جرایم کمک کند.[3]

۲. تأثیر جهانی‌شدن و فناوری هوش مصنوعی در پاسخ به چالش‌ها

جهانی شدن به جرایم تروریستی بین المللی سرعت بخشیده است. پیشرفت‌های فناوری به قدرت تحرک تروریست‌ها کمک کرده و ارتباط آنها را با یکدیگر هم در داخل و هم در خارج بسیار آسان ساخته، به طوری که در این میان هدف برخی گروه های تروریستی حتی تغییر نظم بین المللی و ایجاد نظم جدید تعریف شده است. فرایند جهانی شدن حمایت از جرایم تروریستی را گسترش داده است. با توجه به اینکه جهانی شدن پیامدهای منفی به همراه دارد و باعث به حاشیه راندن برخی گروه ها و نابرابری های اجتماعی و اقتصادی جهانی می‌شود، جرایم تروریسـتی حمایت بیشـتری از سـوی بسـیاری از مردم به حاشـیه رانده شـده در ملت‌های متعدد کسب کرده است .

تحولات فناوری هوش مصـنوعی در مقابله با جرایم تروریسـتی در سـکوهای مجازی به یکی از ابزارهای کلیدی در امنیت سـایبری تبدیل شده است. این فناوری‌ها توانایی شناسایی و فیلتر کردن محتوای تروریستی مانند ویدئوها، تصاویر و متون افراطی را دارند.[4]

---

1 https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/transparency-reporting-on-terrorist-and-violent-extremist-content-online_3f72a170/901cb8cf-en.pdf

2. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_natioal_ct_policy_responses_web.pdf

3 .https://parispeaceforum.org/app/uploads/2025/02/forging-global-cooperation-on-ai-risks-cyber-policy-as-a-governance-blueprint.pdf

4 https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf

به‌دیگر تعبیر، هوش مصنوعی با بهره‌گیری از پردازش زبان طبیعی[1] و شبکه‌های عصبی عمیق[2]، در شناسایی و فیلتر کردن محتوای تروریستی در سکوهای برخط، به‌ویژه شبکه‌های اجتماعی، پیشرفت‌های چشمگیری داشته است. این فناوری‌ها به‌طور خودکار قادرند پیام‌ها، تصاویر و ویدیوهایی که محتوای تروریستی یا تحریک به خشونت دارند را شناسایی کرده و از انتشار آن‌ها پیشگیری کنند.[3] فیس‌بوک با بهره‌گیری از الگوریتم‌های پردازش زبان طبیعی و شبکه‌های عصبی، توانسته است محتوای تروریستی را پیش از گزارش کاربران شناسایی و حذف کند. یوتیوب نیز با ترکیب پردازش زبان طبیعی و یادگیری عمیق، ویدیوهای تروریستی را شناسایی کرده و در سال ۲۰۱۷ اعلام کرد که بیش از ۹۳٪ از این ویدیوها را پیش از گزارش کاربران حذف کرده است.[4] توییتردر سال ۲۰۱۹ با استفاده از الگوهای پیشرفته پردازش زبان طبیعی توانسته است بیش از ۵۰٪ از حساب‌های کاربری تروریستی را پیش از گزارش کاربران شناسایی کند.[5] با این حال، چالش‌هایی نظیر حفظ حریم خصوصی و نیاز به تطابق سریع با تغییرات الگوریتم‌های تروریست‌ها همچنان وجود دارد.

یکی از چالش‌های عمده در مبارزه با تروریسم دیجیتال، نظارت و رصد اطلاعات در سطح جهانی است. سامانه‌های هوش مصنوعی قادرند حجم عظیم داده‌ها را از منابع مختلف مانند چت‌ها، ایمیل‌ها و ویدئوها تجزیه و تحلیل کرده و تهدیدات امنیتی را شناسایی کنند. این توانایی می‌تواند در زمان‌های حساس واکنش سریع به بحران‌ها را تسریع کند. همچنین، در مواجهه با حملات سایبری از سوی گروه‌های تروریستی، هوش مصنوعی می‌تواند الگوهای حملات را شناسایی و اقدامات پیشگیرانه را به‌طور خودکار انجام دهد. با این حال، استفاده از این فناوری‌ها در نظارت برخط ممکن است چالش‌هایی در زمینه حریم خصوصی و حقوق فردی ایجاد کند که نیازمند توازن دقیق میان امنیت و حفظ حقوق بشر است. برای پیشگیری از نقض آزادی‌های فردی، حکمرانی هوش مصنوعی باید بر اساس قوانین و مقررات شفاف و متوازن باشد که هم امنیت و هم حقوق بشر را حفظ کند. یکی از چالش‌های مهم، احتمال خطا در شناسایی تهدیدات توسط سامانه‌های هوش مصنوعی است که ممکن است منجر به شناسایی اشتباه محتوای غیرمجرم به‌عنوان تهدید شود. همچنین، گروه‌های تروریستی ممکن است از تکنیک‌های ضد هوش مصنوعی برای فریب دادن سامانه‌ها استفاده کنند، که نیازمند توسعه فناوری‌های مقاوم و روزآمد است (Syllaidopoulos, Ntalianis & Salmon, 2025: 54).

تحولات فناوری هوش مصنوعی در مقابله با تروریسم دیجیتال ظرفیت زیادی دارد، اما برای استفاده مؤثر از آن، لازم است که هماهنگی دقیقی میان دولت‌ها، بخش خصوصی و نهادهای حقوق بشری وجود داشته باشد. نظارت مستمر و ایجاد قوانین و چارچوب‌های اخلاقی برای پیشگیری از سوءاستفاده از این فناوری‌ها ضروری است تا بتوان از ظرفیت‌های هوش مصنوعی به‌طور مسئولانه و مؤثر بهره‌برداری کرد.[6] در ضمن، این تحولات در حوزه هوش مصنوعی، ظرفیت‌های چشم‌گیری برای مقابله با جرایم تروریستی در سکوهای مجازی ایجاد کرده است. با این حال، استفاده مؤثر و مسئولانه از این ظرفیت‌ها نیازمند حکمرانی چندلایه، رعایت اصول اخلاقی، و همکاری‌های جهانی است. آینده مقابله با جرایم تروریستی در سکوهای مجازی، در گرو تلفیق نوآوری فناورانه با اصول حقوق بشری و سیاست‌گذاری هوشمند خواهد بود. با این حال، برای بهره‌برداری بهینه از این فناوری، نیازمند حکمرانی صحیح، رعایت اصول اخلاقی و توجه به چالش‌های حقوقی و امنیتی هستیم تا از سوءاستفاده‌های احتمالی پیشگیری شود و در عین حال از کارآمدی آن در مبارزه با تهدیدهای تروریستی بهره‌برداری کامل انجام شود.(Wall, 2025: 1)

