Private Law Research
Vol 12, No. 45, Winter 2024, pp 143-170.
https://jplr.atu.ac.ir
DOI: 10.22054/jplr.2024.68659.2691

ATU PRESS

Original Research/Review/... Received: 17/Jul/2022 Accepted: 05/Feb/2024 eISSN: 2476-6232 ISSN: 2345-3583

Protecting the Right to Informational Privacy against the Threats Caused by Military Artificial Intelligence

Fereshteh Banafi*

Ph.D of Public International Law, Teacher at Law Group of Islamic Azad Unuversity of Booshehr, Booshehr, Iran.

Abstract

Artificial intelligence is the ability of a computer system to solve problems and perform tasks that would otherwise require human intelligence. Artificial intelligence technologies have evolved for decades. Today, many countries are going to develop artificial intelligence in their military programs. Using artificial intelligence for the military purpose will cause many human rights challenges, especially in the area of privacy which is regarded as a fundamental right in a conflict. This privacy extends to cyberspace, to ensure informational privacy and protection of data. Therefore, this research descriptively analyzes the legal and political arrangements and gaps in international humanitarian law and international human rights to protect the privacy in military artificial intelligence between the parties in a conflict and concludes that despite the shortcomings of international humanitarian law and international human rights law, resisting national security to protect informational privacy and delegate the definition of international human rights frameworks in the field of artificial intelligence as part of the authority of private companies besides formal and informal legislation can fill gaps in the rules governing the use of artificial intelligence in a conflict.

It should be noted that in recent years, the human rights community has been busy with digital rights, and especially with the effects of artificial intelligence technology, and there has been increasing attention to the relationship between international human rights laws and standards governing military artificial intelligence.With regard to the use of artificial intelligence, one cannot ignore the danger of constant tension between the purpose and nature of artificial intelligence on the one hand and its use for ethical decision-making in military matters, even with the presence of human control. It should be noted that the advantages of using artificial intelligence in the military field

* Corresponding Author: fereshtehbanafi@yahoo.com
How to Cite: Banafi, F. (2023). Protecting the Right to Informational Privacy against the Threats Caused by Military Artificial Intelligence. *Private Law Research*, 12(45), 143-170. doi: 10.22054/jplr.2024.68659.2691.

have great potentialities, but it may also create several challenges. For example, Artificial Intelligent technologies can facilitate autonomous operations, lead to more informed military decision-making, and increase the speed and scale of military operations. However, it may be unpredictable or vulnerable in some ways. Therefore, in addition to the benefits of artificial intelligence in military industries and lowering the cost of the physical presence of the them, threats caused by the use of artificial intelligence, especially in fully autonomous weapons, and the violation of informational privacy and the establishment of a system of responsibility and accountability for filling legal loopholes caused by the use of artificial intelligence is very necessary.

In this regard, the first possible danger from a military environment under the supervision of artificial intelligence in case of the silence of humanitarian and international human rights rules, data contamination and as a result the loss of digital, physical, political and community security and the distortion of the fundamental right to human dignity. The competition of countries in the use of artificial intelligence to upset the balance of power in the world community has created an increasing concern about the fall of rights and ethics. In this regard, suggestions can be made to amend the rules of international human rights in order to regulate the regulations of military artificial intelligence during the conflict. First, it is a violation of national security for information privacy. The mere fact that a national action is taken to protect national security cannot be a document of violation of fundamental human rights laws by a country. Second, international human rights standards in the field of artificial intelligence should be included in the statutes of private companies. Empowering employees as part of the authority of companies is one of the things that can limit the use of artificial intelligence outside the framework of human rights. And, the promotion of the rules of international humanitarian law whether formally or informally.

Informal legislation includes common understandings based on non-binding resolutions and declarations, guidelines and regulations of uniform professional conduct, the practices of industries, domestic laws and policies, civil society reports and political policies, and international and transnational dialogues. Also, redefining and amending official human rights treaties by international institutions can cover digital rights under the rules of international human rights and humanitarian rights. Despite this, although data protection and information privacy regimes are not applicable due to the exclusion of national security of countries, but by establishing informal norms and legislation in international humanitarian law, it is possible to help include the ethics of artificial intelligence in the contemporary laws of war. It is a key factor in human control, which is necessary to comply with international humanitarian law and to satisfy ethical concerns, as a basis for internationally agreed limits on independence in weapons systems. This research has tried to provide a strategy upon which helping the international community to

strengthen the rules of humanitarian law and international human rights against the threats caused by the use of artificial intelligence in the military context in the field of violation of the right to informational privacy and accountability of those who violates it.

Keywords: Artificial Intelligence, Informational Privacy, International Humanitarian Law, Human Rights, War.

پژوهش حقوق خصوصی
سال دوازدهم، شماره ۴۵، زمستان ۱۴۰۲، ۱۷۰-۱۴۳
https://jplr.atu.ac.ir
DOI: 10.22054/jplr.2024.68659.2691

مقاله پژوهشی
تاریخ پذیرش: ۱۴۰۲/۱۱/۱۶
تاریخ دریافت: ۱۴۰۱/۰۴/۲۶
eISSN: 2476-6232 ISSN: 2345-3583

حفاظت از حقّ حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی

فرشته بنافی* دکترای حقوق بین‌الملل عمومی، مدرس گروه حقوق دانشگاه آزاد بوشهر، بوشهر، ایران.

چکیده

هوش مصنوعی توانایی یک سیستم کامپیوتری در حلّ مشکلات و انجام وظایفی است که در صورت نبودن آن به هوش انسانی نیاز است. فناوری‌های هوش مصنوعی برای چندین دهه تکامل یافته‌اند. امروزه بسیاری از کشورها در حال توسعهٔ هوش مصنوعی در برنامه‌های نظامی خود هستند که با چالش‌های حقوق بشری فراوانی به‌ویژه در زمینهٔ حفظ حریم خصوصی به‌عنوان حقّی بنیادین در یک مخاصمه مواجه می‌باشند. این حریم با توسعه به فضای مجازی، متضمّن حریم خصوصی اطلاعاتی و حفاظت از داده‌ها می‌گردد؛ لذا این پژوهش به روش توصیفی-تحلیلی تمهیدات و خلأهای قانونی و سیاسی موجود در حقوق بین‌الملل بشردوستانه و حقوق بشر بین‌المللی جهت صیانت از حریم خصوصی در هوش مصنوعی نظامی برای طرف‌های متخاصم را احصا می‌نماید و به این نتیجه می‌رسد که علی‌رغم کاستی‌های مقررات حقوق بین‌الملل بشردوستانه و حقوق بشر، تخطی از امنیت ملّی جهت حفظ حریم خصوصی اطلاعاتی، تفویض تعیین چهارچوب‌های حقوق بشر در زمینهٔ هوش مصنوعی به‌عنوان بخشی از اختیارات شرکت‌های خصوصی، در کنار قانون‌گذاری رسمی و غیررسمی می‌تواند خلأهای قانونی مربوط به استفاده از هوش مصنوعی در یک مخاصمه را پوشش دهد.

واژگان کلیدی: حریم خصوصی اطلاعاتی، حقوق بشر، حقوق بین‌الملل بشردوستانه، هوش مصنوعی، جنگ.

* نویسنده مسئول: fereshtehbanafi@yahoo.com

مقدّمه

فناوری‌های نظامی هوش مصنوعی پیوسته در حال تکامل و بهبود هستند و ممکن است در مجموعه‌ای از محیط‌های عملیاتی مختلف مفید واقع شوند.[۱] این فناوری‌ها شامل تشخیص الگو، یادگیری ماشین، بینایی رایانه‌ای،[۲] درک زبان طبیعی و تشخیص گفتار است.[۳] این فناوری‌ها برای افزایش توانایی‌های انسان‌ها و ماشین‌ها به‌کار گرفته می‌شوند و به آن‌ها کمک می‌کنند تا تصمیم‌هایی با کیفیت بالاتر و سرعت بیشتر بگیرند. این‌ها سیستم‌هایی هستند که برای حلّ تکالیف و دستیابی به اهدافی خاص طراحی شده‌اند که از برخی جهات با فرآیندهای شناختی انسان‌ها در درک استدلال، یادگیری، برقراری ارتباط بین تصمیم‌گیری و عمل، موازی هستند. عملکرد این سیستم‌ها می‌تواند آنها را برای کارهایی مانند شناسایی تانک‌های جنگی در تصاویر ماهواره‌ای، شناسایی اهداف با ارزش در میان جمعیت با استفاده از تشخیص چهره، ترجمهٔ متن برای کسب اطلاعات از منابعی که در دسترس عموم قرار دارند و تولید متن در عملیات اطلاعاتی بسیار مفید باشد. همچنین در زمینه‌هایی مانند سیستم‌های توصیه، تشخیص ناهنجاری، سیستم‌های پیش‌بینی و بازی‌های کامپیوتریِ رقابتی بسیار توانمند است. یک سیستم هوش مصنوعی می‌تواند به ارتش در کشف تقلّب در خدمات قراردادیِ خود، پیش‌بینی زمان خرابی سیستم‌های تسلیحاتی به دلیل مشکلات تعمیر و نگهداری یا توسعهٔ استراتژی‌های برنده در شبیه‌سازی مخاصمه و همچنین تولید پهپادهای پیشرفته جهت تجسس، شناسایی، ارزیابی و از بین بردن هدفِ تعیین‌شده کمک کند. همه این برنامه‌ها و موارد دیگر، می‌توانند در عملیات‌های روزمره و مخاصمات بعدی، باعث بالا رفتن ضریب نیرو باشند.

