Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

حقوق جزای بین‌الملل و تهدیدات جدید هوش مصنوعی: راهکارها و رویکردها

هدیه افروزی — دانشجوی کارشناسی ارشد حقوق کیفری و جرم‌شناسی واحد لاهیجان ، دانشگاه آزاد اسلامی،لاهیجان، ایران

هایده شیرزاد راجعونی — دانشجوی کارشناسی ارشد حقوق کیفری و جرم‌شناسی واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران

دکتر امیررضا محمودی — استادیار، گروه حقوق، واحد لاهیجان،دانشگاه آزاد اسلامی، لاهیجان، ایران

فصلنامه علمی فقه و حقوق نوین

Print ISSN: 2717- 1469
Online ISSN: 2717 – 1477

ISC.SID.NOORMAGZ.MAGIRAN
GOOGLESCHOLAR.ENSANI
www.jaml .ir

سال ۱۴۰۴، سال ششم، شماره ۲۵،
صفحات ۲۰-۱

چکیده

در دهه‌های اخیر، ظهور هوش مصنوعی **(AI)** تحولات چشمگیری در عرصه‌های گوناگون حقوقی، به‌ویژه حقوق جزای بین‌الملل، به‌وجود آورده است. این فناوری نوین و پیچیده با برخورداری از قابلیت‌هایی همچون پیش‌بینی جرائم، تحلیل دقیق الگوهای رفتاری، و تسهیل فرآیند تصمیم‌گیری قضایی، ظرفیت آن را دارد که روندهای قضایی و قانونی را به‌طور قابل‌توجهی بهینه و کارآمد سازد. با این حال، ورود گسترده هوش مصنوعی به نظام عدالت کیفری، با چالش‌ها و تهدیدهایی جدی نسبت به اصول بنیادین حقوق بشر و عدالت همراه است؛ از جمله تبعیض‌های نژادی و اجتماعی، نقض گسترده حریم خصوصی، و ابهام جدی در تعیین دقیق مسئولیت کیفری. مقاله حاضر با رویکردی تحلیلی و انتقادی، به بررسی تهدیدات نوظهور ناشی از کاربرد هوش مصنوعی در بستر حقوق جزای بین‌الملل پرداخته و راهکارهایی مؤثر برای مواجهه با این چالش‌ها ارائه می‌دهد. در پایان نیز، نویسنده پیشنهادهایی عملی و اجرایی جهت تدوین چارچوب‌های قانونی نوین به‌منظور تضمین عدالت، ارتقای شفافیت و صیانت از حقوق بنیادین انسان در عصر فناوری هوشمند و تحول‌گرا مطرح می‌سازد.

واژگان کلیدی: هوش مصنوعی، حقوق جزای بین‌الملل، مسئولیت کیفری، عدالت کیفری، تبعیض الگوریتمی

طبقه‌بندی JEL: فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

International Criminal Law and New Threats of Artificial Intelligence: Solutions and Approaches

Scientific Journal of Modern Jurisprudence and Law

Print ISSN: 2717- 1469
Online ISSN: 2717 - 1477

Profile in ISC,SID, Noormags, Magiran, Ensani, GoogleScholar
www.jaml .ir

Year 2025و Sixth year ,Issue 25

Pages 1-20

Hedeya Afrouzi	Master's student in Criminal Law and Criminology, Lahijan Branch, Islamic Azad University, Lahijan, Iran
Haydeh Shirzad Rajyouni	Master's student in Criminal Law and Criminology, Lahijan Branch, Islamic Azad University, Lahijan, Iran
Dr. Amirreza Mahmoudi	Assistant Professor, Law Department, Lahijan Branch, Islamic Azad University, Lahijan, Iran

Abstract

In recent decades, the emergence of artificial intelligence (AI) has brought about significant changes in various legal fields, especially international criminal law. This new and sophisticated technology, with capabilities such as crime prediction, accurate analysis of behavioral patterns, and facilitation of the judicial decision-making process, has the potential to significantly optimize and streamline judicial and legal processes. However, the widespread introduction of AI into the criminal justice system is accompanied by serious challenges and threats to the fundamental principles of human rights and justice; including racial and social discrimination, widespread violations of privacy, and serious ambiguity in the precise determination of criminal liability. The present article, with an analytical and critical approach, examines the emerging threats arising from the application of AI in the context of international criminal law and offers effective solutions to face these challenges. Finally, the author presents practical and executive suggestions for developing new legal frameworks to ensure justice, promote transparency, and protect fundamental human rights in the era of smart and transformative technology.

