

## L'exception de Connexité en Procédure Civile de l'Iran et de la France

**Badie Fathi\***

Assistant Professor of Faculty of Law and Political Sciences  
of Allameh Tabataba'i University, Tehran, Iran.

### Abstract

Il est possible que deux ou plusieurs affaires connexes devant deux juridictions distinctes et également compétentes est en train d'être instruit et en ce cas il exige que ces affaires mettent ensemble, envisageant ces raisons: la réduction des coûts sociaux et économiques, de permettre au juge de connaître correctement le problème et de résoudre tous les aspects du litige plus rapidement, la bonne administration de la justice, la prévention des jugements contradictoires et l'intérêt d'une bonne justice de les faire instruire et juger ensemble. Dans ce cas, le demandeur et le défendeur ont le droit et même l'obligation de soulever de Exception de connexité Selon l'article 103 de la loi de procédure civile d'Iran approuvée le 9 avril 2000 après JC. L'exception de connexité peut être soulevée devant les deux juridictions. Les systèmes de procédure civile de l'Iran et de la France sont similaires à cet égard, mais il existe également des différences : par exemple, si L'exception de connexité est acceptée, les affaires connexes devraient-elles être renvoyées devant le premier tribunal ou le deuxième tribunal ? Il est nécessaire d'avoir un lien entre les affaires dans la procédure civile iranienne et française. Le lien peut être un lien simple, un lien suffisant et un lien complet (l'indivisibilité des prétentions). Il semble qu'un lien simple ne puisse pas de se dessaisir et de renvoyer de l'affaire, mais un lien suffisant et un lien complète peuvent de se dessaisir et de renvoyer de l'affaire. Parce que dans ce cas il existe entre les litiges un lien tel qu'il soit de l'intérêt d'une bonne justice de les faire instruire ou juger ensemble. En Iran L'exception de connexité a caractéristique de l'ordre public Donc Le juge peut, d'office, ordonner la jonction de plusieurs instances pendantes devant lui Mais en France Il résulte des articles 101 et 103 Code de procédure civile que le renvoi pour connexité doit être demandé par les parties. On admet que le juge ne peut relever d'office l'existence d'une connexité entre deux affaires. L'exception de connexité peut être soulevée par l'une des parties, mais aussi par un tiers mis en cause ou intervenant volontairement au litige Et pour raison d'ordre public. Le délai de soulevée L'exception de connexité, contrairement à la règle stipulée à l'article 87 du Code de procédure civile, qui stipule que les exceptions doivent être


\* Corresponding Author: [bazm.2636@yahoo.com](mailto:bazm.2636@yahoo.com)

**How to Cite:** Fathi, B. (2023). L'exception de Connexité en Procédure civile de l'Iran et de la France. *Private Law Research*, 12(45), 9-35. doi: 10.22054/jplr.2024.75175.2778

soulevées avant la fin de la première audience, Elle peut être déposée devant la Cour d'appel et la Cour de cassation. Par conséquent le délai pour soulever l'exception de connexité n'est qu'à la fin de la première audience. En France, il y a toujours eu un scepticisme face aux exceptions à la tradition héritée du droit romain. Parce que les soulevées entraînent des retards dans les procédures et la justice. Selon cette tradition issue de la domination romaine in limine litis, à l'article 74 du Code de procédure civile, il est stipulé que Les exceptions doivent, à peine d'irrecevabilité, être soulevées simultanément et avant toute défense au fond ou fin de non-recevoir. Il en est ainsi alors même que les règles invoquées au soutien de l'exception seraient d'ordre public. La demande de communication de pièces ne constitue pas une cause d'irrecevabilité des exceptions. Les dispositions de l'alinéa premier ne font pas non plus obstacle à l'application des articles 103, 111, 112 et 118. Il est précisé à l'article 103 que L'exception de connexité peut être proposée en tout état de cause, sauf à être écartée si elle a été soulevée tardivement dans une intention dilatoire. Ce qui est dit à l'article 103 «sauf à être écartée si elle a été soulevée tardivement dans une intention dilatoire» peut être critiquable. , Parce que l'objectif principal L'exception de connexité est la prévention des jugements contradictoires et avec cette déclaration, cet objectif est violé. en France Les recours contre les décisions rendues sur la connexité par les juridictions du premier degré sont formés et jugés comme en matière d'exception d'incompétence. En cas de recours multiples, la décision appartient à la cour d'appel la première saisie qui, si elle fait droit à l'exception, attribue l'affaire à celle des juridictions qui, selon les circonstances, paraît la mieux placée pour en connaître. Mais en Iran Les les décisions Concernant L'exception de connexité ne sont sujettes à aucun recours. Il s'agit d'une faille dans la loi et il est suggéré de la modifier. le fait de ne pas pouvoir porter plainte dans ce domaine est l'un des défauts de la loi sur la procédure civile, et il est suggéré que la loi soit amendée. Lorsque les juridictions saisies ne sont pas de même degré, l'exception de connexité ne peut être soulevée que devant la juridiction du degré inférieur. Bien que cela soit contraire au principe Double degré de juridiction. Les tribunaux français ont rarement accepté la connexité internationale Mais en Iran, selon l'article 971 du Code civil, cela n'est pas acceptable.