---

۱. برای اطلاعات بیشتر در مورد تأثیر هوش مصنوعی بر آیندهٔ جنگ مراجعه کنید به مرادپیری، هادی، خزایی، حمیدرضا، «نقش فناوری‌های نوین اطلاعاتی در جنگ‌های آینده»، فصلنامه مطالعات قدرت نرم، سال ۱۰، ش ۲۳، (۱۳۹۹) صص ۱۷۴-۱۷۱.

2. Computer Vision

3. Chai, Junyi et al., *Machine Learning with Applications: Deep learning in computer vision: A critical review of emerging techniques and application scenarios*, (Elsvier, vol. 6, 2021), p 1.

اگرچه مزیّت استفاده از هوش مصنوعی در زمینهٔ نظامی دارای پتانسیل بالایی است، اما ممکن است چالش‌های متعددی را نیز ایجاد کند. برای مثال، فناوری هوش مصنوعی می‌تواند عملیات‌های خودمختار را تسهیل کند، منجر به تصمیم‌گیری آگاهانه‌تر نظامی شود و سرعت و مقیاس عملیات نظامی را افزایش دهد. با این حال، ممکن است از برخی جهات غیرقابل پیش‌بینی یا آسیب‌پذیر باشد؛ لذا در کنار فواید ذکرشده برای استفاده از هوش مصنوعی در صنایع نظامی و پایین آوردن هزینهٔ حضور فیزیکی نظامیان، تهدیداتی ناشی از به‌کارگیری هوش مصنوعی به‌ویژه در سلاح‌های کاملاً خودمختار و نقض حریم خصوصی اطلاعاتی و برقراری نظام مسئولیت و پاسخگویی جهت پر کردن خلأهای حقوقی ناشی از استفاده از هوش مصنوعی وجود دارد.

در کل، هوش مصنوعی را می‌توان در هفت مورد برای اهداف نظامی به‌کار برد: (۱) تجسس، نظارت و شناسایی؛ (۲) فعالیت پشتیبانی لجستیک؛ (۳) قابلیت‌های دفاعی و تهاجمی سایبری؛ (۴) دستکاری اطلاعات و دفاع در برابر «جعل‌های گسترده»؛ (۵) متمرکزسازی ساختارهای نظامی فرماندهی و کنترل؛ (۶) وسایل نقلیهٔ نیمه‌خودکار و تمام‌خودکار؛ و (۷) سیستم‌های تسلیحاتی خودمختار مرگ‌بار. حقوق بین‌الملل بر آخرین مورد از این هفت کاربرد نظامی متمرکز است. دولت‌ها، سازمان‌های حقوق بشری و متخصصان هوش مصنوعی، به دنبال یافتن و پُر کردن خلأهایی هستند تا هیچ‌کس اعم از سرباز، فرمانده، برنامه‌نویس، توسعه‌دهنده، سازنده یا خود سیستم تسلیحاتی، در مواردی که استفاده از سیستم‌های تسلیحاتی خودمختار مرگ‌بار در نبرد باعث «نقض جدّی قوانین بشردوستانه بین‌المللی» می‌گردد، نتواند از زیر بار مسئولیت پاسخگویی شانه خالی کند.[1] جنبش توقف ربات‌های قاتل و سایر گروه‌های بشردوستانه معتقد هستند که سلاح‌های کاملاً خودمختار به این دلیل که نمی‌توان سیستم پاسخگویی مناسبی برای آن‌ها در نظر گرفت، باید غیرقانونی

1. Crootof, Rebecca, "War Torts: Accountability for Autonomous Weapons", University of Pennsylvania Law Review, vol. 164, no 6, (2016) pp 1385-1386.

اعلام شوند. بااین‌حال قوانین بین‌المللی، دولت‌ها و اشخاص را با استناد به قوانین مخاصمات مسلحانه مسئول می‌داند.[۱]

به‌عنوان نمونه، در سال ۲۰۲۱، پس از تسلط طالبان بر افغانستان، گزارشی در مورد اقدامات فوری ارتش کانادا، وزارت امور خارجه ایالات متحده و آژانس توسعهٔ بین‌المللی ایالات متحده منشر شد که بر اساس آن، این نهادها به سرعت فرآیندی را برای حذف حضور دیجیتالی حامیان افغان از وب‌سایت خود، از ترس انتقام توسط رژیم جدید افغانستان آغاز کردند. در واقع، هم طالبان و هم نیروهای ائتلاف تحت رهبری ایالات متحده به اسکنرهای قابل حملِ مجهّز به هوش مصنوعی که کار آنها جمع‌آوری داده‌های مربوط به چشم، اثر انگشت، عکس و زندگی‌نامه افراد بود، تکیه داشته‌اند و این اطلاعاتِ جمع‌آوری‌شده به کمک هوش مصنوعی نظامی در زمان تسلط ایالات متحده بر افغانستان، اکنون امنیت آن دسته از افغان‌هایی را که با آمریکایی‌ها همکاری می‌کردند، بیشتر تهدید می‌کند.[۲] آنچه ذکر گردید، نمونه‌ای است که در آن حریم خصوصی، حفاظت از داده‌ها، پردازش خودکار، اطلاعات بیومتریک و درگیری مسلحانه با یکدیگر تلاقی پیدا می‌کنند و این نشان می‌دهد که علاوه بر ربات‌های قاتل و حملات سایبری، اقیانوسی از مسائل حقوقی در زمینهٔ نقض حریم خصوصی اطلاعاتی اشخاص و نهادها برای تحقیق در زمینهٔ هوش مصنوعی وجود دارد؛ بنابراین با وجود چنین نقض‌هایی، باید چارچوبی را برای یک رژیم کنترل تسلیحات جدید برای کاهش خطرات مرتبط با انواع خاصی از برنامه‌های هوش مصنوعی ارائه نمود. با وجود این و تا زمانی که چنین چارچوبی محقق شود، ضرورت دارد تا بررسی شود که آیا چارچوب‌های قانونی موجود، پیش از این به تحدید استفاده از هوش مصنوعی نظامی جهت حفظ حریم خصوصی اطلاعاتی در قالب یک معاهده پرداخته‌اند یا خیر و در صورت مثبت بودن پاسخ، چگونه این امر محقق گردیده است. به‌عنوان نمونه، شورای امنیت سازمان ملل

---

1. Ivey, Matthew, "the Ethical Midfield in Artificial Intelligence: Practical Reflections for National Security Lawyers", Georgetown Journal Legal Ethics, vol.33, n1, (2020). p 118.
2. Freeze, Colin, "Fearing reprisals, Afghans rush to scrub digital presence after Taliban takeover", Globe & Mail Canada, (2021).

متحد، وزرای دفاع و امورخارجهٔ کشورها می‌توانند بررسی نمایند که آیا می‌توان به‌کارگیری هوش مصنوعی را با عقد یک معاهدهٔ همه‌جانبه تحدید نمود؟ در این راستا، بررسی نقش‌هایی که حقوق بشر برای حفظ حریم خصوصی و حفاظت از داده‌ها در تنظیم هوش مصنوعی نظامی و دیگر فناوری‌های نوظهور مورد استفاده در زمان مخاصمه و تکنولوژی جمع‌آوری داده‌ها دارد، بسیار ضروری است.

هرچند تمرکز این پژوهش بر هوش مصنوعی است، اما بخشی از یک کار تحقیقاتی گسترده‌تر است که به‌طور وسیع، نقش حقوق دیجیتال را در تنظیم مخاصمات مسلحانه آینده بررسی می‌نماید. با دیجیتالی‌شدن میدان جنگ، باید توجه علمی و عملی بیشتری به استفاده هم‌زمان از حقوق برای حفظ حریم خصوصی اطلاعات، امنیت سایبری، مالکیت داده‌ها و قابلیت حمل‌ونقل، شخصیت و استقلال دیجیتالی و اثرات بازدارنده آنها بر طرف‌های متخاصم نمود. این پژوهش، تمهیدات قانونی و سیاسی، جهت تنظیم قراردادهای شرکتی بخش خصوصی و همتایان دولتی آن‌ها به‌عنوان بخشی از مشارکت عمومی-خصوصی که ماشین‌های نظامی هوش مصنوعی را به‌پیش می‌برد، مورد بررسی قرار می‌دهد و در چهار مبحث به نقش حقوق بین‌الملل بشردوستانه و حقوق بشر در گنجاندن اخلاق هوش مصنوعی در قوانین جنگ معاصر در زمینه حفظ حریم خصوصی می‌پردازد.