1 .Natural Language Processing (NLP)
2 .Deep Neural Networks (Deep Learning)
3 .https://www.chathamhouse.org/sites/default/files/2019-08-07-AICounterterrorism.pdf
4 .https://www.wired.com/story/google-youtube-ai-extremist-content/
5 .https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf
۶ . دولت‌ها برای پیشگیری از جرایم سایبری به پالایش متوسل می‌شوند، اما محدودیت‌های فنی و اجرایی اغلب مانع تحقق اهداف می‌شود و حقوق شهروندان را تهدید می‌کند. بی‌توجهی به ضرورت و تناسب، مداخلات دولت را افزایش داده و آسیب‌های ناشی از پالایش نادرست، حتی بدون جرم‌انگاری قانونی، می‌تواند نمونه‌ای از جرم دولتی باشد(Pournejafi, et al, 2023: 163).

هماهنگ کردن تلاش‌ها در سطوح بین‌المللی و منطقه‌ای برای مبارزه با جرایم تروریستی در همه اشکال و مظاهر آن در اینترنت و استفاده از اینترنت به‌عنوان ابزاری برای مقابله با گسترش جرایم تروریستی. درعین‌حال، استراتژی تشخیص می‌دهد که کشورهای عضو ممکن است برای انجام این تعهدات به کمک نیاز داشته باشند.[1]

۳. همکاری بین‌المللی و ابعاد حقوقی مقابله با جرایم تروریستی در سکوهای مجازی؛ از تهدیدات فناوری‌های نوین تا حکمرانی هوش مصنوعی در سکوهای مجازی

با پیشرفت فناوری اطلاعات و ارتباطات، به‌ویژه هوش مصنوعی، تهدیدات تروریستی به فضای مجازی گسترش یافته و گروه‌های تروریستی از سکوهای مجازی برای ترویج افراطی‌گری و برنامه‌ریزی حملات استفاده می‌کنند. علاوه بر این، گروه‌های تروریستی می‌توانند از فنون ضد هوش مصنوعی برای فریب سامانه‌ها بهره‌برداری کنند.

سازمان‌های بین‌المللی مانند سازمان ملل متحد و اتحادیه اروپا می‌توانند در تدوین قوانین و کنوانسیون‌های مشترک برای مقابله با تروریسم در فضای مجازی نقش ایفا کنند. این کنوانسیون‌ها باید از حقوق بشر محافظت کرده و ابزارهای لازم برای مقابله با تروریسم را در اختیار کشورها قرار دهند. حکمرانی هوش مصنوعی باید بر اساس اصول حقوق بشر و آزادی‌های اساسی باشد و نظارت‌ها باید شفاف و محدود به موارد ضروری باشند.

۱.۳. تقویت ظرفیت‌های بین‌المللی و همکاری جهانی در قبال تهدیدات فناوری‌های نوین ناشی از جرایم تروریستی

برنامه جهانی مبارزه با جرایم تروریستی در سکوهای مجازی و فناوری‌های نوین در آوریل ۲۰۲۰ تصویب شد و پشتیبانی ظرفیت‌سازی را برای کشورهای عضو، سازمان‌های بین‌المللی و منطقه‌ای برای توسعه و اجرای پاسخ‌های مؤثر به چالش‌ها و فرصت‌هایی که اینترنت و سایر فناوری‌های اطلاعات و ارتباطات درآن موجود است، ارائه می‌کند. از اینرو، برنامه جهانی از تعهد راهبردی سازمان ملل متحد به جهانی بدون جرایم تروریستی از طریق، «توسعه دانش و افزایش آگاهی از چالش‌ها و فرصت های مرتبط با فناوری های جدید در جرایم تروریستی»، «تقویت مهارت ها و ظرفیت های مورد نیاز برای توسعه و اجرای پاسخ های مؤثر سیاست ملی ضد جرایم تروریستی به چالش‌ها و فرصت های فناوری های جدید»، «تقویت مهارت ها و ظرفیت های مورد نیاز برای حفاظت از زیرساخت‌های حیاتی در برابر جرایم تروریستی در سکوهای مجازی» و «افزایش ظرفیت‌های عدالت کیفری برای مقابله و بررسی بهره‌گیری تروریستی از فناوری‌های نوین»، قابل اجراست.[2]

قطعنامه‌های ۲۱۷۸ (۲۰۱۴) و ۲۳۹۶ (۲۰۱۷) شورای امنیت از کشورهای عضو می‌خواهد هنگام اتخاذ تدابیر ملی برای پیشگیری نسبت به بهره‌گیری تروریست‌ها از فناوری و ارتباطات برای ارتکاب جرایم تروریستی در سکوهای مجازی، همکاری کنند.[3] قطعنامه ۲۳۹۶ (۲۰۱۷) همچنین کشورهای عضو را تشویق می‌کند تا همکاری با بخش خصوصی، به‌ویژه با شرکت‌های فناوری ارتباطات اطلاعات، در جمع‌آوری داده‌های مجازی و شواهد در پرونده‌های مربوط به جرایم تروریستی را افزایش دهند.[4]

افزون بر این، هشتمین بررسی راهبرد جهانی ضد جرایم تروریستی سازمان ملل متحد در خصوص بهره‌گیری بالقوه از فناوری‌های نوین و نوظهور برای اهداف تروریستی ابراز نگرانی می‌کند[5] و در این راستا از همه کشورهای عضو می‌خواهد که اقدامات بیشتری را برای مقابله با استفاده از چنین فناوری‌هایی در نظر بگیرند.

---

1. https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence
2 .https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity
3 .https://main.un.org/securitycouncil/en/s/res/2178-%282014%29
4. https://main.un.org/securitycouncil/en/content/sres23962017

۵ . هوش مصنوعی به فناوری قابل توجهی تبدیل شده است که بخش های گوناگونی از جمله فضای مجازی را متحول کرده است. همانطور که حکمرانی هوش مصنوعی به پیشرفت خود ادامه می دهد، چالش های پیچیده ای را برای چارچوب های حقوقی بین المللی موجود حاکم بر فضای مجازی ایجاد می‌کند.