**Keywords:** Lien complet, lien Suffisant, L'exception de connexité, La bonne Administration de la Justice.

## ایراد امر مرتبط در آیین دادرسی مدنی ایران و فرانسه

بدیع فتحی\*  استادیار دانشکده حقوق و علوم سیاسی دانشگاه علامه طباطبائی، تهران، ایران.

### چکیده

ممکن است دو یا چند دعوا در یک مرجع یا چند مرجع که دارای صلاحیت هستند، در حال رسیدگی و این پرونده‌ها با یکدیگر مرتبط باشند. در این حالت صرفه‌جویی در هزینه‌های اجتماعی و اقتصادی اصحاب دعوا، جلوگیری از صدور آرای متعارض و به‌طور کلی قضاوت و اداره شایسته جریان دادرسی ایجاب می‌کند که این پرونده‌ها با یکدیگر ادغام یا تجمیع شوند. در این صورت اصحاب دعوا حق و حتی تکلیف دارند که ایراد امر مرتبط را مطرح کنند. از آن‌رو که به باور نگارنده ایراد امر مرتبط جزء ایرادهای دارای ویژگی نظم عمومی است و دادگاه نیز می‌تواند راساً چنین ایرادی را مطرح کند و از همین‌رو نیز مهلت طرح آن تا پایان جلسه نخست دادرسی نیست. در فرانسه نیازی نیست که ایراد امر مرتبط هم‌زمان یا پیش از دفاع ماهوی یا ایراد عدم پذیرش دعوا طرح شود. به نظر می‌رسد که در صورت وجود پرونده‌های مرتبط در مراجع با درجه عالی و تالی در ایران نیز همچون فرانسه، این ایراد به نفع مرجع عالی قابل طرح است. این امر هرچند خلاف اصل دودرجه‌ای بودن رسیدگی است، اما به جهت وابستگی آیینی دعوای مرتبط و در راستای اصل اداره شایسته جریان دادرسی، در نهایت قضاوت شایسته را تأمین می‌کند. قانون آیین دادرسی مدنی ایران در مورد قابلیت شکایت از ایراد نپذیرفتن امر مرتبط، دارای کاستی است، اما در فرانسه این ایراد همانند قرار نبود صلاحیت، قابل شکایت است.