۱. حقوق بین‌الملل بشردوستانه و به‌کارگیری هوش مصنوعی در زمان جنگ

در واقع سیستم‌های هوشمند نظامی، به دلیل استقلال در عملکرد خود در انتخاب و حمله به اهداف و با عنایت به خطر فقدان کنترل انسانی بر سلاح‌ها و استفاده از زور، از منظر قانون، اخلاق و حقوق بشردوستانه نگران‌کننده هستند. فقدان کنترل انسانی به دلیل غیرقابل پیش‌بینی‌بودن، خطراتی را متوجه غیرنظامیان می‌نماید و طبق حقوق بشردوستانه بین‌المللی، مسئولیت قانونی سربازان طرف مخاصمه را به خاطر انجام حمله در شرایط نبود کنترل کافی بر سلاح خود و همچنین، نگرانی‌های اخلاقی، به‌علت فقدان عامل انسانی در تصمیم‌گیری برای استفاده از زور جهت حفظ مسئولیت اخلاقی و کرامت انسانی به دنبال دارد. در این راستا، کمیتهٔ بین‌المللی صلیب سرخ، نقش مهمی در ارزیابی پیامدهای تحولات معاصر و

آینده در مخاصمات مسلحانه از جمله بررسی ابزار و روش‌های جدید مخاصمات، به‌ویژه از نظر سازگاری آنها با قواعد حقوق بین‌المللِ بشردوستانه و خطرات ناشی از پیامدهای نامطلوب انسانی بر افراد تحت حمایت دارد.[۱]

در سال‌های اخیر کمیته بین‌المللی صلیب سرخ بر «کنترل و ارزیابی انسانی» به‌عنوان یک مؤلفهٔ اساسی در تنظیم هوش مصنوعی در زمان جنگ تأکید داشته است و با استناد به دکترین کلاسیک حقوق بین‌الملل بشردوستانه در مورد لزوم رعایت تمایز، تناسب و لحاظ اقدامات احتیاطی در یک حمله نظامی، به‌ویژه استفاده از سلاح‌های خودمختار، استدلال می‌کند که مبنای رعایت دکترین مذکور «ارزیابی موردی بر اساس شرایط موجود» جهت طراحی و اجرای حملات، صرفاً می‌تواند توسط انسان اتخاذ شود تا مشروعیت قانونی و مقبولیت اخلاقی آن تضمین گردد. کمیتهٔ بین‌المللی صلیب سرخ به مواضع کشورهای عضو کنوانسیون در مورد ممنوعیت یا محدودیت به‌کارگیری برخی سلاح‌های متعارف که ممکن است بیش‌ازحد خطرناک یا دارای اثرات نامشخص باشد،[۲] استناد می‌کند که طبق آن کشورهای عضو کنوانسیون مزبور به‌رسمیت شناخته‌اند که «مسئولیت انسانی» جهت استفاده از سیستم‌های تسلیحاتی و زور «باید حفظ شود» و بسیاری از کشورها، سازمان‌های بین‌المللی – از جمله صلیب سرخ – و سازمان‌های مردم‌نهاد، بر الزام وجود کنترل انسانی برای اطمینان از انطباق با قوانین بین‌المللی بشردوستانه و سازگاری با ارزش‌های اخلاقی تأکید کرده‌اند.

کمیتهٔ بین‌المللی صلیب سرخ تأکید می‌کند که به هنگام مخاصمات مسلحانه «استفاده بالقوه از سیستم‌های هوش مصنوعی برای تصمیم‌گیری‌هایی که ذیل قوانین خاص حقوق بین‌الملل بشردوستانه قرار می‌گیرند، همانند زمان بازداشت افراد، مستلزم کنترل دقیق و ارزیابی انسانی است».[۳] کشورها نیز جهت تنظیم قواعد هوش مصنوعی در زمان مخاصمات

---

1. International Committee of the Red Cross, "Artificial intelligence and machine learning in armed conflict: A human-centred approach", International Review of the Red Cross, vol. 102, (2020) p 464.
2. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, (1980), amended on 21 December 2001.
3. International Committee of the Red Cross, "Artificial intelligence and machine learning in armed conflict: A human-centered approach", (June 6, 2019) p 7-8,

باید بر «مدل‌های انسان‌محور» که مبتنی بر حقوق بین‌الملل بشردوستانه است، تمرکز نمایند و خود را متعهد به حفظ کنترل کافی و ارزیابی دقیق انسانی در تصمیم گیری‌ها جهت هدف قرار دادن یک منطقه نمایند.

برای حمایت از این مقررات انسان‌محور، برخی از حقوق‌دانان، ماده ۳۶ پروتکل الحاقی اول به کنوانسیون‌های ۱۹۴۹ ژنو را مطمح نظر قرار داده‌اند.[۱] این ماده مقرر می‌دارد که کشورهای متعاهد «در مطالعه، توسعه، دستیابی یا پذیرش یک سلاح، ابزار یا روش‌های جدید جنگی، موظف هستند تعیین کنند که آیا استفاده از آن، در برخی یا همه شرایط، طبق این پروتکل یا هر قاعدهٔ دیگر حقوق بین‌الملل که برای طرف‌های متعاهد قابل اعمال است، ممنوع شده است یا خیر.»[۲] ماده مذکور، دولت‌ها را مکلف می‌دارد تا ماهیت قانونی و غیرقانونیِ سلاح‌ها، ابزار یا روش‌های نوین جنگی را با توجه به مقررات پروتکل اول الحاقی و سایر قواعد حقوق بین‌الملل تعیین کنند؛[۳] لذا کلیهٔ مقررات انسان‌محور با موضوع هوش مصنوعی باید حول محور حقوق بشر و قوانین حقوق بشردوستانه تنظیم شوند.[۴]

---

https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-humancentred- approach

1. Thompson, Chengeta, "Are Autonomous Weapon Systems the Subject of Article 36 of Additional Protocol I to the Geneva Conventions?", (2014) p 15. Available at SSRN: http://dx.doi.org/10.2139/ssrn.2755182.

ثامپسون معتقد است هنگامی که یک ماشین، بدون دخالت عامل انسانی تصمیم به استفاده از نیروی مرگ‌بار می‌گیرد، هرگز نمی‌توان این استفاده از زور را تحت کنترل معنادار یا مؤثر انسانی قرار داد؛ بنابراین برای اینکه یک سیستم تسلیحاتی ذیل ماده ۳۶ پروتکل اول الحاقی به‌عنوان سلاح قرار گیرد، باید تحت دخالت مستقیم و معنادار انسانی و کنترل مؤثر باشد.

2. Protocol Additional to the Geneva Conventions (12 August 1949), and Relating to the Protection of Victims of International Armed Conflicts, (June 8 1977), art. 36

۳. شریفی طرازکوهی، حسین؛ برمکی، جعفر، «چالش‌های حقوقی قابلیت فضای سایبری در پرتو ماده ۳۶ پروتکل یکم الحاقی ۱۹۷۷»، مجله حقوقی بین‌المللی، ش ۶۲، (۱۳۹۹) ص ۱۲۶.

۴. علاوه بر تعهد مندرج در ماده ۳۶ پروتکل اول الحاقی به کنوانسیون ۱۹۴۹ ژنو که برای تمام کشورهای عضو و غیرعضو الزام‌آور است، اغلب کشورها از جمله هلند، نروژ، سوئد، بلژیک، ایالات متحده و استرالیا در حقوق داخلی خود کمیته‌هایی جهت ارزیابی سلاح‌ها، ابزارها و روش‌های نوین جنگی ایجاد نموده‌اند. با این‌حال تا کنون، تعداد کمی، اگر وجود داشته باشند، جرأت کرده‌اند به بررسی واقعی شیوهٔ اعمال رژیم‌های حقوق بشر خاص در حقوق

از دیگر چالش‌های حقوق بشردوستانه در موضوع هوش مصنوعیِ نظامی، حفاظت از داده‌ها و حفظ حریم خصوصی اطلاعاتی در زمان مخاصمات مسلحانه است. به‌عنوان نمونه، جمع‌آوری داده‌ها از جمعیت‌های آسیب‌دیده از جنگ، مسئولیت غیرقابل انکاری را بر دوش سازمان‌های بشردوستانه می‌گذارد تا اطمینان حاصل شود که داده‌های افراد آسیب‌دیده در یک مخاصمهٔ مسلحانه برخلاف هدفی که برای آن جمع‌آوری شده است، مورد سوءاستفاده قرار نگیرد و آن‌ها را در معرض خطر قرار ندهد. علاوه‌براین، روش‌هایی که از طریق آن داده‌ها و اطلاعات منتشر می‌شوند، چگونگی آغاز مخاصمات و سایر موقعیت‌های خشونت‌آمیز را در مواردی مانند مخاصمه مسلحانه داخلی در کشور میانمار[1] و قتل‌عام اقلیت مسلمان آشکار می‌سازند.

اطلاعات نادرست و سخنان نفرت‌انگیز و «واقعیت‌های نادرست جدید» که از طریق «جعل عمیق»[2]، با استفاده از یادگیری ماشینی برای تولید محتوای ویدئویی، صوتی و متنی مصنوعی ارائه شده است از جمله خطرات جدیدی هستند که با استفاده گسترده از پلتفرم‌های رسانه‌های اجتماعی و سایر ابزارهای انتشار آنلاین همراه شده‌اند.[3]

در شرایط مخاصمه مسلحانهٔ بین‌المللی و غیربین‌المللی و سایر موقعیت‌های خشونت‌بار، همانند اغتشاشات و آشوب‌های خیابانی، استفاده از فناوری‌ها توسط عموم مردم به شرکت‌های پشتیبان رسانه‌های اجتماعی، پیام‌رسانی و بسترهای جست‌وجو، قدرت فزاینده‌ای در جعل واقعیات و تغییر مسیر اعتراضات و شکست یک جبههٔ مخاصمه مسلحانه را می‌دهد. در جریان مخاصمات مسلحانه و آشوب‌های خیابانی، شرکت‌های بزرگ فناوری با استفاده

بین‌الملل بشردوستانه یا قدرت آن‌ها برای محدود کردن شیوه‌های خاص طراحی، توسعه، استقرار و به‌کارگیری هوش مصنوعی بپردازند.