Keywords: Artificial Intelligence, International Criminal Law, Criminal Liability, Criminal Justice, Algorithmic Discrimination

JEL Classification: **Jurisprudence - Law - Criminal and Criminology - International Law - Private Law**

مقدمه

در دنیای امروز، هوش مصنوعی به یکی از مهم‌ترین و پرشتاب‌ترین پیشرفت‌های فناورانه تبدیل شده است که کاربرد گسترده‌ای در حوزه‌های مختلف، از جمله صنعت، پزشکی، آموزش و به‌ویژه حقوق یافته است. به‌طور خاص، در حوزه حقوق جزای بین‌الملل، ظهور و گسترش این فناوری، تغییرات عمده‌ای را به دنبال داشته است. سیستم‌های هوش مصنوعی به‌تدریج جایگزین روش‌های سنتی در فرآیندهای قضائی و پلیسی شده‌اند و توانسته‌اند با سرعت و دقت بیشتر، داده‌ها را تحلیل کرده، الگوهای رفتاری مجرمانه را شناسایی کرده و وقوع جرائم را پیش‌بینی نمایند. بنابراین، به نظر می‌رسد هوش مصنوعی می‌تواند نقش مهمی در ارتقای کارایی، دقت و سرعت فرآیندهای قضائی و اجرای عدالت در سطح جهانی ایفا کند.

در عین حال، با وجود ظرفیت‌های قابل توجه این فناوری در بهبود نظام‌های حقوقی و قضائی، بهره‌گیری از هوش مصنوعی در حوزه حقوق جزای بین‌الملل با چالش‌ها و تهدیدات نوظهوری مواجه است. یکی از اصلی‌ترین نگرانی‌ها در این زمینه، موضوع مسئولیت کیفری است؛ چرا که در صورت ارتکاب جرم توسط سامانه‌های هوش مصنوعی، این پرسش مطرح می‌شود که چه کسی باید پاسخگو باشد؟ آیا مسئولیت متوجه طراحان و توسعه‌دهندگان این فناوری است یا این‌که خود سیستم‌های هوش مصنوعی باید به نحوی مسئول شناخته شوند؟ افزون بر این، تهدیداتی نظیر نقض حریم خصوصی افراد، تبعیض‌های نژادی و اجتماعی در تحلیل داده‌ها و تصمیم‌گیری‌های خودکار، و همچنین خطراتی که متوجه استقلال و بی‌طرفی قضائی است، از جمله چالش‌های جدی ناشی از استفاده گسترده از هوش مصنوعی در عرصه‌های بین‌المللی به شمار می‌آیند.

هوش مصنوعی می‌تواند به‌طور خاص در زمینه‌هایی مانند پیش‌بینی رفتار مجرمانه، شناسایی جرائم سازمان‌یافته، و تحلیل سریع داده‌های جمع‌آوری شده از سوی نیروهای پلیس، ابزارهایی کارآمد و مفید ارائه دهد. به‌عنوان مثال، به‌کارگیری الگوریتم‌های پیشرفته برای شبیه‌سازی و تحلیل الگوهای جرائم، می‌تواند وقوع جرم در مناطق خاص را پیش‌بینی کرده و در نتیجه به ارتقای امنیت عمومی و پیشگیری از جرائم در سطح جهانی کمک نماید (عباسی کلیمانی، ۱۴۰۲، ۵). با این حال، همین فناوری‌ها می‌توانند زمینه‌ساز نقض جدی حقوق بشر و حریم خصوصی شوند؛ به‌ویژه در شرایطی که داده‌های افراد و گروه‌ها بدون رضایت یا آگاهی کافی پردازش شوند و در نهایت، تصمیمات قضائی بر مبنای اطلاعات ناقص یا سوگیر اتخاذ گردند.