**واژگان کلیدی:** ارتباط کامل، ارتباط کافی، ارتباط ساده، ایراد امر مرتبط، اداره شایسته جریان دادرسی.

## مقدمه

فناوری‌های نظامی هوش مصنوعی پیوسته در حال تکامل و بهبود هستند و ممکن است در مجموعه‌ای از محیط‌های عملیاتی مختلف مفید واقع شوند.<sup>۱</sup> این فناوری‌ها شامل تشخیص الگو، یادگیری ماشین، بینایی رایانه‌ای،<sup>۲</sup> درک زبان طبیعی و تشخیص گفتار است.<sup>۳</sup> این فناوری‌ها برای افزایش توانایی‌های انسان‌ها و ماشین‌ها به کار 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، ترجمه 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 کامپیوتری رقابتی بسیار توانمند است. یک سیستم هوش مصنوعی می‌تواند به ارتش در کشف تقلب در خدمات قراردادی خود، پیش‌بینی زمان خرابی سیستم‌های تسلیحاتی به دلیل مشکلات تعمیر و نگهداری یا توسعه استراتژی‌های برنده در شبیه‌سازی مخاصمه و همچنین تولید پهپادهای پیشرفته جهت تجسس، شناسایی، ارزیابی و از بین بردن هدف تعیین شده کمک کند. همه

۱. برای اطلاعات بیشتر در مورد تأثیر هوش مصنوعی بر آینده 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*, (Elsevier, vol. 6, 2021), p 1.

این برنامه‌ها و موارد دیگر، می‌توانند در عملیات‌های روزمره و مخاصمات بعدی، باعث بالا رفتن ضریب نیرو باشند.<sup>۱</sup>

اگرچه مزیت استفاده از هوش مصنوعی در زمینه 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 ذکر شده برای استفاده از هوش مصنوعی در صنایع نظامی و پایین آوردن هزینه 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 نقلیه 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 پر 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 جدی قوانین بشردوستانه بین‌المللی» می‌گردد، نتواند از زیر بار مسئولیت پاسخگویی شانه خالی کند.<sup>۲</sup> جنبش توقف

۱. ضریب نیرو یا نیروافزا، عامل یا ترکیبی از عواملی که به پرسنل یا سلاح‌ها (یا سایر سخت‌افزارها) توانایی انجام کارهای بزرگتری را می‌دهد که بدون آن میسر نیست.

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

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 اعلام شوند. با این حال قوانین بین‌المللی، دولت‌ها و اشخاص را با استناد به قوانین مخاصمات مسلحانه مسئول می‌داند.<sup>۱</sup>

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 توسعه بین‌المللی ایالات متحده منتشر شد که بر اساس آن، این نهادها به سرعت فرآیندی را برای حذف حضور دیجیتال 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 حمل مجهز به هوش مصنوعی که کار آنها جمع‌آوری داده‌های مربوط به چشم، اثر انگشت، عکس و زندگی‌نامه افراد بود، تکیه داشته‌اند و این اطلاعات جمع‌آوری شده 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.<sup>۲</sup> 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 زمینه نقض حریم خصوصی اطلاعاتی اشخاص و نهادها برای تحقیق در زمینه 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

---

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).

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 متحد، وزرای دفاع و امور خارجه کشورهای می‌توانند بررسی نمایند که آیا می‌توان به کارگیری هوش مصنوعی را با عقد یک معاهده 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 محاصمه 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 پیش‌بینی بودن، خطراتی را متوجه غیرنظامیان می‌نماید و طبق حقوق بشردوستانه بین‌المللی، مسئولیت قانونی سربازان طرف محاصمه 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، کمیته 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 بین‌الملل بشردوستانه و خطرات ناشی از پیامدهای نامطلوب انسانی بر افراد تحت حمایت دارد.<sup>۱</sup>

در سال‌های اخیر کمیته بین‌المللی صلیب سرخ بر «کنترل و ارزیابی انسانی» به‌عنوان یک مؤلفه 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. کمیته بین‌المللی صلیب سرخ به مواضع کشورهای عضو کنوانسیون در مورد ممنوعیت یا محدودیت به کارگیری برخی سلاح‌های متعارف که ممکن است بیش از حد خطرناک یا دارای اثرات نامشخص باشد،<sup>۲</sup> استناد می‌کند که طبق آن کشورهای عضو کنوانسیون مزبور به رسمیت 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.

کمیته بین‌المللی صلیب سرخ تأکید می‌کند که به‌هنگام 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

---

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.