1. Stevenson, Alexandra, "Facebook Admits It Was Used to Incite Violence in Myanmar", New York Times, (6 November 2018) available at: www.nytimes.com/2018/11/06/technology/myanmar-facebook.html.
2. Deep Fake
3. Rejali, Saman, Heiniger, Yannick, "the Role of Digital Technologies in Humanitarian Law, Policy and Action: Charting a Path Forward", International Review of the Red Cross, vol. 102, (2020) pp 1-2.

از هوش مصنوعی، تأثیرات جهانی در انعکاس آزادی بیان از یک‌سو و انتشار اطلاعات نادرست در حساب‌های رسانه‌های اجتماعی از سوی دیگر داشته‌اند. این امر در زمان همه‌گیری ویروس کرونا نمود بیشتر دارد؛ زیرا جمعیت‌های آسیب‌دیده برای دریافت اطلاعات و برقراری ارتباط با یکدیگر بیش از هر زمان دیگری به چنین پلتفرم‌هایی وابسته هستند.

به این ترتیب، فناوری‌های جدید هوش مصنوعی می‌توانند به‌طور غیرمستقیم در دامن‌زدن به ایجاد خصومت، نقض حریم خصوصی و ترویج اطلاعات نادرست به‌ویژه در زمان مخاصمات، آشوب‌های خیابانی و جنگ رسانه‌ای مؤثر باشند و به دلیل خلأهای حقوقی در زمینه سلاح‌های با فناوری هوش مصنوعی، بازتعریفی از قواعد، مقررات و تعاریف موجود حقوق بین‌الملل بشردوستانه ضرورت دارد.[۱] در همین راستا، کمیتهٔ بین‌المللی صلیب سرخ می‌تواند با بسط مفاهیم حقوق بشردوستانه به هوش مصنوعی، نقش مهمی در تحول حقوق دیجیتالی به نفع جمعیت درگیر در یک مخاصمه ایفا نمایند.

۲. هوش مصنوعی نظامی و حقوق بشر

فناوری‌های هوش مصنوعی منعکس‌کنندهٔ ارزش‌ها و انتخاب‌های افرادی است که آنها را ساخته و استفاده می‌کنند؛ لذا این پتانسیل را دارند تا بر حقوق بشر، دموکراسی و حاکمیت قانون تأثیر منفی بگذارند.[۲] یکی از حقوق بنیادین که در ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی و در مجموعه‌ای از معاهدات منطقه‌ای خاص با موضوع حقوق بشر بدان تصریح شده است، حقّ حفظ حریم خصوصی است. در گزارش کمیساریای عالی حقوق بشرِ سازمان ملل متحد آمده است: «از این حق چنین می‌توان استنباط نمود که افراد باید دارای یک حریم مستقل برای توسعه، تعامل و آزادی، یک «حریم خصوصی» جهت تعامل با یا بدون دیگران، عاری از مداخلهٔ دولت یا مداخلهٔ بی‌جا توسط سایر افراد ناخوانده، داشته

---

۱. شریفی طرازکوهی، حسین، جعفر برمکی، همان، ص ۱۴۱.

2. Leslie, David, et al., "Artificial Intelligence, Human Rights, Democracy, and the Rule of Law, a Primer", the Council of Europe, and the Alan Turing Institute, (2021) p 15.

باشند. این فضای خصوصی با گسترش به اینترنت، آنچه به‌عنوان «حریم خصوصی اطلاعاتی» شناخته می‌شود را دربر خواهد گرفت.[1]»

نهادهای معاهداتی حقوق بشر و دادگاه‌های منطقه‌ای نیز رویهٔ قضایی غنی پیرامون مفهوم حریم خصوصی اطلاعاتی تدوین کرده‌اند تا در مواجهه با محیط تکنولوژیک در حال تغییر، معنای در حال تحولّ حقّ تاریخی حفظ حریم خصوصی را مقرر نمایند. این معنا اکنون به یک حقّ مرتبط، یعنی حقّ حفاظت از داده‌ها، تبدیل شده است. ترکیب «حریم خصوصی اطلاعاتی» و «حفاظت از داده‌ها» مجموعه‌ای از اصول اساسی و تعهدات شکلی و ماهوی را بر دوش کشورها جهت احترام و تضمین حقوق دیجیتال قرار می‌دهد تا اثرات خارجی منفی هوش مصنوعی به‌کار رفته در زمان جنگ را محدود نماید.

حقوق بشر، مقررات روشنی در مورد انصاف، شفافیت، تدابیر مناسب جهت مقابله با سوءاستفاده، همچنین ارزیابی و نظارت، و روش‌های جبران خسارت به قربانیان احتمالی را مطمح نظر قرار داده است؛[2] بنابراین کاربرد آن می‌تواند یک دولت را ملزم نماید تا در طراحی و آموزش الگوریتم‌های پیش‌بینی‌کننده در هوش مصنوعی، تمهیدات بیشتری را لحاظ نماید. همچنین چنانچه تکامل هوش مصنوعی نظامی با نقض حریم خصوصی اطلاعاتی، از جمله اطلاعات شخصی همراه باشد، حقوق بشر می‌تواند راه‌حلی جهت محدودیت آن از طریق اصولی همچون مشروعیت، ضرورت[3] و تناسب، تعیین سقف برای ذخیره‌سازی داده‌ها[4] و محدودیت ذخیره‌سازی[5] داده‌ها، ارائه کند. با وجود این، هرچند

---

1. Report of the United Nations High Commissioner for Human Rights about the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/39/29, (2018) para. 5
2. Ibid, para. 26-42-46-58-61
3. Necessity
4. Storage specification

۵. اصل محدودیت ذخیره‌سازی (Storage Limitation Principle)، یک اصل کلیدی در حفظ حریم خصوصی داده‌ها است، با این مضمون که سازمان‌ها نباید داده‌های شخصی را برای مدت‌زمان طولانی نگه دارند و برای هرگونه دادهٔ شخصی یا دادهٔ های مجازی در حال پردازش قابل اعمال است، اما برای داده‌های شخصی که ناشناخته اند و نمی‌توان آنها را مجدداً با موضوع داده‌ای خاص مرتبط نمود، اعمال نمی‌گردد.

حقوق بشر هنجارهای جذابی را ارائه می‌دهد، اما سؤالات مهمی در مورد گستره و ماهیت کاربرد هم‌زمان و فراسرزمینی حقوق بشر در زمان مخاصمات مسلحانه مطرح می‌گردد.

با عنایت به سکوت معاهدات حقوق بشردوستانه در مورد قوانین خاصّ حاکم بر حریم خصوصی اطلاعاتی و حفاظت از داده‌ها، این مسئله مطرح می‌گردد که آیا این سکوت، یک ویژگی یا یک اشکال محسوب می‌گردد. باید اذعان داشت، یک بخش از قوانین ممکن است در رابطه با موضوع خاصّی که توسط قوانین دیگر مورد توجه قرار گرفته است، ساکت باشند. به‌عنوان مثال، حقّ آزادی بیان که یکی از حقوق بنیادین حقوق بشر است، ذیل مخاصمات مسلحانه قرار نمی‌گیرد. به این تقدیر، چنانچه حقوق مخاصمات مسلحانه در مورد یک موضوع کاملاً ساکت باشد، ممکن است بتوان چنین استدلال کرد که قوانین بین‌المللیِ حقوق بشر باید به‌طور خودکار آن «خلأ» را پر کند.[1]

علاوه‌براین، خلأهای موجود در مخاصمات مسلحانه ممکن است یک حذف عامدانه باشد که منعکس‌کنندهٔ واقعیت مخاصمات مسلحانه است؛ لذا نمی‌توان تصور کرد که حقوق بشر بدون تغییر و انعطاف‌پذیری نسبت به شرایط ویژهٔ برخی از مخاصمات اعمال شود؛ بنابراین تحلیل مورد به مورد تعهدات حقوق بشری و حقوق بین‌الملل بشردوستانه با توجه به ویژگی‌های منحصربه‌فرد هر مخاصمهٔ مسلحانه جهت نقض و تعیین اولویت برخی تعهدات حقوق بشری نسبت به سایر تعهدات همانند امنیت ملی که استثنائی بر برخی تعهدات حقوق بشری است، ضرورت دارد.