این چالش‌ها، نیازمند بازنگری در قوانین و مقررات موجود در حوزه حقوق جزای بین‌الملل است. مقررات فعلی که بر پایه مسئولیت فردی و عینی طراحی شده‌اند، ممکن است پاسخ‌گوی چالش‌هایی که از ظهور هوش مصنوعی در این حوزه نشأت می‌گیرند، نباشند. به‌ویژه در سطح بین‌المللی، مسائلی همچون فقدان هماهنگی میان نظام‌های حقوقی کشورها و نبود مقررات جامع و یکپارچه برای تنظیم استفاده از هوش مصنوعی در فرآیندهای قضائی و پلیسی، نیازمند توجه و بررسی جدی هستند (پور قصاب امیری و علوی‌تبار، ۱۴۰۳، ۲۰۳).

در این مقاله، هدف اصلی بررسی تأثیرات هوش مصنوعی بر حقوق جزای بین‌الملل و چالش‌های ناشی از آن است. ابتدا به

تهدیدات جدیدی که این فناوری در حوزه حقوق جزا ایجاد کرده است، پرداخته می‌شود. سپس با تحلیل رویکردها و راهکارهای موجود، به بررسی راه‌حل‌های قانونی و فنی مقابله با این چالش‌ها خواهیم پرداخت. در نهایت، پیشنهاداتی برای تدوین قوانین و مقررات جدید در سطح بین‌المللی ارائه خواهد شد تا ضمن استفاده مؤثر از ظرفیت‌های هوش مصنوعی، تهدیدات موجود نیز کنترل گردد و عدالت کیفری تقویت شود.

با گسترش روزافزون کاربردهای هوش مصنوعی در عرصه‌های مختلف اجتماعی و حقوقی، ادبیات علمی پیرامون تأثیرات این فناوری بر نظام عدالت کیفری ــ به‌ویژه در سطح بین‌المللی ــ رشد قابل توجهی داشته است. این پژوهش‌ها عمدتاً در سه محور اصلی متمرکز بوده‌اند: سوگیری‌های الگوریتمی و تهدید عدالت کیفری، مسئولیت حقوقی در قبال عملکرد سامانه‌های خودمختار، و نقض حریم خصوصی و آزادی‌های فردی. در سطح جهانی، پژوهش Angwin ، Larson، Mattu و Kirchner (2016) یکی از نخستین مطالعاتی بود که تبعیض نژادی در الگوریتم‌های پیش‌بینی خطر، مانند سیستم COMPAS در ایالات متحده، را افشا کرد. این مطالعه نشان داد که این سیستم، متهمان سیاه‌پوست را حتی در صورت نداشتن سابقه کیفری، در گروه‌های پرخطر دسته‌بندی می‌کرد. این یافته‌ها موجب شد تا توجه جهانی به سوگیری‌های موجود در داده‌ها و الگوریتم‌های قضائی جلب شود.

Zarsky (2016) و Binns (2018) نیز با تمرکز بر ضرورت شفافیت و پاسخ‌گویی در الگوریتم‌ها، چالش‌های حقوقی تصمیم‌گیری‌های خودکار را ــ به‌ویژه در حوزه‌هایی که حقوق بنیادین افراد در معرض خطر قرار می‌گیرد ــ مورد بحث قرار دادند. در حوزه سیاست‌گذاری، Gray و همکاران (۲۰۲۳) در گزارشی برای سازمان ملل، بر ضرورت همکاری‌های بین‌المللی برای تنظیم مقررات مربوط به کاربرد هوش مصنوعی در نظام‌های قضائی تأکید کردند و خواستار ایجاد چارچوب‌های جهانی برای تضمین عدالت، شفافیت و حفاظت از حقوق بشر در استفاده‌های قضائی از این فناوری شدند. در همین راستا، اتحادیه اروپا با تصویب قانون جامع AI Act در سال ۲۰۲۴، نخستین چارچوب حقوقی جامع را برای دسته‌بندی و کنترل ریسک‌های هوش مصنوعی ــ به‌ویژه در حوزه‌هایی با ریسک بالا مانند دادرسی کیفری ــ تدوین کرد (European Commission, 2024). بر اساس این قانون، الگوریتم‌های مورد استفاده در پیش‌بینی جرم یا تعیین مجازات، مشمول الزامات سخت‌گیرانه شفافیت و ارزیابی ریسک شده‌اند.