از کشورهای عضو خواسته می‌شود تا با هم و با سایر ذینفعان مربوطه از جمله دانشگاه، بخش خصوصی و جامعه مدنی همکاری کنند تا اطمینان حاصل کنند که تروریست‌ها پناهگاه امن برخط پیدا نمی کنند و در عین حال اینترنت باز، قابل همکاری، قابل اعتماد و ایمن را ترویج می کنند که کارایی و نوآوری را تقویت می‌کند.[۱]

در ضمن، در راهبرد جهانی مبارزه با تروریسم سازمان ملل متحد[۲]، کشورهای عضو تصمیم گرفتند با توجه به محرمانه بودن، احترام به حقوق بشر و با رعایت سایر تعهدات تحت حقوق بین‌المللی، با سازمان ملل متحد همکاری کنند تا راه‌هایی را بررسی کنند.[۳] هماهنگی در تشریک مساعی بین‌المللی و منطقه‌ای برای مبارزه با جرایم تروریستی در کلیه اشکال و مظاهر آن در فضای مجازی و استفاده از اینترنت به‌عنوان ابزاری برای مقابله با گسترش جرایم تروریستی در سکوهای مجازی امکان رویارویی مؤثر را فراهم می‌آورد. در عین حال، راهبرد تشخیص می‌دهد که کشورهای عضو ممکن است برای انجام این تعهدات به کمک نیاز داشته باشند.[۴]

«برنامه جهانی مبارزه با تروریسم راجع‌به امنیت مجازی و فناوری‌های نوین»[۵] در آوریل ۲۰۲۰ با هدف ارتقای ظرفیت‌های کشورهای عضو، سازمان های بین‌المللی و منطقه ای و نهادهای سازمان ملل متحد برای افزایش آگاهی در مورد تهدید ناشی از جرایم تروریستی در سکوهای مجازی و ارتقای ظرفیت‌های فنی مورد نیاز برای پیشگیری به تصویب رسید. کاهش و پاسخگویی به گروه‌های تروریستی و تندرو خشونت‌آمیز که از فناوری‌های نوین نظیر اینترنت و هوش مصنوعی سوء استفاده می‌کنند.[6] این برنامه همچنین قصد دارد با جمع‌آوری شواهد پزشکی قانونی دیجیتال و از طریق استفاده از فناوری‌های نوین، ظرفیت‌های کشورهای عضو را برای سنجش و رویارویی با جرایم تروریستی در سکوهای مجازی افزایش دهد.[۷]

لازم به‌ذکر است در پایان اکتبر ۲۰۲۲، کمیته مبارزه با تروریسم شورای امنیت سازمان ملل متحد به اتفاق آرا اعلامیه دهلی را به تصویب رساند و کشورهای عضو را متعهد به پیشگیری و مبارزه با اشکال جرایم تروریستی در سکوهای مجازی، به‌ویژه با استفاده از هواپیماهای بدون سرنشین، رسانه‌های اجتماعی، و تأمین مالی جرایم تروریستی برخط[۸] کرد.[۹]

۲.۳.چالش‌ها و ابعاد حقوقی کنوانسیون سازمان ملل متحد علیه جرایم سایبری؛ امنیت، حریم خصوصی و تهدیدات حقوق بشری در سکوهای مجازی

1. https://www.stimson.org/2024/un-security-council-cyber-threats-to-international-security/

2 .A/RES/60/288

3. https://documents.un.org/doc/undoc/gen/n05/504/88/pdf/n0550488.pdf

4 .https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence

5. Global Counter Terrorism Programme on Cybersecurity and New Technologies; https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/mya_project_itemid_27.pdf

۶. این برنامه از راهبرد جهانی ضد جرایم تروریستی با رویکرد پیشگیری و مبارزه با جرایم تروریستی حمایت می‌کند. بر این اساس، برنامه جهانی از تعهد راهبردی سازمان ملل به جهانی بدون جرم تروریستی از طریق« ایجاد درک جمعی در مورد تهدید کاربردهای مخرب از فناوری‌های نوین توسط تروریست‌ها»، «بهبود قابلیت های ملی برای حفاظت از زیرساخت‌های حیاتی در برابر جرایم تروریستی در سکوهای مجازی»، «بررسی جرایم تروریستی برخط با جمع‌آوری شواهد دیجیتالی و از طریق استفاده از فناوری‌های نوین، و «ترویج مشارکت‌های بین‌المللی برای همکاری علیه بهره‌گیری تروریستی از فناوری‌های نوین»، اقدام می‌نماید.

7. https://learn.unoct-connectandlearn.org/course/index.php?categoryid=26

8. Online Terrorist Financing

9 .Delhi Declaration on Countering the Use of New and Emerging Technologies for Terrorist Purposes, New Delhi, India, 29 October2022,https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/outcome_document_ctc_special_mtg_final_e.pdf

تلاش‌ها برای تدوین معاهده‌ای بین‌المللی در زمینهٔ جرایم سایبری از سال ۲۰۱۰ با ابتکار روسیه آغاز شد. این تلاش‌ها پس از تصویب قطعنامه ۲۴۷/۷۴ در سال ۲۰۱۹ و تشکیل کمیته ویژه در سازمان ملل متحد[۱]، به تصویب پیش‌نویس کنوانسیون سازمان ملل متحد علیه جرایم سایبری در آگوست ۲۰۲۳ منجر شد. در ضمن، سازمان ملل متحد در چارچوب مجمع عمومی طی سال ۲۰۲۱، برای تدوین کنوانسیون بین‌المللی جامع مبارزه با بهره‌گیری از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه اولین جلسه سازمانی خود را برگزار کرد.[2] هدف از تهیه پیش‌نویس مزبور «تقویت همکاری‌های بین المللی برای مبارزه با برخی جرایم ارتکابی از طریق سامانه‌های فناوری اطلاعات و ارتباطات و به اشتراک گذاری مدارک به صورت الکترونیکی جرایم جدی»[۳] و با هدف نهایی تهیه پیش‌نویس «کنوانسیون سازمان ملل متحد علیه جرایم سایبری»[۴] بود که پیش‌نویس نهایی این معاهده در اوت ۲۰۲۴ با اجماع عمومی، علی‌رغم انتقادات حقوق بشری، به تصویب رسید.[۵] این معاهده به‌عنوان نخستین سند الزام‌آور در حوزهٔ جرایم در فضای مجازی شناخته می‌شود.[۶]