این سؤالات تفسیریِ پیچیده با مسئلهٔ حل‌نشدهٔ اجرای موازی قوانین عرفی و معاهداتی حاکم بر حقوق بشر در زمان مخاصمات مسلحانه ترکیب می‌شود. در همین راستا، مستثنی‌شدن امنیت ملی کشورها در رژیم حفاظت از داده‌ها، موضوعی نگران‌کننده است. در حقیقت، در اکثر کشورها، قوانین ملی حفاظت از داده‌ها، محدودیت‌هایی برای حفاظت از اطلاعاتی که برای امنیت ملی، دفاع از حاکمیت، نظم عمومی و بررسی برخی جرایم کیفری ضروری هستند قائل می‌شوند. کمیسیون حقوق بین‌الملل اولویت امنیت ملی و سایر

---

1. Murray, Daragh, et al., *Practitioners' guide to human rights law in armed conflict*, (Oxford University Press, 2016) p102.

موارد فوق الذکر جهت تخطی از حریم خصوصی اطلاعاتی را به‌عنوان اصل قابلیت تخطی نام‌گذاری کرده است.[۱] چنین به‌نظر می‌رسد که این امر چارچوب قانونی حفاظت از داده‌ها را با برنامه‌های هوش مصنوعیِ توسعه‌یافته و مورد استفاده در مخاصمات مسلحانه و همچنین هرگونه پردازشی که توسط آژانس‌های امنیتی و اطلاعاتی انجام می‌شود، مسدود می‌کند. در واقع، پیش‌نویس پیشنهادشدهٔ اخیر در مورد مقررات هوش مصنوعی که توسط اتحادیه اروپا تهیه شده است، به‌صراحت آن «سیستم‌های هوش مصنوعی را که منحصراً برای اهداف نظامی توسعه یافته‌اند یا مورد استفاده قرار می‌گیرند»[۲] مستثنی نموده است.

آخرین نگرانی به یکی از بازیگران کلیدی در فضای نظامی هوش مصنوعی، یعنی شرکت‌های چندملیتی خصوصی ارتباط می‌یابد. در دیدگاه سنتی، معاهدات حقوق بشری، متضمن تعهدات حقوقی دولت‌های عضو هستند و به تعهدات سایر بازیگران با شخصیت‌های حقوقی غیردولتی نمی‌پردازد. اگرچه دولت‌ها می‌توانند مستقیماً تعهداتی را بر شرکت‌ها تحمیل کنند و از این راه باعث توسعهٔ حقوق بین‌الملل گردند، اما آن‌ها تاکنون این کار را نکرده‌اند. هرچند هنجارهای مربوط به تجارت و حقوق بشر همانند تعهدات معاهداتی الزام‌آور نیستند، اما اثر حقوقی آنها همانند «حقوق نرم»" است.[۳]

با عنایت به آنچه ذکر گردید، با اصلاح کنوانسیون‌های حقوق بشری موجود از طریق اضافه کردن قوانینی مرتبط با هوش مصنوعی یا اضافه کردن پروتکل‌های الحاقی به

---

۱. به ضمیمه چهارم گزارش کمیسیون حقوق بین‌الملل در مورد پنجاه‌وهشتمین جلسه کاری آن، با موضوع: حفاظت از داده‌های شخصی در گردش فرامرزی اطلاعات، ضمیمه سند سازمان ملل متحد به شماره ۱۰ ((A/61/10, 224 2006)) مراجعه کنید.

http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf.

۲. پیش‌نویس پارلمان و شورای اروپا در مورد تنظیم مقررات هماهنگ در مورد هوش مصنوعی (قانون هوش مصنوعی) و اصلاح برخی از مفاد قانونی،

COM/2021/206 final,
https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

3. International Council on Human Rights Policy (ICHRP) ,"Beyond Voluntarism: Human Rights and the Developing International Legal Obligations of Companies", Geneva, Switzerland, (2002) p73.

کنوانسیون‌های موجود یا تصویب کنوانسیون‌ها یا کنوانسیون چهارچوب‌های حقوق بشری، می‌توان مجموعه‌ای از قوانین الزام‌آور در زمینهٔ هوش مصنوعی را تصویب کرد و تا آن زمان، برای اطمینان از اینکه طراحی، توسعه و استقرار سیستم‌های هوش مصنوعی ناقض قوانین حقوق بشر نگردند، ضرورت دارد تا سازمان‌های بین‌المللی و منطقه‌ای اعم از دولتی و غیردولتی، اصل مراقبت مقتضی را مطمح نظر قرار دهند. همچنین استفاده از اصل ارزیابی آثار، یکی از ابزارهای عملی برای شناسایی، پیشگیری، کاهش و پاسخگویی در مقابل اثرات نامطلوب استفاده از سیستم‌های دارای قابلیت هوش مصنوعی در نقض حقوق بشر بدان استناد گردد.

۳. خطرات ناشی از عدم تنظیم مقررات مربوط به هوش مصنوعی در محیط نظامی

منطق هوش مصنوعی بر طبقه‌بندی و کدگذاری حیات انسان‌ها به داده‌های قابل محاسبه است. بااین‌حال همهٔ اینها در تضاد کامل با ماهیت دقیق، لاینفک و پیچیدهٔ تفکر اخلاقی است. حلّ وظایف چالش‌برانگیز اخلاقی، از جمله شناسایی اهداف بالقوه، با هوش مصنوعی، حتی با پیچیده‌ترین تکنیک‌های یادگیری ماشین از نظر اخلاقی دشوار و از وظایف منحصر انسانی است. به‌این‌ترتیب با کاربرد روزافزون فناوری‌های نوظهور مانند هوش مصنوعی و سیستم‌های خودمختار، نیاز آشکاری به نسخهٔ به‌روزشدهٔ کنوانسیون ژنو جهت بازتعریف مفاهیم حقوق بشر، حفظ حق حریم خصوصی و انتساب فعل متخلفانه جهت برقراری مسئولیت بین‌المللی وجود دارد.

هنگامی که کنوانسیون ژنو در سال ۱۹۴۹ ایجاد شد، روش‌های دیجیتالی انتشار محتوا به پخش رادیویی و تلویزیونی محدود می‌گردید و قدرت محاسباتی رایانه‌ای در مراحل اولیه بود. از آن زمان، نه‌تنها جنگ از طریق حملات سایبری و تبلیغات رسانه‌های اجتماعی به اینترنت گسترش یافته است، بلکه جنگ اطلاعاتی عادی شده و ربات‌ها نیروی فزاینده‌ای در میدان نبرد هستند. جنگ جاری روسیه و اوکراین نمونه کاملی از این دست است که چگونه استفادهٔ نرم‌افزاری از سلاح‌های خودمختار و هوش مصنوعی، به‌ویژه از طریق حملات

سایبری و راه‌اندازی کمپین‌های اطلاعاتی نادرست در کنار هواپیماهای بدون سرنشین و سلاح‌های مافوق صوت جریان یک مخاصمه را تغییر می‌دهد. با وجود این، نسخه اصلاح‌شده‌ای از کنوانسیون ژنو وجود ندارد؛ لذا یک ارزیابی واقع‌بینانه از فن‌آورهای جدید بر اساس ویژگی‌های فنی و نحوهٔ استفاده از آنها در چارچوب قواعد حقوق بشر و حقوق بشردوستانه ضروری است.

به‌این‌ترتیب، با توجه به ضعف حقوق بشردوستانه و حقوق بشر بین‌المللی در تنظیم مقررات توسعه و استقرار برنامه‌های نظامی هوش مصنوعی این سؤال مطرح می‌گردد که خطرات احتمالی ناشی از یک محیط نظامی تحت نظارت هوش مصنوعی چیست؟ در پاسخ می‌توان اولین خطر را «آلودگی داده‌ها» دانست که «آسیب‌های بیرونی ناشی از جمع‌آوری و سوءاستفاده از داده‌های شخصی»[1] را دربر می‌گیرد. استفاده از هوش مصنوعی می‌تواند امنیت دیجیتالی، فیزیکی و سیاسی کشورها و اشخاص طرف حملات سایبری را تهدید کند. لازم به ذکر است که داده‌های شخصی هیچ نقشی در جنگ‌های فیزیکی ندارند و حفاظت از آن‌ها همانند زمان صلح در زمان مخاصمه نیز امکان‌پذیر است. حتی اگر داده‌های شخصی در یک مخاصمه نقش داشته باشد، بر اساس دو اصل حقوق بشر بین‌المللی، همانند زمان صلح استفاده غیرمجاز و نقض حریم خصوصی اطلاعاتی ممنوع است. حقوق بشر نقض حریم خصوصی مربوط به داده‌های پزشکی را ممنوع می‌کند و این امر می‌تواند سایر داده‌های شخصی حساس را نیز دربرگیرد. علاوه بر این، بر اساس اصل ضرورت نظامی، داده‌های شخصی مصون از حمله هستند. مخاصمهٔ مسلحانه یک رویداد غیرعادی است که اَعمال و عملکرد قوانین و رویه‌ها را در حدّ ضرورت تغییر می‌دهد و استفادهٔ غیرمجاز از داده‌های شخصی ارتباط چندانی با غلبه بر قدرت نظامی دشمن ندارد.[2]

---

1. Ben-Shahar, Omri, "Data Pollution", Journal of Legal Analysis, Vol. 11, (2019) P 104.
2. McDermott, Helen, “Application of the International Human Rights Law Framework in Cyber Space In Human Rights and 21st Century Challenges”, Oxford University Press, (2020) p190.