ارزیابی انسانی است»<sup>۱</sup>. کشورها نیز جهت تنظیم قواعد هوش مصنوعی در زمان مخاصمات 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 تصمیم‌گیری‌ها 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.<sup>۲</sup> این ماده مقرر می‌دارد که کشورهای متعاقد «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 قاعده دیگر حقوق بین‌الملل که برای طرف‌های متعاقد قابل اعمال است، ممنوع شده است یا خیر»<sup>۳</sup> ماده مذکور، دولت‌ها را مکلف می‌دارد تا ماهیت قانونی و غیرقانونی سلاح‌ها، ابزار یا روش‌های نوین جنگی را با توجه به مقررات پروتکل اول الحاقی و سایر قواعد حقوق بین‌الملل تعیین کنند؛<sup>۴</sup> لذا کلیه مقررات انسان‌محور با موضوع هوش مصنوعی باید حول محور حقوق بشر و قوانین حقوق بشردوستانه تنظیم شوند.<sup>۵</sup>

1. International Committee of the Red Cross, "Artificial intelligence and machine learning in armed conflict: A human-centered approach", (June 6, 2019) p 7-8, <https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-humancentred-approach>

2. 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>.

نامپسون 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.

3. 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

۴. شریفی طراز کوهی، حسین؛ برمکی، جعفر، «چالش‌های حقوقی قابلیت فضای سایبری در پروتوکل یکم الحاقی ۱۹۷۷»، مجله حقوقی بین‌المللی، ش ۶۲، (۱۳۹۹) ص ۱۲۶.

۵. 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

از دیگر چالش‌های حقوق بشردوستانه در موضوع هوش مصنوعی 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 مخاصمه 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<sup>۱</sup> و قتل عام اقلیت مسلمان آشکار می‌سازند.

اطلاعات نادرست و سخنان نفرت‌انگیز و «واقعیت‌های نادرست جدید» که از طریق «جعل عمیق»<sup>۲</sup>، 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.<sup>۳</sup>

در شرایط مخاصمه مسلحانه 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 جبهه مخاصمه مسلحانه را می‌دهد.

---

خود کمیته‌هایی جهت ارزیابی سلاح‌ها، ابزارها و روش‌های نوین جنگی ایجاد نموده‌اند. با این حال تا کنون، تعداد کمی، اگر وجود داشته باشند، جرأت کرده‌اند به بررسی واقعی شیوه اعمال رژیم‌های حقوق بشر خاص در حقوق بین‌الملل بشردوستانه یا قدرت آن‌ها برای محدود کردن شیوه‌های خاص طراحی، توسعه، استقرار و به‌کارگیری هوش مصنوعی پردازند.

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](http://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.

در جریان مخاصمات مسلحانه و آشوب‌های خیابانی، شرکت‌های بزرگ فناوری با استفاده 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. در همین راستا، کمیته بین‌المللی صلیب سرخ می‌تواند با بسط مفاهیم حقوق بشردوستانه به هوش مصنوعی، نقش مهمی در تحول حقوق دیجیتال به نفع جمعیت درگیر در یک مخاصمه ایفا نمایند.

## ۲. هوش مصنوعی نظامی و حقوق بشر

فناوری‌های هوش مصنوعی منعکس‌کننده 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.<sup>۲</sup> 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، حق حفظ حریم خصوصی است. در گزارش کمیساری عالی حقوق بشر 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

---

۱. شریفی طراز کوهی، 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.

با یا بدون دیگران، عاری از مداخله دولت یا مداخله بی جا توسط سایر افراد ناخوانده، داشته باشند. این فضای خصوصی با گسترش به اینترنت، آنچه به عنوان «حریم خصوصی اطلاعاتی» شناخته می شود را دربر خواهد گرفت.<sup>۱</sup>