کنوانسیون به‌منظور تسهیل همکاری بین‌المللی در مقابله با جرایم سایبری به تصویب رسید. همچنین، پیش‌نویس کنوانسیون سازمان ملل برای مقابله با استفاده مجرمانه از فناوری‌های اطلاعات و ارتباطات با ۸۹ ماده در سال ۲۰۲۱ تدوین شد و در راستای قطعنامه ۲۷۴/۷۴ سازمان ملل متحد تصویب گردید.[۷]

لازم به‌ذکر است تعریف هدف و توصیف گستره مفاهیم فنی و حقوقی چنین کنوانسیونی مملو از پیچیدگی است. ایجاد تعادل بین نیاز به اجرای قانون مؤثر با حمایت از حریم خصوصی و حقوق بشر یک چالش مهم باقی مانده است. البته این کنوانسیون طیفی از جرایم اصلی وابسته به سکوهای مجازی و تعداد محدودی از جرایم ارتکابی در سکوهای مجازی را جرم‌انگاری کرده و دولت‌های عضو را موظف می‌کند تا قابلیت‌های تحقیقات و اجرای مجازی را توسعه دهند و این اختیارات نوین را در خصوص سایر جرایم با استفاده از شبکه‌های رایانه‌ای اجرا کنند. در واقع، کنوانسیون بر رویارویی با بهره‌گیری‌های منفی از فناوری متمرکز است، نه ترویج کاربردهای مثبت.[۸] طیف وسیعی از جرایم از جمله دسترسی غیرقانونی، شنود غیرمجاز، تخریب داده‌های الکترونیکی، سوءاستفاده جنسی از کودکان و پول‌شویی عواید ناشی از جرم را جرم‌انگاری می‌کند.

---

1 .Resolution 74/247 of the United Nations General Assembly. "Countering the use of information and communications technologies for criminal purposes," A/Res//74/247 adopted 27 December 2019; available at https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement.

۲.در سال ۲۰۱۷، روسیه این کنوانسیون را با هدف رسیدگی به «چالش‌ها و تهدیدهای ناشی از جرایم ارتکابی در حوزه فناوری اطلاعات و ارتباطات» پیشنهاد کرد(Ahmad, 2024: 1). البته روند کنوانسیون سازمان ملل متحد علیه جرایم سایبری برگرفته از قطعنامه ۲۴۷/۷۴ مجمع عمومی سازمان ملل متحد است که در ژانویه ۲۰۲۰ به تصویب رسید و کمیته موقتی را برای پیش نویس متن ایجاد کرد. با این حال، مذاکرات به رهبری کمیته متوقف شد؛ زیرا نمایندگان به شدت بر سر برخی مفاد توافق نداشتند؛

- https://project-disco.org/privacy/draft-un-convention-against-cybercrime-implications-for-digital-global-governance/

3. https://www.unodc.org/unodc/en/cybercrime/convention/home.html

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Documents/A_AC.291_22_Rev.1_E.pdf

4. "Draft United Nations Convention against Cybercrime", UN General Assembly, A/AC.291/L.16, New York, 29 July–9 August 2024, 7 August 2024, https://documents.un.org/doc/undoc/gen/v24/055/48/pdf/v2405548.pdf

5 .UN. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, [New York]: UN, 7 Aug. 2024

۶. در ۲۳ ژانویه ۲۰۲۴ مؤسسه صلح سایبری (Peace Institute Cyber) ضمن مبادرت به ارائه پیشنهادهایی به جلسه پایانی کمیته موقت برای تدوین کنوانسیون جامع بین‌المللی مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه، اذعان داشت که هدف اصلی پیش‌نویس کنوانسیون سازمان ملل متحد علیه جرایم سایبری باید پاسخگویی به نیازهای بزه‌دیدگان جرایم ارتکابی در سکوهای مجازی و حمایت از تلاش‌ها برای به دست آوردن عدالت و درمان برای کسانی باشد که تحت‌تأثیر جرایم مزبور قرار گرفته‌اند؛

- https://cyberpeaceinstitute.org/news/proposed-cybercrime-convention-risks-making-cyberspace-less-secure/#acb5750e-3fd4-4f57-8d17-1a4a591a908a

7 .https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf

8 .https://unu.edu/cpr/blog-post/understanding-uns-new-international-treaty-fight-cybercrime

بااین‌حال، نگرانی‌های حقوق بشری پیرامون این کنوانسیون از جمله اختیارات گسترده نظارتی، نبود پادمان‌های کافی برای حفاظت از حریم خصوصی و خطر نقض آزادی‌های اساسی به‌وضوح نمایان است. در متن کنوانسیون، اصول و موازین حقوق بشر به‌ویژه در زمینه آزادی بیان و حریم خصوصی به‌طور کامل لحاظ نشده و این موضوع می‌تواند به سوءاستفاده از این معاهده برای نظارت و سرکوب منجر شود(Farajzadeh, 2024: 98). از این‌رو، متن کنوانسیون کنوانسیون دارای نکاتی قابل تأمل است که در ذیل بدان‌ها اشاره می‌شود:

الف- کنوانسیون دامنه بسیار وسیعی از اقدام‌های مجرمانه را پذیرفته است. این سازمان در پی رویارویی با سوءاستفاده از سامانه‌های فناوری اطلاعات و ارتباطات برای اهداف جنایی بوده که با آزادی عمل گسترده‌ای به قلمروهای حاکمیتی سایر کشورها در تعریف جرم و جنایت در چارچوب مقررات داخلی‌شان توصیف شده است. این رویکرد فراتر از تعریف مورد پذیرش در جرایم ارتکابی در سکوهای مجازی به‌عنوان جرایمی با قصد مجرمانه علیه محرمانگی، یکپارچگی و در دسترس بودن داده‌ها و سامانه‌های رایانه‌ای است. بدون تعریف دقیق و شفاف از جرایم ارتکابی در سکوهای مجازی که شامل اهداف و مقاصد مجرمانه باشد، موجب خواهد شد تا کنوانسیون خطر قدرت بخشیدن به دولت ها برای جرم انگاری اقدام‌های مشروع منافع عمومی، نظیر تحقیقات روزنامه نگاری و هک اخلاقی را به‌دنبال داشته باشد.