همچنین استفاده از هوش مصنوعی به‌منظور خودکارسازی وظایف مربوط به نظارت، ترغیب و تدلیس «ممکن است تهدیدات مرتبط با تهاجم به حریم خصوصی و تحریک جامعه را گسترش دهد». به‌این‌ترتیب باید نگران یک جوّ اطلاعاتی مبتنی بر هوش مصنوعی بود که نهادهای سیاسی و بصیرت جامعه را از بین می‌برد و درعین‌حال حق بنیادین کرامت انسانی را مخدوش می‌کند. چنین فضایی با مشارکت شرکای خصوصی در این پروژه‌ها تشدید می‌شود.

علاوه بر این، تشدید رقابت تسلیحاتی اَبرقدرت‌ها در هوش مصنوعی بر ایجاد اجماع عمومی پیرامون استانداردهای اخلاقی اساسی در مورد حاکمیت داده‌ها سایه افکنده است. رقابت کشورها در استفاده از هوش مصنوعی جهت برهم‌زدن توازن قدرت در جامعهٔ جهانی، نگرانی فزاینده‌ای در مورد سقوط حقوق و اخلاق ایجاد کرده است؛[1] بنابراین تنظیم مقررات در زمینه هوش مصنوعی به‌ویژه در حوزهٔ مخاصمات مسلحانه، اعم از جنگ‌های فیزیکی و سایبری و بازتعریف قواعد حقوق بشردوستانه و حقوق بشر بین‌المللی متناسب با مسائل حقوق دیجیتالی ضروری است.

۴. راهکارهای حفظ حریم خصوصی اطلاعاتی هوش مصنوعیِ نظامی

با توجه به چالش‌هایی که در بخش‌های پیشین بدان اشاره شد، این سؤال مطرح می‌گردد که چگونه می‌توان کنوانسیون‌ها و منشورهای حقوق بشری بین‌المللی و منطقه ای را اصلاح کرد تا به پتانسیل کامل خود در تنظیم مقررات هوش مصنوعی در زمان مخاصمه دست یابند؟ یکی از این راهکارهای پیشنهادی، تخطی از امنیت ملی جهت حفظ حریم خصوصی اطلاعاتی است. برای پرداختن به مشکلات اصل قابلیت تخطی، می‌توان به تصمیم اخیر دیوان دادگستری اتحادیه اروپا در قضیهٔ سازمان غیردولتی حریم خصوصی علیه وزیر امور خارجه و مشترک‌المنافع بریتانیا[2] اشاره کرد. به‌عنوان بخشی از آن پرونده، خواهان استدلال نمود که گردآوری گستردهٔ فراداده‌های ارتباطی توسط سازمان‌های امنیتی و اطلاعاتی بریتانیا بر اساس

1. Ivey, Matthew, Ibid., p 122.
2. Privacy International v Secretary of State for Foreign and Commonwealth Affairs, (2020) para 32.

قوانین اتحادیه اروپا غیرقانونی است؛ زیرا ناقض برخی از پادمان‌های اساسی اتحادیه می‌باشد. برعکس، دولت بریتانیا، با همراهی کشورهای چک، استونی، ایرلند، فرانسه، قبرس، مجارستان، لهستان و سوئد مدعی شد که رژیم اطلاعاتی کشورش خارج از محدودهٔ قوانین اتحادیه اروپا است و برای ادعای خود به بند ۲ ماده ۴ پیمان اتحادیه اروپا استناد کرد که اشعار می دارد: «امنیت ملی صرفاً جزء مسئولیت‌های هر کشور عضو باقی می‌ماند». همچنین بند ۳ ماده ۱ دستوالعمل حفظ حریم خصوصی الکترونیکی اتحادیه اروپا را مستند ادعای خود قرار داد که بیان می‌دارد این دستورالعمل «در مورد فعالیت‌هایی که خارج از پیمان اتحادیه اروپا هستند مانند «فعالیت‌های مربوط به امنیت عمومی، دفاع، امنیت کشورها...»[1] اعمال نمی‌شود. به دیگر سخن، نه کشور تلاش کردند برای گریز از نظارت قانونی بر فعالیت‌های امنیت ملی خود، به اصل قابلیت تخطی مندرج در رژیم حفاظت از داده‌ها که بر اساس دستورالعمل حفظ حریم خصوصی الکترونیکی اتحادیه اروپا ایجاد شده است، استناد نمایند، اما دادگاه تفسیر آن‌ها را رد کرد و بدین ترتیب مسئله امنیت ملی را به چالش کشید. از نظر دیوان دادگستری اتحادیه اروپایی، «اگرچه تعیین منافع اساسی امنیتی کشورهای عضو بر عهدهٔ خود آن‌ها است و آن‌ها می‌توانند تدابیر مناسب را جهت تضمین امنیت داخلی و خارجی خود اتخاذ نمایند، اما به صرف این واقعیت که اقدام ملی اتخاذشده به منظور حفاظت از امنیت ملی است، نمی‌تواند قوانین اتحادیه اروپا را نقض و کشورهای عضو را از تعهد خود مبنی بر رعایت آن قانون مستثنی سازد.»[2]

دیوان دادگستری اتحادیه اروپا همچنین خاطرنشان ساخت با توجه به اینکه بسیاری از عملیات‌های اطلاعاتی مورد بحث مربوط به دستور وصول وجوه به ارائه‌دهندگان شبکه‌های ارتباط عمومی الکترونیکی می‌باشد، اشتباه است که به‌عنوان یک قاعدهٔ کلی فرض شود که همه این عملیات‌ها به‌طور پیش فرض ذیل امنیت ملی کشورها بوده و مشمول معافیت از

1. Directive on Privacy and Electronic Communications, Official Journal, L 201, (2002) P 37–47.
2. Privacy International v Secretary of State for Foreign and Commonwealth Affairs, (2020) para 44.

قوانین اتحادیه اروپا هستند. در عوض، باید بر اساس اینکه چه کسی و به چه روشی عملیات پردازش داده‌ای خاص را انجام داده است، قائل به تفکیک شد.[1]

علاوه بر این، دیوان دادگستری اتحادیه اروپا در حکم شماره ۱/۱۵، پیش‌نویس توافقنامهٔ منعقده بین کانادا و اتحادیه اروپا با موضوع انتقال و پردازش داده‌های مرتبط با ذخیرهٔ هویت مسافران[2] را مورد بررسی قرار داد. ذخیره هویت مسافران، اطلاعات شخصی است که توسط شرکت‌های هواپیمایی در مورد هر یک از مسافران جمع‌آوری شده است. چنین داده‌هایی «برای پیشگیری و مبارزه با تروریسم و سایر جرایم جدّی فراملی»[3] بسیار مهم هستند. دادگاه اروپایی علی‌رغم پیامدهای کیفری و امنیت ملی داده‌های مورد بحث، از تجزیه و تحلیل توافق منصرف نشد و برخی مفاد پیش‌نویس توافقنامه را ناقض مواد ۷، ۸ و بند ۱ ماده ۵۲ منشور حقوق بنیادین اتحادیه اروپا[4] دانست. نظر دادگاه اروپایی بر لزوم رعایت نظام حفاظت از داده‌ها در این پرونده بود؛ زیرا اطلاعات توسط هواپیماهای تجاری خصوصی جمع‌آوری و به اشتراک گذاشته شده بود و این موضوع برای جدا نمودن جنبه‌های امنیتی آن کفایت می‌کرد. به‌عبارت‌دیگر، چنانچه اطلاعات به‌اشتراک گذاشته‌شده در نهایت برای مقاصد حفاظت از امنیت ملی مورد استفاده قرار گیرند، نمی‌توان این اطلاعات را در زمرهٔ اطلاعات طبقه‌بندی‌شدهٔ مرتبط با امنیت ملی فرض نمود. اتخاذ این رویکرد می‌تواند راه را برای رژیم‌های حفاظت از داده‌ها در صنایع فناوری نظامی هوش مصنوعی هموار کند.

با عنایت به آنچه ذکر گردید، «تسلط بخش خصوصی در طراحی فناوری‌های هوش مصنوعی برای مقاصد نظامی» اغلب به‌عنوان یک منبع نگرانی تلقی می‌شوند؛ لذا پیشنهاد دوم می‌تواند تفویض تعیین چارچوب‌های حقوق بشری در زمینه هوش مصنوعی به‌عنوان بخشی از اختیارات شرکت‌های خصوصی در اساسنامه این شرکت‌ها از طریق دولت‌ها، سازمان‌ها و نهادهای بین‌المللی و منطقه‌ای طرف‌حساب این شرکت‌ها باشد.

---

1. Ibid, p 46.
2. Draft Agreement Between Canada and the European Union on the Transfer of Passenger Name Record data, (2014).
3. Court of Justice of the European Union, Grand Chamber, Opinion (1/15) pursuant to Article 218(11) Treaty on the Functioning of the European Union, (2017) para. 19.
4. Charter of Fundamental Rights of the European Union, (2012).