نهادهای معاهداتی حقوق بشر و دادگاههای منطقه‌ای نیز رویه قضایی غنی پیرامون مفهوم حریم خصوصی اطلاعاتی تدوین کرده‌اند تا در مواجهه با محیط تکنولوژیک در حال تغییر، معنای در حال تحول حق تاریخی حفظ حریم خصوصی را مقرر نمایند. این معنا اکنون به یک حق مرتبط، یعنی حق 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 می دهد تا اثرات خارجی منفی هوش مصنوعی به کار 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 مطرح نظر قرار داده است؛<sup>۲</sup> بنابراین کاربرد آن می تواند یک دولت را ملزم نماید تا در طراحی و آموزش الگوریتم‌های پیش‌بینی کننده 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 می تواند راه‌حلی جهت محدودیت آن از طریق اصولی همچون مشروعیت، ضرورت<sup>۳</sup> و تناسب، تعیین سقف برای ذخیره‌سازی داده‌ها<sup>۴</sup> و محدودیت ذخیره‌سازی<sup>۵</sup> 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 داده شخصی یا داده‌های مجازی در حال پردازش قابل اعمال است، اما برای داده‌های شخصی که ناشناخته اند و نمی توان آنها را مجدداً با موضوع داده‌ای خاص مرتبط نمود، اعمال نمی گردد.

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 بشر دوستانه در مورد قوانین خاص 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 خاصی که توسط قوانین دیگر مورد توجه قرار گرفته است، ساکت باشند. به‌عنوان مثال، حق 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 بین‌المللی حقوق بشر باید به‌طور خودکار آن «خلاً» را پر کند.<sup>۱</sup>

علاوه‌براین، خلأهای موجود در مخاصمات مسلحانه ممکن است یک حذف عامدانه باشد که منعکس‌کننده واقعیت مخاصمات مسلحانه است؛ لذا نمی‌توان تصور کرد که حقوق بشر بدون تغییر و انعطاف‌پذیری نسبت به شرایط ویژه برخی از مخاصمات اعمال شود؛ بنابراین تحلیل مورد به مورد تعهدات حقوق بشری و حقوق بین‌الملل بشر دوستانه با توجه به ویژگی‌های منحصربه‌فرد هر مخاصمه 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 تفسیری پیچیده با مسئله حل‌نشده اجرای موازی قوانین عرفی و معاهداتی حاکم بر حقوق بشر در زمان مخاصمات مسلحانه ترکیب می‌شود. در همین راستا، مستثنی شدن 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 به عنوان اصل قابلیت تخطی نام گذاری کرده است.<sup>۱</sup> چنین به نظر می رسد که این امر چارچوب قانونی حفاظت از داده ها را با برنامه های هوش مصنوعی توسعه یافته و مورد استفاده در مخاصمات مسلحانه و همچنین هرگونه پردازشی که توسط آژانس های امنیتی و اطلاعاتی انجام می شود، مسدود می کند. در واقع، پیش نویس پیشنهاد شده اخیر در مورد مقررات هوش مصنوعی که توسط اتحادیه اروپا تهیه شده است، به صراحت آن «سیستم های هوش مصنوعی را که منحصرأ برای اهداف نظامی توسعه یافته اند یا مورد استفاده قرار می گیرند»<sup>۲</sup> مستثنی نموده است.

آخرین نگرانی به یکی از بازیگران کلیدی در فضای نظامی هوش مصنوعی، یعنی شرکت های چندملیتی خصوصی ارتباط می یابد. در دیدگاه سنتی، معاهدات حقوق بشری، متضمن تعهدات حقوقی دولت های عضو هستند و به تعهدات سایر بازیگران با شخصیت های حقوقی غیردولتی نمی پردازد. اگرچه دولت ها می توانند مستقیماً تعهداتی را بر شرکت ها تحمیل کنند و از این راه باعث توسعه حقوق بین الملل گردند، اما آن ها تاکنون این کار را نکرده اند. هرچند هنجارهای مربوط به تجارت و حقوق بشر همانند تعهدات معاهداتی الزام آور نیستند، اما اثر حقوقی آنها همانند «حقوق نرم»<sup>۳</sup> است.

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

---

۱. به ضمیمه چهارم گزارش کمیسیون حقوق بین الملل در مورد پنجاه و هشتمین جلسه کاری آن، با موضوع: حفاظت از داده های 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](http://legal.un.org/ilc/documentation/english/reports/a_61_10.pdf).