ب- کنوانسیون این اختیار را به دولت‌ها می‌دهد تا ارائه‌دهندگان خدمات را وادار کنند تا در صورت درخواست، داده‌ها را با نظارت ارائه دهند که این امر خود موجب ورود آسیب بالقوه به مصرف‌کنندگان، حریم خصوصی و اقتصاد دیجیتال می‌شود. البته کنوانسیون فاقد حمایت کافی برای حقوق بشر است؛ کنوانسیون به‌طور عمده حقوق بشر را در چارچوب مقررات داخلی تعریف می‌کند، که منجر به حمایت‌های نابرابر در بین کشورها می‌شود که حمایت از حقوق بشر را به تفسیر فردی دولت‌ها موکول می‌کند. با این همه، در حالی که یک معاهده الزام‌آور قانونی پیرامون جرایم ارتکابی در سکوهای مجازی ظرفیت قابل توجهی برای پاسخگویی به چشم‌انداز تهدیدهای موجود در سکوهای مجازی در حال تحول دارد، اما متأسفانه دارای نواقص قابل تأمل و جدی است. کنوانسیون با تحمیل تعهدات قابل توجه بر ارائه‌دهندگان خدمات و ترویج مجموعه‌ای نظارتی از پادمان‌های حقوق بشر، محیط تجاری بین‌المللی را تضعیف می‌کند و به رشد اقتصادی آسیب می‌زند. این در حالی است که با توانمندسازی جمع‌آوری و ذخیره‌سازی گسترده داده‌ها توسط دولت‌ها، می‌تواند خطر نقض امنیت و دسترسی غیرمجاز به اطلاعات حیاتی را افزایش دهد (Delsol, 2024: 1).

۳.۳. رویکردِ حقوقیِ بین‌المللی در حکمرانی هوش مصنوعی برای مقابله با جرایم تروریستی ارتکابی در سکوهای مجازی

با پیشرفت فناوری‌های دیجیتال و هوش مصنوعی، فضای مجازی به بستری برای ارتکاب جرایم تروریستی تبدیل شده است که چالش‌هایی برای نهادهای قضایی و حکمرانی حقوق بشر ایجاد نموده است. هوش مصنوعی می‌تواند در شناسایی و مقابله با جرایم تروریستی نقش مؤثری ایفا کند، مشروط بر اینکه توازن میان امنیت و حقوق بشر حفظ گردد. از این رو، حقوق بین‌الملل نقش مهمی در شکل‌دهی به حکمرانی هوش مصنوعی در فضای مجازی ایفا می‌کند، اما برای تنظیم مؤثر تأثیر حکمرانی هوش مصنوعی بر مسئولیت‌پذیری، حریم خصوصی، امنیت و حقوق بشر، نیازمند تطبیق و تکامل مستمر است(Bhushan, 2024: 387). بنابراین، معاهدات بین‌المللی، نظیر کنوانسیون بوداپست، به حفاظت از حقوق فردی و مقابله با تروریسم پرداخته‌اند. همکاری بین‌المللی و طراحی دقیق سامانه‌های هوش مصنوعی برای مقابله با تهدیدات تروریستی امری ضروری است تا از نقض حریم خصوصی و حقوق بشر پیشگیری شود.

منشور ملل متحد به‌عنوان سنگ بنای حقوق بین الملل عمل می‌کند و اصولی مانند حاکمیت دولت، عدم مداخله و حل و فصل مسالمت آمیز اختلافات را ایجاد می‌کند. این اصول همچنان به هدایت روابط بین‌الملل در زمینهٔ هوش مصنوعی و فضای مجازی ادامه می‌دهند.

معاهدات حقوق بشر، مانند اعلامیه جهانی حقوق بشر و میثاق بین المللی حقوق مدنی و سیاسی، حقوق و آزادی‌های اساسی را که در عصر دیجیتال قابل اجرا هستند، تضمین می‌کنند. این حقوق شامل حق حریم خصوصی، آزادی بیان و منع تبعیض می‌شود. حقوق بین‌المللی بشردوستانه که به‌عنوان حقوق مخاصمات نیز شناخته می‌شود، حقوقی را برای محافظت از نظامیان و غیرنظامیان در جریان مخاصمات مسلحانه وضع می‌کند.[۱]

«کنوانسیون بوداپست راجع‌به جرایم سایبری» تنها معاهده بین‌المللی است که رفتارها و گونه‌شناسی‌های انجام شده از طریق رایانه و سامانه‌های های اطلاعاتی را جرم انگاری می‌کند. این سند حاوی مقررات اساسی و رویه‌ای برای تحقیق، اجرا و قضاوت در مورد جرایم ارتکابی از طریق سامانه‌های رایانه‌ای و فناوری‌های اطلاعاتی است. سند مزبور به جرایم جنایی ارتکابی از طریق فضای مجازی نظیر هک، سرقت داده‌ها و کلاهبرداری برخط می پردازد.[۲] این همکاری بین‌المللی را در تحقیق و تعقیب جرایم ارتکابی در سکوهای مجازی ترویج می‌کند. این معاهده بر حقوق افراد دارای معلولیت و نیاز به فناوری‌های فراگیر و در دسترس از جمله سامانه‌های هوش مصنوعی تأکید می‌کند. این امر بر اهمیت حصول اطمینان از اینکه هوش مصنوعی و فضای مجازی تبعیض را تداوم نمی‌بخشد یا افراد دارای معلولیت را به حاشیه رانده نمی‌کند، تأکید می‌کند(Larson, 2010: 116).[۳]

در خلال کنفرانس اختاپوس ۲۰۱۸ در زمینه همکاری علیه جرایم سایبری[۴]، اداره کل حقوق بشر و حاکمیت قانون شورای اروپا نشستی را در مورد هوش مصنوعی و جرایم سایبری[۵] برگزار کرد که در آن نمایندگان شورای اروپا فعالیت‌ها و یافته‌های اولیه خود را در مورد سیاست هوش مصنوعی ارائه کردند.[۶] سخنرانان برخی از چالش‌هایی را که هوش مصنوعی برای مقامات مجری قانون ایجاد می‌کند، برجسته کردند و در مورد آنها بحث کردند، مانند جرم انگاری فیلم و جعل اسناد و اینکه چگونه مقامات می‌توانند چالش را برای به‌دست آوردن و حفظ شواهد الکترونیکی در دادگاه پیش ببرند.[۷] کنفرانس اختاپوس ۲۰۲۱ همکاری علیه جرایم سایبری[۸] از ۱۶ تا ۱۸ نوامبر ۲۰۲۱ به طور کامل به صورت برخط به دلیل وضعیت کووید-۱۹ برگزار شد، نشست فرعی «هوش مصنوعی، جرایم سایبری و شواهد الکترونیکی» را برگزار کرد.[۹]

---

۱ این در مورد استفاده از فناوری هوش مصنوعی و سامانه‌های تسلیحاتی خودمختار (Autonomous Weapons Systems "AWS") در جنگ اعمال می‌شود و از رعایت اصول تمایز، تناسب و ضرورت نظامی اطمینان می‌دهد.

2. Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series - No. 185, https://rm.coe.int/1680081561

۳ .در خلال کنفرانس هشت در سال ۲۰۲۱ در مورد همکاری علیه جرایم سایبری که به مناسبت بیستمین سالگرد کنوانسیون بوداپست برگزار شد، اعلام شد که کمیته وزرای شورای اروپا تصویب دومین پروتکل الحاقی به کنوانسیون بوداپست را در مورد افزایش همکاری و افشای مدارک الکترونیکی به‌عنوان سند اصلی تصویب کرد؛

- Council of Europe, "Second Additional Protocol to the Budapest Convention adopted by the Committee of Ministers of the Council of Europe", Strasbourg, 17 November 2021, available at: https://www.coe.int/en/web/cybercrime/-/second-additional-protocol-to-the-cybercrime-convention-adopted-by-the-committee-of-ministers-of-the-council-of-europe.

4. 2018 Octopus Conference on Cooperation against Cybercrime, https://rm.coe.int/3021-90-octo18-keymessages/16808c67bb

5. The Conference program of the 2018 Octopus conference on cooperation against cybercrime is available at: https://rm.coe.int/3021-90-octo18-prog/16808c2b04.

6. Activities of the Council of Europe on Artificial Intelligence (AI), 9 May, 2018, available at: https://rm.coe.int/cdmsi-2018-misc8-list-ai-projects-9may2018/16808b4eac.

7. See the presentations of this panel at the Plenary Closing session of the 2018 Octopus Conference, available at: https://www.coe.int/en/web/cybercrime/resources-octopus-2018.

8. 2021 Octopus Conference on Cooperation against Cybercrime, https://www.pseti.psu.edu/the-order-of-the-octopus-2021/

9 .The presentation and materials of this panel are available at: https://www.coe.int/en/web/cybercrime/workshop-cybercrime-e-evidence-and-artificial-intelligence.

«کنوانسیون شورای اروپا در مورد حمایت از کودکان در برابر استثمار جنسی و سوءاستفاده جنسی»[1] موسوم به «کنوانسیون لانزاروته شورای اروپا»[2] یک معاهده بین‌المللی است که شامل تدابیر حقوقی اساسی برای حمایت از کودکان در برابر خشونت جنسی از جمله بهره‌کشی جنسی و سوء استفاده از کودکان برخط است. این کنوانسیون به منظور مبارزه با جرایم علیه کودکان و پیشگیری از سوءاستفاده‌های جنسی از آنها، با تقویت همکاری بین‌المللی، کشورهای عضو را ملزم به تصویب و اجرای قوانین مناسب برای مقابله با این جرایم می‌کند. علاوه بر این، این کنوانسیون با بهره‌گیری از فناوری‌های هوش مصنوعی، به شناسایی و پیشگیری از سوءاستفاده‌های جنسی در فضای برخط کمک می‌نماید. هوش مصنوعی قادر است محتوای غیرقانونی را شناسایی کرده و از دسترسی به آن پیشگیری کند، همچنین ابزارهایی را برای حمایت از کودکان در فضای دیجیتال توسعه دهد. هدف اصلی کنوانسیون، تسهیل پیشگیری از سوءاستفاده‌های جنسی و حفاظت از حقوق کودکان در فضای دیجیتال است.

«کنوانسیون شورای اروپا در مورد پیشگیری و مبارزه با خشونت علیه زنان و خشونت خانگی»[3] موسوم به «کنوانسیون استانبول» یکی دیگر از معاهده‌های شورای اروپا است که هدف اصلی آن حمایت از زنان در برابر هر نوع خشونت و مقابله و از بین بردن همه اشکال خشونت علیه زنان از جمله جنبه‌های خشونت خانگی است. این کنوانسیون، اولین سند الزام آور قانونی است که مدعی ایجاد «یک چارچوب قانونی و رویکرد جامع برای مبارزه با خشونت علیه زنان» است و بر پیشگیری از خشونت خانگی، حمایت از بزه‌دیدگان و تعقیب مجرمان متهم تمرکز دارد.

در چارچوب رویکرد حقوقی بین‌المللی برای مقابله با جرایم تروریستی در سکوهای مجازی، استفاده از سامانه‌های هوش مصنوعی در نظام عدالت کیفری در حال رشد است، اما بسیاری از مقامات قضایی و اجرائی هنوز آمادگی کامل برای مواجهه با ابعاد فنی و حقوقی این فناوری را ندارند، به‌ویژه زمانی که این فناوری برای اهداف مخرب مورد استفاده قرار گیرد. علاوه بر این، شواهد کافی برای اثبات آموزش و توانمندی مقامات جهانی در جمع‌آوری شواهد فرامرزی وجود ندارد. در نتیجه، برای انجام تحقیقات مؤثر، همکاری و هماهنگی بین‌المللی ضروری است، چرا که مقامات ملی ممکن است از منابع لازم برخوردار نباشند.

۴. چالش‌ها و راهکارهای حقوقی در حکمرانی هوش مصنوعی برای مقابله با جرایم تروریستی در سکوهای مجازی؛ ضرورت توسعه مقررات بین‌المللی هماهنگ و انعطاف‌پذیر

کاربرد اصول و معاهدات حقوقی خاص برای هوش مصنوعی و فضای مجازی می‌تواند پیچیده باشد. برای نمونه، حق حفظ حریم خصوصی، همانطور که در حقوق بین‌المللی حقوق بشر تصریح شده است، ممکن است نیاز به تفسیر مجدد در مواجهه با فناوری‌های نظارتی پیشرفته و شیوه‌های جمع‌آوری داده‌ها داشته باشد که توسط هوش مصنوعی تسهیل می‌شوند. به طور مشابه، حقوق مخاصمات و حقوق بشردوستانه بین‌المللی باید برای رسیدگی به چالش‌های ناشی از سامانه‌های تسلیحاتی خودمختار و استفاده از هوش مصنوعی در درگیری‌های مسلحانه تطبیق داده شوند(Amoroso, 2020: 96-97). از آنجایی که حکمرانی هوش مصنوعی از مرزهای ملی فراتر می رود، تقویت چارچوب حقوقی بین‌المللی برای رسیدگی به چالش های مرتبط با حکمرانی هوش مصنوعی ضروری می‌شود. ایجاد اصول اخلاقی پذیرفته شده جهانی برای توسعه و استقرار هوش مصنوعی می‌تواند چارچوب مشترکی را برای کشورها برای تنظیم سامانه‌های هوش مصنوعی فراهم کند. این می‌تواند شامل اصولی مانند شفافیت، انصاف، نظارت انسانی و پاسخگویی باشد. استانداردسازی اصول اخلاقی به همان اندازه در پرداختن به پیامدهای اخلاقی فناوری‌های هوش مصنوعی بسیار مهم است(Bhushan, 2024: 387).