اگرچه رویکرد بخش خصوصی در استخدام ارتش با مخاطراتی همراه است، اما باید اذعان داشت که چنین رویکردی متضمّن تعهدات قانونی نیز خواهد بود؛ لذا همانگونه که انقلاب هوش مصنوعی تحت هدایت شرکت‌های خصوصی است، می‌توان جهت تعیین دستورالعمل‌های حقوق بشری نیز به اساسنامه این شرکت‌ها تکیه کرد. به‌عنوان نمونه، می‌توان به مقررات عمومی حفاظت از داده اتحادیه اروپا[1] که در سال ۲۰۱۸ لازم‌الاجرا شد، اشاره نمود. این مقررات، گسترده هستند و کلیه ناظران و پردازشگران اطلاعات که در خارج از اتحادیه اروپا مستقر هستند و کالا و خدمات به عوامل اطلاعاتی اتحادیه اروپا عرضه یا بر رفتار و عملکرد آن‌ها نظارت می‌کنند را شامل می‌شود. به‌این ترتیب، با گذشت زمان، هرچه کسب و کارهای بیشتری برای بهره‌مندی از مزایای اقتصادی چنین تعریفی با مقررات عمومی حفاظت از دادهٔ اتحادیه اروپا سازگار می‌شوند، ممکن است این مقررات (درست یا نادرست) به‌عنوان یک استاندارد بین‌المللی تلقی شوند. از این مقررات می‌توان به‌عنوان نقطهٔ شروع مشترک بین‌المللی در مورد مقررات حفاظت از داده‌ها در قوانین ملی و منطقه‌ای نام برد؛ لذا اتحادیه اروپا از قدرت اقتصادی بازار خود استفاده می‌کند تا در نهایت دولت‌ها و شرکت‌ها را وادار نماید تا به‌طور کامل از یک حقّ مستقل برای حفاظت از داده‌ها استقبال کنند. همچنین عملکردی مشابه، در زمینه محدود کردن مسابقه تسلیحاتی هوش مصنوعی از طریق مقررات پردازش داده‌های هدفمند با اثرات فراسرزمینی می‌تواند شکل گیرد و اگر کاربرد نظامی هوش مصنوعی مانعی ایجاد نکند، پیشنهاد تنظیم پیش‌نویس مقررات هوش مصنوعی می‌تواند مسیر را هموار نماید.

مثال دیگر، ورود موضوع توانمندسازی کارکنان در اساسنامه شرکت‌ها به مقولهٔ هوش مصنوعی است. این امر در جریان رسوایی گوگل-پنتاگون در سال ۲۰۱۸ رخ داد و طی آن، ۳۱۰۰ کارمند، نامه‌ای را امضا و «به مشارکت کارمندان شرکت گوگل در برنامهٔ پنتاگون جهت استفاده از هوش مصنوعی برای تفسیر تصاویر ویدئویی برای بهبود هدف‌گیری

1. European Union General Data Protection Regulation, (2016).

حملات هواپیماهای بدون سرنشین»[1] اعتراض کردند. گوگل در نهایت به دلیل اقدامات کارمندانش به کار خود در پروژه «میون»[2] پنتاگون که از الگوریتم‌های هوش مصنوعی برای شناسایی هسته‌های مقاومت در عراق و سوریه استفاده می کرد، پایان داد.[3] با وجود این، در سال ۲۰۲۰، گوگل قراردادی جدید با واحد نوآوری دفاعی پنتاگون در زمینه امنیت و مدیریت اَپ‌ها امضا کرد.[4] به‌این‌ترتیب یک دستورالعمل حقوق بشر بین‌المللی در مورد مسابقه تسلیحاتی هوش مصنوعی می‌تواند متضمّن استراتژی هایی جهت توانمندسازی و تقویت نقش کارکنان در اساسنامه یک شرکت باشد. به‌عنوان مثال، کارکنان را می‌توان از طریق داشتن نماینده در هیئت مدیره، ایجاد شوراهای کارکنان، اختصاص رأی غیرالزام آور کارکنان در مورد موضوعات خاص، نظرسنجی از آنان یا به‌وسیله «ترویج تغییر در ساختار و هنجارهای شرکت توانمند ساخت»[5].

سومین راهکار پیشنهادی، ترویج قوانین رسمی و غیررسمیِ حقوق بین‌الملل بشردوستانه است. باید اذعان داشت که معاهدات و ضوابط کنونی حقوق بین‌الملل بشردوستانه عملکرد ضعیفی در مدیریت خطرات احتمالی ناشی از انقلاب نظامی در هوش مصنوعی دارند و با توجه به اینکه تدوین قوانین معاهداتی پیرامون توسعه و استقرار هوش مصنوعی در آیندهٔ نزدیک محقق نخواهد شد، باید بررسی کرد که کدام هنجارها می‌توانند در تقویت قانون

---

1. Shane, Scott, Wakabayashi, Daisuke, "The Business of War': Google Employees Protest Work for the Pentagon", NewYork Times, (2018).
2. Project Maven.
۳. پروژه Maven بینایی رایانه‌ای و الگوریتم‌های هوش مصنوعی را در فایل‌های جمع‌آوری اطلاعات ترکیب می‌کرد تا فیلم‌های هوایی وسایل نقلیه ومناطق خالی از سکنه را بررسی کنند و به‌طور خودکار فعالیت‌های خصمانه را برای هدف‌گیری شناسایی نمایند. در این ظرفیت، هوش مصنوعی در نظر گرفته شده است تا کار تحلیلگران انسانی را که در حال حاضر ساعت‌ها به جست‌وجوی فیلم‌های پهپادها برای کسب اطلاعات عملی می‌پردازند، خودکار کند و به‌طور بالقوه به تحلیلگران آزادی عمل بیشتری می‌داد تا بر اساس داده‌ها تصمیمات کارآمدتر و به‌موقع‌تری بگیرند.
4. Tucker, Partick, "What Google's New Contract Reveals About the Pentagon's Evolving Clouds", Defense One (2020).
5. McDonnell, Brett H., "Strategies for an Employee Role in Corporate Governance", Wake Forest Law Review, Vol. 46, (2011) p. 429.

حمایت از حقوق بشر در زمینه فناوری‌های نوظهور نظامی منشأ اثر باشند. پاسخ را می‌توان در فرایند قانون‌گذاری غیررسمی و رسمی جست‌وجو کرد.

قانون‌گذاری غیررسمی منابعی همانند تفاهمات مشترک مبتنی بر گفت‌وگوی بین‌المللی و فراملی، قطعنامه‌ها و اعلامیه‌های غیرالزام‌آور، دستورالعمل‌ها و آیین‌نامه‌های رفتار حرفه‌ای، گزارش‌های جامعه مدنی و خط‌مشی‌های سیاسی، رویه صنایع و حتی قوانین و سیاست‌های داخلی را شامل می‌گردد. احتمالاً چنین منابعی نسبت به مفاد معاهده دقیق‌تر و انعطاف‌پذیرتر هستند و بنابراین بهتر می‌توانند توسعهٔ پیش‌بینی‌نشدهٔ فناوری را پوشش دهند. در این زمینه، گسترش سریع سیستم‌های هوش مصنوعی، افزایش چارچوب‌های اخلاقی برای هدایت نمودن توسعه و نحوهٔ استفاده از این فناوری‌ها را تسریع کرده است و اینها نتیجهٔ تلاش دولت‌ها، صنایع، مؤسسات دانشگاهی، سازمان‌های بین‌المللی و سازمان‌های غیردولتی می‌باشد. مرکز اینترنت و جامعه برکمن کلاین، محتوای ۳۶ سند برجستهٔ «اصول هوش مصنوعی» را بررسی و هشت موضوع مشترک را تعیین کرده است که شامل حریم خصوصی، مسئولیت‌پذیری، ایمنی و امنیت، شفافیت و توضیح‌پذیری، انصاف و عدم تبعیض، کنترل انسانی فناوری، مسئولیت‌پذیریِ حرفه‌ای و ارتقای ارزش‌های انسانی هستند.[1]

تدوین چنین دستورالعمل‌ها و آیین‌نامه‌های رفتاری غیرالزام‌آور به شیوه‌ای یکسان، می‌تواند به ایجاد درکی مشترک که حامی ارزش‌های حقوق بشری حتی بدون استفاده از زبان قانون باشد، کمک نماید. به موازات منابع غیررسمی، کمیته بین‌المللی صلیب سرخ نیز می‌تواند با همکاری دولت‌ها اقداماتی را جهت تغییر معاهدات رسمی حقوق بشردوستانه انجام دهد تا مسئله حقوق دیجیتال نیز به تدریج ذیل این معاهدات قرار گیرد. به‌عنوان مثال در اقدامی فوری می‌تواند خواستار یک کمپین تنظیم تفسیر جدید از اصول با محوریت تجزیه و تحلیل گستره و ماهیت استفاده از حقوق حریم خصوصی و حفاظت از داده‌ها در جریان مخاصمات مسلحانه به‌طور کلی و به‌طور ویژه در زمینهٔ هوش مصنوعی نظامی باشد.

---

1. Fjeld, Jessica, et. al. , "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI", the Berkman Klein Center for Internet and Society at Harvard University, Research Publication No. 2020-1, (2020) p 20.