در ایران، پژوهش شیخوند و همکاران (۱۴۰۲) با تأکید بر تمایز میان «تصمیم‌سازی» و «تصمیم‌گیری» در فرآیندهای قضائی مبتنی بر هوش مصنوعی، نسبت به کاهش نقش قاضی در برابر تحلیل‌های الگوریتمی هشدار داده و بر لزوم حفظ استقلال قاضی تأکید کرده‌اند. همچنین، حسینی، واحدیاریجان و یزدانی (۱۴۰۳) با رویکردی فقهی، مسئولیت مدنی ناشی از عملکرد سامانه‌های هوشمند را بررسی کرده و استدلال نموده‌اند که در نبود شخصیت حقوقی برای این سامانه‌ها، مسئولیت متوجه طراحان و بهره‌برداران آن‌ها خواهد بود. از سوی دیگر، سوشینا و سوبنین (۱۴۰۲) در یک مطالعه تطبیقی، نشان داده‌اند که نبود تنوع در داده‌های آموزشی می‌تواند به بازتولید تبعیض‌های اجتماعی و قومی در فرآیندهای قضائی منجر شود. پیشرفت فناوری‌های نوین الکترونیکی و ارتباطی، دگرگونی‌های گسترده‌ای در تمامی

ابعاد زندگی بشر به‌وجود آورده است و حوزه حقوق جزا نیز از این تحولات بی‌نصیب نمانده است. یکی از مهم‌ترین تأثیرات تکنولوژی بر حقوق کیفری، فراهم آوردن زمینه‌های جدید برای ارتکاب جرم توسط بزهکاران است که در پی آن، افق‌های نوینی برای حمایت کیفری و ایجاد مسئولیت کیفری شکل گرفته است. نخستین گام در مقابله حقوقی با این دسته از جرایم، جرم‌انگاری رفتارهای مجرمانه بوده است (رضوی‌فرد و موسوی، ۱۳۹۵، ۲). در خصوص تعریف جرایم رایانه‌ای، قانون‌گذار ایران تعریف جامع و کلی ارائه نداده و صرفاً به تعیین مصادیق آن بسنده کرده است. این در حالی است که پلیس فدرال آمریکا، جرم رایانه‌ای را هر رفتاری تعریف می‌کند که در انجام آن از رایانه بهره گرفته شده باشد. در حال حاضر، این دیدگاه رایج است که هر جرمی که در فرایند ارتکاب آن به نوعی از دانش و فناوری رایانه‌ای استفاده شود، در زمره جرایم رایانه‌ای قرار می‌گیرد. این تعریف «دانش‌محور» بر نقش دانش تخصصی در ارتکاب این جرایم تأکید دارد، چراکه ممکن است ارتکاب برخی از این جرایم حتی بدون به‌کارگیری مستقیم رایانه نیز صورت گیرد، برای مثال با بهره‌گیری از امواج الکترومغناطیسی (رضوی‌فرد و موسوی، ۱۳۹۵، ۷). در ایران، سابقه قانون‌گذاری در زمینه جرایم رایانه‌ای به سال ۱۳۸۸ بازمی‌گردد. کلیات لایحه قانون جرائم رایانه‌ای در تاریخ ۲۷ آبان ۱۳۸۷ به تصویب مجلس شورای اسلامی رسید و پس از رفع ایرادات شورای نگهبان، در تاریخ ۷ تیر ۱۳۸۸ به تأیید نهایی آن شورا رسید. این جرم‌انگاری در ایران، هم‌راستا با پیشرفت‌های جهانی در عرصه فناوری اطلاعات و با تأثیرپذیری از تجربه کشورهایی چون ایالات متحده آمریکا که از پیشگامان این حوزه محسوب می‌شود، انجام پذیرفت (رضوی‌فرد و موسوی، ۱۳۹۵، ۶).