1. The Lanzarote Convention (*The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse*) entered in force on 1 July 2010, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201/signatures.

2. Lanzarote Convention

3 .The Istanbul Convention (*The Council of Europe Convention on preventing and combating violence against women and domestic violence*) entered into force on 1 August 2014 and it has been ratified by 34 countries. See the chart of signatures and ratifications at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/210/signatures?p_auth=OwhAGtPd.

سامانه‌های هوش مصنوعی باید به گونه‌ای توسعه داده شوند که به حقوق بشر احترام بگذارند و از آن حمایت کنند. باید تدابیری برای پیشگیری از تبعیض، سوگیری و نقض حریم خصوصی و آزادی های فردی در نظر گرفته شود. حاکمیت هوش مصنوعی در فضای مجازی تعهد به حمایت از حقوق بشر و ترویج برابری را ایجاد خواهد کرد. چارچوب‌های قانونی باید به تأثیرات تبعیض آمیز بالقوه فناوری های هوش مصنوعی بپردازند و اطمینان حاصل کنند که استقرار آنها به حقوق افراد بدون توجه به جمعیت شناسی احترام گذاشته و از آنها محافظت می‌کند(Lin and Kerr, 2021: 121).

مقررات بین‌المللی حکمرانی هوش مصنوعی باید با سرعت تحولات فناوری همگام و انعطاف‌پذیر باشند تا اثربخشی خود را حفظ کنند. هماهنگی میان دولت‌ها و پیشگیری از تضادهای قانونی برای ایجاد استانداردهای جهانی ضروری است. همکاری بین‌المللی و تبادل دانش میان کارشناسان و نهادها می‌تولند چالش‌های هوش مصنوعی را کاهش دهد. این چارچوب‌ها باید رویکردی میان‌رشته‌ای شامل فناوری، حقوق، اخلاق و حقوق بشر داشته باشند و استفاده مسئولانه از هوش مصنوعی در فضای مجازی و مقابله با جرایم تروریستی را تضمین کنند. تلاش هماهنگ جهانی برای توسعه و استقرار هوش مصنوعی مسئولانه حیاتی است(Bhushan, 2024: 387).

با این همه، اجرای اصول اخلاقی در حکمرانی هوش مصنوعی و مقابله با جرایم تروریستی در فضای مجازی نیازمند رویکردی جامع و چندجانبه است. این رویکرد شامل تدوین استانداردهای اخلاقی روشن، ایجاد نهادهای نظارتی مستقل، تنظیم توافق‌های بین‌المللی و بهره‌گیری از سامانه‌های هشداردهنده برای شناسایی محتوای تروریستی است. تفاوت‌های فرهنگی و مسائل حریم خصوصی باید مدنظر قرار گیرند و همکاری جهانی برای ایجاد چارچوب‌های مشترک، نقش کلیدی در تضمین امنیت، شفافیت و رعایت حقوق بشر در فضای دیجیتال ایفا می‌کند.

نتیجه‌گیری

جرایم تروریستی در سکوهای مجازی به دلیل نقش راهبردی فضای مجازی در سطوح مختلف، به‌ویژه در زمینه‌های اقتصادی، سیاسی، فرهنگی و امنیتی، تهدیدی جدی به شمار می‌آید. این جرایم با استفاده از فناوری‌های پیشرفته‌ای چون نرم‌افزارهای رمزگذاری و ابزارهای استراق‌سمع برای نفوذ به شبکه‌ها و سامانه‌های امنیتی، به‌طور فزاینده‌ای گسترش یافته‌اند. گروه‌های تروریستی با بهره‌برداری از فضای مجازی، به‌ویژه از طریق تبلیغات رسانه‌ای، جاسوسی، تخریب وب‌گاه‌ها و جذب نیرو، اهداف خود را دنبال می‌کنند. پیشرفت‌های فناوری هوش مصنوعی همچنین موجب هوشمندسازی ربات‌ها شده است که قادرند وظایف انسانی را انجام دهند و این فناوری‌ها در راستای تقویت عملیات‌های مجریان قانون مورد استفاده قرار می‌گیرند.

حکمرانی هوش مصنوعی، به‌عنوان یک فناوری پیشرفته، می‌تواند تحولی اساسی در نحوه برخورد نهادهای قضایی و پلیس با جرایم تروریستی ایجاد کند. در این راستا، می‌توان سازوکارهای عملیاتی‌ای را پیشنهاد داد که افزایش توانمندی در مقابله و پیشگیری از این جرایم را تسهیل می‌کند. این سازوکارها به شرح زیر می‌باشد:

الف- در زمینه شناسایی ابزارهای توانمندسازی کارکنان عدالت کیفری، باید به شناسایی و استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی و فناوری‌های اطلاعات و ارتباطات (از جمله داده‌های کلان) اهمیت ویژه‌ای داده شود، تا مقامات اجرایی قانون قادر باشند به‌طور مؤثری در مقابله با جرایم تروریستی در سکوهای مجازی عمل کنند.

ب- کشورهای مختلف باید شکاف‌های موجود در ساختارهای حقوقی خود را شناسایی و نسبت به اصلاح و روزآمدی آن‌ها اقدام نمایند تا امکان تحقیق و تعقیب مؤثر جرایم تسهیل‌شده توسط فناوری، نظیر تصویب مقررات جدید یا روزآمدی مقررات فعلی با زبان بی‌طرفانه فراهم گردد. همچنین، توسعه همکاری‌های بین‌المللی باید در اولویت قرار گیرد.

ج- دولت‌ها باید همکاری‌های میان‌المللی خود را با سازمان‌های بین‌المللی و منطقه‌ای، جامعه مدنی، بخش خصوصی و دانشگاه‌ها گسترش دهند تا نوآوری‌ها، تحقیقات و توسعه فناوری‌های پیشرفته در زمینه‌های اجرای قانون و عدالت کیفری، به‌ویژه در حوزه پیشگیری و مقابله با جرایم تروریستی در سکوهای مجازی، تقویت گردد.