نتیجه

در سال‌های اخیر، جامعهٔ حقوق بشر به حقوق دیجیتالی و به‌ویژه به تأثیرات فناوری هوش مصنوعی مشغول بوده و توجه فزاینده‌ای برای ارتباط قوانین بین‌المللی حقوق بشر و استانداردهای حاکم بر هوش مصنوعی نظامی وجود داشته است. با فرض استفاده از هوش مصنوعی به‌عنوان یک ابزار، نمی‌توان خطر تنش دائمی بین هدف و ماهیت هوش مصنوعی از یک‌سو و استفاده از آن برای تصمیم‌گیری مبتنی بر اخلاق در مسائل نظامی را حتی با وجود کنترل انسانی نادیده گرفت.

در همین راستا نخستین خطر احتمالی از یک محیط نظامیِ تحت نظارت هوش مصنوعی در صورت سکوت قواعد حقوق بشردوستانه و حقوق بشر بین‌المللی، آلودگی داده‌ها و در نتیجه ازبین رفتن امنیت دیجیتالی، فیزیکی، سیاسی و بصیرت جامعه و مخدوش‌شدن حق بنیادین کرامت انسانی است. رقابت کشورها در استفاده از هوش مصنوعی جهت بَرهم زدن توازن قدرت در جامعه جهانی، نگرانی فزاینده‌ای در مورد سقوط حقوق و اخلاق ایجاد کرده است. در این راستا، پیشنهادهایی جهت اصلاح قواعد حقوق بشر بین‌المللی به‌منظور تنظیم مقررات هوش مصنوعی نظامی در جریان مخاصمه می‌توان ارائه کرد. نخست، تخطی از امنیت ملی در قبال حفظ حریم خصوصی اطلاعاتی است. به‌صرف این واقعیت که اقدام ملی اتخاذشده به‌منظور حفاظت از امنیت ملی است، نمی‌تواند مستندی جهت نقض قوانین بنیادین حقوق بشر توسط یک کشور باشد. دوم، استانداردهای حقوق بشر بین‌المللی در زمینهٔ هوش مصنوعی در اساسنامه شرکت‌های خصوصی گنجانده شود. توانمندسازی کارکنان به‌عنوان بخشی از اختیارات شرکت‌ها از مواردی است که میتواند استفادهٔ خارج از چارچوب حقوق بشر از هوش مصنوعی را محدود نماید. سوم، ترویج قوانین رسمی و غیررسمی حقوق بین‌الملل بشردوستانه است.

قانون‌گذاری غیررسمی شامل تفاهمات مشترک مبتنی بر گفت‌وگوهای بین‌المللی و فراملی، قطعنامه‌ها و اعلامیه‌های غیرالزام‌آور، دستورالعمل‌ها و آیین‌نامه‌های رفتار حرفه‌ای متحدالشکل، گزارش‌های جامعه مدنی و خط‌مشی‌های سیاسی، رویه صنایع و حتی قوانین و

سیاست‌های داخلی را شامل می‌گردد. همچنین بازتعریف و اصلاح معاهدات رسمی حقوق بشری توسط کمیتهٔ بین‌المللی صلیب سرخ و نهادهای بین‌المللی می‌تواند حقوق دیجیتالی را تحت پوشش قواعد حقوق بشر بین‌المللی و حقوق بشردوستانه قرار دهد. باوجود این، هرچند رژیم‌های حفاظت از داده‌ها و حفظ حریم خصوصی اطلاعاتی، به دلیل مستثنی نمودن امنیت ملی کشورها قابل اجرا نیستند، اما با وضع هنجارها و قانون‌گذاری غیررسمی در حقوق بین‌الملل بشردوستانه می‌توان به گنجاندن اخلاق هوش مصنوعی در قوانین جنگ معاصر کمک کرد و از عامل کلیدی کنترل انسانی که برای رعایت قوانین بشردوستانه بین‌المللی و ارضای نگرانی‌های اخلاقی ضروری است، به‌عنوان مبنایی برای محدودیت‌های مورد توافق بین‌المللی در مورد استقلال در سیستم‌های تسلیحاتی یاری جست. این پژوهش تلاش نموده است تا یک استراتژی ارائه نماید و به کمک آن، جامعه بین‌المللی را جهت تقویت قواعد حقوق بشردوستانه و حقوق بشر بین‌المللی در مقابل تهدیدات ناشی از استفاده از هوش مصنوعی در بستر نظامی در زمینهٔ نقض حق حریم خصوصی اطلاعاتی و پاسخگویی ناقضین آن یاری نماید.

منابع

مرادپیری، هادی ؛ خزایی، حمیدرضا. « نقش فناوری های نوین اطلاعاتی در جنگهای آینده»، فصلنامه مطالعات قدرت نرم، سال ۱۰، ش ۲۳، (۱۳۹۹)

شریفی طرازکوهی، حسین؛ برمکی، جعفر، «چالشهای حقوقی قابلیت فضای سایبری در پرتو ماده ۳۶ پروتکل یکم الحاقی ۱۹۷۷»، مجله حقوقی بین‌المللی، ش ۶۲، (۱۳۹۹)

References

Ben-Shahar, Omri, “Data Pollution”, Journal of Legal Analysis, Vol. 11, (2019)

Chai, Junyi, et al., *Machine Learning with Applications: Deep learning in computer vision: A critical review of emerging techniques and application scenarios*, (Elsvier, vol. 6, 2021).

Crootof, Rebecca, "War Torts: Accountability for Autonomous Weapons", University of Pennsylvania Law Review, vol. 164, no 6, (2016).

Directive on Privacy and Electronic Communications, Official Journal L 201, (2002).

Fjeld, Jessica, et. al., "Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI", the Berkman Klein Center for Internet and Society at Harvard University, Research Publication No. 2020-1, (2020).

Freeze, Colin, "Fearing reprisals, Afghans rush to scrub digital presence after Taliban takeover", Globe & Mail Canada, (2021).

Ivey, Matthew,"the Ethical Midfield in Artificial Intelligence: Practical Reflections for National Security Lawyers", Georgetown Journal Legal Ethics, vol.33, n 1, (2020).

International Committee of the Red Cross, “Artificial Intelligence and machine learning in armed conflict: A human-centred approach”, International Review of the Red Cross, vol. 102, (2020).

International Council on Human Rights Policy (ICHRP), “Beyond Voluntarism: Human Rights and the Developing International Legal Obligations of Companies”, Geneva, Switzerland, (2002).

Leslie, David, et al., “Artificial Intelligence, Human Rights, Democracy, and the Rule of Law, a Primer”, the Council of Europe, and the Alan Turing Institute, (2021).

McDermott, Helen,”Application of the International Human Rights Law Framework in Cyber Space In Human Rights and 21st Century Challenges”, Oxford University Press, (2020).

McDonnell, Brett H., “Strategies for an Employee Role in Corporate Governance”, Wake Forest Law Review, Vol. 46, (2011).

Murray, Daragh, et al., *Practitioners' guide to human rights law in armed conflict*, (Oxford University Press, 2016).

Rejali, Saman, and Heiniger, Yannick, “the Role of Digital Technologies in Humanitarian Law, Policy and Action: Charting a Path Forward”, International Review of the Red Cross, vol. 102, (2020).

Shane, Scott, and Wakabayashi, Daisuke, “The Business of War’: Google Employees Protest Work for the Pentagon”, NewYork Times, (2018).

Stevenson, Alexandra, Facebook Admits It Was Used to Incite Violence in Myanmar, New York Times,(6 November 2018) available at: www.nytimes.com/2018/11/06/technology/myanmar-facebook.html.

Thompson, Chengeta, “Are Autonomous Weapon Systems the Subject of Article 36 of Additional Protocol I to the Geneva Conventions?”, (2014). Available at: SSRN: http://dx.doi.org/10.2139/ssrn.2755182

Tucker, Partick, “What Google’s New Contract Reveals About the Pentagon’s Evolving Clouds”, Defense One, (2020).

Opinions

Court of Justice of the European Union, Grand Chamber, Opinion (1/15) pursuant to Article 218(11) Treaty on the Functioning of the European Union, (2017) para. 19.

Privacy International v Secretary of State for Foreign and Commonwealth Affairs, (2020).

DOCUMENTS

COM/2021/206final,https://eur-lex.europa.eu/legal content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

Charter of Fundamental Rights of the European Union, (2012).

Draft Agreement Between Canada and the European Union on the Transfer of Passenger Name Record data, (2014).

- European Union General Data Protection Regulation, (2016).

International Committee of the Red Cross, "Artificial intelligence and machine learning in armed conflict: A human-centered approach", (June 6, 2019): https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-humancentred- approach

http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 36, (June 8 1977)

Report of the United Nations High Commissioner for Human Rights about the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/39/29, (2018).

Tanslated References into English

Muradpiri, Hadi; Khazaei, Hamidreza, "The Role of New Information Technologies in Future Wars", *Soft Power Studies*, Year 10, Issue 23, (2019). [In Persian]

Sharifi Tarzkohi, Hossein; Barmaki, Jafar, "Legal challenges of cyber space capabilities in the light of Article 36 of the 1st Additional Protocol of 1977" *International Law Review*, Vol. 62, (2019). [In Persian]

استناد به این مقاله: بنافی، فرشته. (۱۴۰۲). حفاظت از حقّ حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی، *پژوهش حقوق خصوصی*، ۱۲(۴۵). ۱۴۳-۱۷۰. doi: 10.22054/jplr.2024.68659.2691