۲. پیش نویس 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-](https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206)

[lex.europa.eu/legalcontent/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206](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 زمینه 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. با این حال همه اینها در تضاد کامل با ماهیت دقیق، لاینفک و پیچیده تفکر اخلاقی است. حل 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. به این ترتیب با کاربرد روزافزون فناوری‌های نوظهور مانند هوش مصنوعی و سیستم‌های خودمختار، نیاز آشکاری به نسخه به‌روزشده 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، نه تنها 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 استفاده 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 یک‌مخاصمه 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 نحوه استفاده از آنها در چارچوب قواعد حقوق بشر و حقوق بشردوستانه ضروری است.

به این ترتیب، 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»<sup>۱</sup> را دربر می‌گیرد. استفاده از هوش مصنوعی می‌تواند امنیت دیجیتال، 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. مخاصمه مسلحانه یک رویداد غیرعادی است که اعمال و عملکرد قوانین و رویه‌ها را در حد ضرورت تغییر می‌دهد و استفاده غیرمجاز از داده‌های شخصی ارتباط چندانی با غلبه بر قدرت نظامی دشمن ندارد.<sup>۲</sup>

---

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

علاوه بر این، تشدید رقابت تسلیحاتی ابرقدرت‌ها 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 جامعه جهانی، نگرانی فزاینده‌ای در مورد سقوط حقوق و اخلاق ایجاد کرده است؛<sup>۱</sup> بنابراین تنظیم مقررات در زمینه هوش مصنوعی به ویژه در حوزه مخاصمات مسلحانه، اعم از جنگ‌های فیزیکی و سایبری و بازتعریف قواعد حقوق بشر دوستانه و حقوق بشر بین‌المللی متناسب با مسائل حقوق دیجیتال ضروری است.

#### ۴. راهکارهای حفظ حریم خصوصی اطلاعاتی هوش مصنوعی 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 منطقه‌ای 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 قضیه سازمان غیردولتی حریم خصوصی علیه وزیر امور خارجه و مشترک المنافع بریتانیا<sup>۲</sup> اشاره کرد. به عنوان بخشی از آن پرونده، خواهان استدلال نمود که گردآوری گسترده 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 محدوده قوانین اتحادیه اروپا است و برای ادعای خود به بند ۲ ماده ۴ پیمان اتحادیه اروپا استناد کرد که اشعار می‌دارد: «امنیت ملی صرفاً جزء مسئولیت‌های هر کشور عضو باقی می‌ماند». همچنین بند ۳ ماده ۱ دستورالعمل 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...»<sup>۱</sup> 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 عهده 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.»<sup>۲</sup>

دیوان دادگستری اتحادیه اروپا همچنین خاطرنشان ساخت با توجه به اینکه بسیاری از عملیات‌های اطلاعاتی مورد بحث مربوط به دستور وصول و جوه به ارائه‌دهندگان شبکه‌های ارتباط عمومی الکترونیکی می‌باشد، اشتباه است که به‌عنوان یک قاعده 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.<sup>۱</sup>