د- در راستای توسعهٔ مستمر فناوری‌ها و رعایت استانداردهای اخلاقی، باید تلاش‌های لازم جهت بهبود فناوری‌های نوین صورت گیرد تا آمادگی لازم برای مقابله با چالش‌های آن‌ها فراهم شود. همچنین، ارتقای استفاده از استانداردهای اخلاقی در به‌کارگیری این فناوری‌ها باید در اولویت قرار گیرد تا از نقض حقوق بشر و آزادی‌های فردی پیشگیری گردد.

این سازوکارها می‌توانند به‌عنوان پیش‌نیازهای اصلی برای مقابله مؤثر با جرایم تروریستی در سکوهای مجازی و توسعه حکمرانی هوش مصنوعی در این زمینه عمل کنند.

References:

Amoroso, Daniele (2020), Autonomous Weapons Systems and International Law: A Study on Human-machine Interactions in Ethically and Legally Sensitive Domains, Nomos.

Ahmad, Nafees (2024), The Draft UN Cybercrime Convention: A Threat to Human Rights, fair observer, March 23, https://www.fairobserver.com/world-news/the-draft-un-cybercrime-convention-a-threat-to-human-rights/#

Atazadeh, Saeed & Ansari, Jalal (2019). "A Review of Concept of Criminal Responsibility for Artificial Intelligence (A Case Study of Self-Driving Cars) in the Law of Islam, Iran, USA and Germany." Comparative Research on Islamic and Western Law, 6(4): 55–86. https://www.doi.org/10.22091/csiw.2020.4821.1661 [In Persian]

Monaco, L (2017) 'Preventing the Next Attack; A Strategy for the War on Terrorism' Foreign Affairs 96(6), pp. 23-29.

Ashley, Kevin D. (2017), Artificial Intelligence and Legal Analytics, New York: Cambridge University Press.

Bhushan, Tripti (2024), Artificial Intelligence, Cyberspace and International Law Artificial Intelligence, Cyberspace and International Law, Indonesian Journal of International Law, 21(2): 281-314. https://www.doi.org/10.17304/ijil.vol21.2.3

Brokenshire, J. (2013), 'National Security and Civil Liberties – Getting the balance right', speech delivered at National Security Summit at Queen Elizabeth Conference Centre, 3 July 2013, https://www.gov.uk/government/ speeches/national-security-and-civil-liberties-getting-thebalance-right

Cornish, P. (2010), 'Technology, Strategy and Counterterrorism', International Affairs, 86(4), p. 888, https://www.jstor.org/stable/40865000

Davis, Aaron L (2021), Artificial Intelligence and the Fight Against International Terrorism, American Intelligence Journal, 38(2): 63-73.

Delsol, Gabriel (2024), Draft UN Convention Against Cybercrime: Implications for Digital Global Governance, Disruptive Competition Project (DisCo), August 14, https://project-disco.org/privacy/draft-un-convention-against-cybercrime-implications-for-digital-global-governance/

Etaki, Abdelghany, et al. (2024). Justifying the Criminalization of Disseminating of Misleading Information in Cyberspace in Light of Criminalization Criteria. Criminal Law Research, 15(1), 147–162. https://www.doi.org/10.22124/jol.2024.26338.2436 [In Persian]

Farajzadeh, Habibeh (2024). "The Cybercrime Convention: A Step Toward Security or a Violation of Human Rights?" United Nations Studies, 5(1): 98–110. https://www.doi.org/10.22034/iruns.2024.213200 [In Persian]

Kaveh, Mohammad-Hadi & Barani, Mohammad (2024). "Criminal Responsibility of Artificial Intelligence in Iranian Criminal Law with a View to European Union Laws." Comparative Criminal Jurisprudence, 4(3): 51–61. https://www.doi.org/10.22034/jccj.2024.452114.1539 [In Persian]

Kumar Saini, Hemant (2023), Artificial Intelligence and Internet of Things: A Boon for the Crime Prevention, International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), 23-24 Nov, 1-43.

Larson, David Allen (2010), Artificial Intelligence: Robots, Avatars, and the Demise of the Human Mediator, Ohio State Journal on Dispute Resolution, 25: 112.

Lin, H. and J. Kerr (2021), On Cyber-Enabled Information Warfare and Information Operations, in: Oxford Handbook of Cybersecurity, Cornish P., ed, New York: Oxford University Press.

Marra, William and Sarah McNeil (2013), Understanding The Loop: Regulating the Next Generation of War Machines, Harvard Journal of Law & Public Policy, 36: 1140. http://dx.doi.org/10.2139/ssrn.2043131

Namamian, Peyman (2024). Countering and Preventing Terrorist Crimes in the Virtual Social Networks. Law of Emerging Technologies, 5(10): 215–233. https://www.doi.org/10.22133/mtlj.2024.410930.1236 [In Persian]

Namamian, Peyman. (2025). The Scope of Documents of Global and Regional Organizations in Strengthening the Legal Capacity to Deal with Terrorist Crimes. Criminal Law Research, 15(2), 173–189. https://www.doi.org/10.22124/jol.2024.26384.2442 [In Persian]

Nikolic, Mateja (2024), Artificial Intelligence: Terrorism and International Relations, Center for International Relations and Sustainable Development, Belgrade: Republic of Serbia, https://www.cirsd.org/en/young-contributors/artificial-intelligence-terrorism-and-international-relations

Pournejafi, L., et al. (2023). Filtering the cyberspace as a crime or a way for its prevention? Criminal Law Research, 13(2), 163–187. https://www.doi.org/10.22124/jol.2022.20840.2214 [In Persian]

Syllaidopoulos, I., Ntalianis, K. S., & Salmon, I. (2025). Comprehensive survey on AI in counter-terrorism and cybersecurity: Challenges and ethical dimensions. Journal ieeexplore, 13: 91740- 91764. https://doi.org/10.1109/access.2025.3572348

Wall, C. (2025). The ghost in the machine: Counterterrorism in the age of artificial intelligence. https://www.tandfonline.com/doi/full/10.1080/1057610X.2025.2475850#d1e108

استناد به این مقاله:

نمامیان، پیمان. (۱۴۰۵)، « واکنش به تهدیدهای ناشی از ارتکاب جرایم تروریستی در سکوهای مجازی با بهره‌گیری از ظرفیت حکمرانی هوش مصنوعی »، **پژوهشنامه حقوق کیفری**، دوره ۱۷، پیاپی ۳۳، صص. ۱۷۹-۱۹۲

DOI: 10.22124/jol.2026.29178.2544