با وجود این تلاش‌های علمی، بررسی پیشینه پژوهش‌ها نشان می‌دهد که همچنان خلأ قابل توجهی در مطالعات جامع وجود دارد که بتواند به‌طور هم‌زمان به ابعاد کیفری، فنی، اخلاقی و بین‌المللی چالش‌های ناشی از هوش مصنوعی پرداخته و راهکارهایی عملی و متناسب با اصول حقوق جزای بین‌الملل ارائه دهد. همچنین، نبود یک چارچوب نظارتی منسجم در سطح بین‌المللی و فقدان نظامی برای تعیین مسئولیت کیفری متناسب با رفتارهای خودمختار سامانه‌های هوشمند، بیانگر ضرورت فوری برای تدوین مقررات نوین در این زمینه است.

الف. تأثیرات هوش مصنوعی بر حقوق جزای بین‌الملل

هوش مصنوعی (AI) به‌عنوان یکی از پیشرفته‌ترین دستاوردهای فناوری در قرن بیست‌ویکم، با توانایی‌های بی‌سابقه‌ای در تحلیل داده‌ها، پیش‌بینی رفتارهای انسانی و پردازش اطلاعات، توانسته است در بسیاری از حوزه‌ها ــ از جمله پزشکی، صنعت، آموزش، و به‌ویژه حقوق جزا ــ تحولات چشمگیری ایجاد کند. در زمینه حقوق جزای بین‌الملل، این فناوری به‌طور فزاینده‌ای در فرآیندهای گوناگون، از جمله پیش‌بینی جرائم، شناسایی الگوهای مجرمانه، تجزیه‌وتحلیل داده‌ها و حتی مراحل قضائی به کار گرفته می‌شود. استفاده گسترده از هوش مصنوعی می‌تواند به بهبود کارایی و سرعت سیستم‌های قضائی کمک شایانی کند، اما در عین حال چالش‌های جدی‌ای برای حقوق بشر، عدالت کیفری و نظم حقوقی ایجاد می‌کند.

۱.پیش‌بینی جرائم و تجزیه‌وتحلیل داده‌ها

یکی از مهم‌ترین کاربردهای هوش مصنوعی در حقوق جزای بین‌الملل، بهره‌گیری از الگوریتم‌های پیش‌بینی

جرم است. این الگوریتم‌ها با پردازش حجم عظیمی از داده‌ها ــ از جمله سوابق پلیسی، تاریخچه جنایی و اطلاعات اجتماعی ــ می‌توانند الگوهای رفتاری مجرمانه را شبیه‌سازی کرده و بر این اساس، پیش‌بینی‌هایی درباره احتمال وقوع جرائم در آینده ارائه دهند. این پیش‌بینی‌ها به مقامات قانونی امکان می‌دهد تا پیش از وقوع جرم، مناطق پرخطر را شناسایی کرده و اقدامات پیشگیرانه مؤثری اتخاذ نمایند. به‌عنوان نمونه، در ایالات متحده، پلیس برخی شهرها از الگوریتم‌هایی مانند «پرسیتی » (PredPol)استفاده کرده‌اند که بر پایه داده‌های تاریخی، مناطقی را که احتمال وقوع جرم در آن‌ها بیشتر است، شناسایی کرده و منابع پلیسی را به آن مناطق اختصاص می‌دهد. این الگوریتم‌ها مستقیماً بر نحوه تخصیص منابع و چگونگی عملکرد نیروهای پلیس تأثیر می‌گذارند.(Binns, 2018, 544)