علاوه بر این، دیوان دادگستری اتحادیه اروپا در حکم شماره ۱/۱۵، پیش‌نویس توافقنامه منعقد بین کانادا و اتحادیه اروپا با موضوع انتقال و پردازش داده‌های مرتبط با ذخیره هویت مسافران<sup>۲</sup> 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 جدی فراملی»<sup>۳</sup> بسیار مهم هستند. دادگاه اروپایی علی‌رغم پیامدهای کیفی 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<sup>۴</sup> 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. به عبارت دیگر، چنانچه اطلاعات به اشتراک گذاشته شده در نهایت برای مقاصد حفاظت از امنیت ملی مورد استفاده قرار گیرند، نمی‌توان این اطلاعات را در زمره اطلاعات طبقه‌بندی شده 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 طرف حساب 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 متضمن 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<sup>۱</sup> 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. به این ترتیب، با گذشت زمان، هرچه کسب و کارهای بیشتری برای بهره‌مندی از مزایای اقتصادی چنین تعریفی با مقررات عمومی حفاظت از داده اتحادیه اروپا سازگار می‌شوند، ممکن است این مقررات (درست یا نادرست) به‌عنوان یک استاندارد بین‌المللی تلقی شوند. از این مقررات می‌توان به‌عنوان نقطه 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 حق 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 مقوله 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 برنامه 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<sup>۱</sup> اعتراض کردند. گوگل در نهایت به دلیل اقدامات کارمندان به کار خود در پروژه «میون»<sup>۲</sup> پنتاگون که از الگوریتم‌های هوش مصنوعی برای شناسایی هسته‌های مقاومت در عراق و سوریه استفاده می‌کرد، پایان داد.<sup>۳</sup> با وجود این، در سال ۲۰۲۰، گوگل قراردادی جدید با واحد نوآوری دفاعی پنتاگون در زمینه امنیت و مدیریت آپ‌ها امضا کرد.<sup>۴</sup> به این ترتیب یک دستورالعمل حقوق بشر بین‌المللی در مورد مسابقه تسلیحاتی هوش مصنوعی می‌تواند متضمن استراتژی‌هایی جهت توانمندسازی و تقویت نقش کارکنان در اساسنامه یک شرکت باشد. به عنوان 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 به وسیله «ترویج تغییر در ساختار و هنجارهای شرکت توانمند ساخت»<sup>۵</sup>.

سومین راهکار پیشنهادی، ترویج قوانین رسمی و غیررسمی 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 آینده 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", New York 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 و مناطق خالی از سکنه را بررسی کنند و به طور 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 پهباداها برای کسب اطلاعات عملی می‌پردازند، خودکار کند و به طور بالقوه به تحلیلگران آزادی عمل بیشتری می‌داد تا بر اساس داده‌ها تصمیمات کارآمدتر و به موقع‌تری 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 توسعه پیش‌بینی‌نشده فناوری را پوشش دهند. در این زمینه، گسترش سریع سیستم‌های هوش مصنوعی، افزایش چارچوب‌های اخلاقی برای هدایت نمودن توسعه و نحوه استفاده از این فناوری‌ها را تسریع کرده است و اینها نتیجه تلاش دولت‌ها، صنایع، مؤسسات دانشگاهی، سازمان‌های بین‌المللی و سازمان‌های غیردولتی می‌باشد. مرکز اینترنت و جامعه برکمن کلاین، محتوای ۳۶ سند برجسته «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، مسئولیت‌پذیری حرفه‌ای و ارتقای ارزش‌های انسانی هستند.<sup>۱</sup>

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 زمینه 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، جامعه حقوق بشر به حقوق دیجیتال 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 یک سو 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 نظامی تحت نظارت هوش مصنوعی در صورت سکوت قواعد حقوق بشردوستانه و حقوق بشر بین‌المللی، آلودگی داده‌ها و در نتیجه از بین رفتن امنیت دیجیتال، فیزیکی، سیاسی و بصیرت جامعه و مخدوش شدن حق بنیادین کرامت انسانی است. رقابت کشورها در استفاده از هوش مصنوعی جهت برهم 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 مباحثه 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 زمینه هوش مصنوعی در اساسنامه شرکت‌های خصوصی گنجانده شود. توانمندسازی کارکنان به‌عنوان بخشی از اختیارات شرکت‌ها از مواردی است که می‌تواند استفاده 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 کمیته بین‌المللی صلیب سرخ و نهادهای بین‌المللی می‌تواند حقوق دیجیتال را تحت پوشش قواعد حقوق بشر بین‌المللی و حقوق بشردوستانه قرار دهد. با وجود این، هر چند 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 زمینه 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 طراز کوهی، 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*, (Elsevier, 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", *New York 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](http://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](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).

### Translated 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:** فتحي، بديع. (۱۴۰۲). ايرادِ امر مرتبط در آيين دادرسي مدني ايران و فرانسه، پژوهش

حقوق خصوصي، ۱۲(۴۵)، ۹-۳۵. doi: 10.22054/jplr.2024.75175.2778



Private Law Research is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.