با این حال، استفاده از چنین الگوریتم‌هایی می‌تواند تهدیداتی جدی برای عدالت و حقوق بشر به همراه داشته باشد. با گسترش هوش مصنوعی، شاهد ظهور شیوه‌های نوینی از ارتکاب جرائم سایبری و اقتصادی هستیم. هوش مصنوعی می‌تواند در طراحی کلاهبرداری‌های پیچیده در فضای مجازی، جعل هویت‌های دیجیتال، یا حتی دستکاری الگوهای بازار به‌کار رود. این تحولات نشان می‌دهد که جرایم فناوری‌محور نه‌تنها پیچیده‌تر شده‌اند، بلکه به‌سرعت در حال فراتر رفتن از ظرفیت‌های پاسخ‌دهی ساختارهای قانونی فعلی هستند (نعمتی، گلچین‌راد و صادقیان لمراسکی، ۲۰۲۵، ۳۰۳). یکی از مهم‌ترین خطرات در این زمینه، وجود سوگیری‌های نژادی و اجتماعی در داده‌هاست. بسیاری از این الگوریتم‌ها بر مبنای داده‌های تاریخی طراحی می‌شوند که ممکن است خود متضمن تبعیض‌های نژادی یا اجتماعی باشند. به بیان دیگر، اگر داده‌های پیشین حاوی رفتارهای تبعیض‌آمیز یا نژادپرستانه در فرآیند دستگیری و پیگرد قانونی بوده باشند، این سوگیری‌ها می‌توانند به‌طور غیرمستقیم در الگوریتم‌ها بازتولید شده و در نهایت منجر به هدف‌گیری ناعادلانه گروه‌های خاصی از جامعه شوند (Angwin et al., 2016, 1). برای نمونه، برخی پژوهش‌ها نشان داده‌اند که الگوریتم‌های پیش‌بینی جرم در ایالات متحده افراد سیاه‌پوست را به‌طور نامتناسب و ناعادلانه‌تری به عنوان افراد پرخطر شناسایی می‌کنند.

۲.شفافیت و مسئولیت‌پذیری الگوریتم‌ها

یکی دیگر از چالش‌های بنیادی هوش مصنوعی در حقوق جزای بین‌الملل، مسأله شفافیت و مسئولیت‌پذیری است. الگوریتم‌های هوش مصنوعی اغلب به‌صورت «جعبه سیاه» عمل می‌کنند؛ بدین معنا که تصمیمات آن‌ها برای انسان‌ها به‌راحتی قابل درک نیست. این امر در حوزه‌های قضائی، به‌ویژه زمانی که الگوریتم‌ها در تعیین مجازات یا پیش‌بینی وضعیت مجرمان مورد استفاده قرار می‌گیرند، می‌تواند بسیار مخاطره‌آمیز باشد. به‌عنوان مثال، اگر قاضی به جای تحلیل انسانی، برای صدور حکم به تصمیمات الگوریتمی تکیه کند، عدم شفافیت و پاسخگویی این سیستم‌ها می‌تواند به صدور احکام ناعادلانه یا غیرقانونی بینجامد (Zarsky, 2016, 119).

این مسئله در حوزه حقوق جزای بین‌الملل پیچیده‌تر می‌شود، چرا که نظام‌های قضائی کشورها از نظر ساختار و الزامات قانونی با یکدیگر تفاوت دارند و استانداردهای مربوط به

شفافیت و پاسخگویی در کاربرد الگوریتم‌ها در سطح جهانی به‌طور منسجم و هماهنگ تدوین نشده‌اند. بنابراین، تدوین دستورالعمل‌ها و قوانین بین‌المللی برای تضمین شفافیت و پاسخگویی سیستم‌های هوش مصنوعی در فرآیندهای قضائی، ضرورتی اجتناب‌ناپذیر است.

۳.نقض حریم خصوصی و آزادی‌های فردی

یکی دیگر از تهدیدات مهم ناشی از کاربرد هوش مصنوعی در حقوق جزای بین‌الملل، نقض حریم خصوصی و آزادی‌های فردی است. به دلیل توانایی‌های گسترده هوش مصنوعی در جمع‌آوری و پردازش حجم عظیمی از داده‌ها، ممکن است اطلاعات حساس افراد ــ از جمله داده‌های خصوصی، مکانی یا مالی ــ بدون رضایت آن‌ها یا به‌صورت غیرقانونی گردآوری و تحلیل شود. این خطر به‌ویژه در زمینه استفاده از سامانه‌های نظارتی مبتنی بر هوش مصنوعی، نظیر شناسایی چهره یا پایش رفتارهای آنلاین، بسیار جدی و نگران‌کننده است(Jouini et al., 2019, 2) . در این میان، توجه به اسناد بین‌المللی حقوق بشر نیز اهمیت ویژه‌ای دارد. این اسناد همچون اعلامیه جهانی حقوق بشر (۱۹۴۸) و میثاق حقوق مدنی و سیاسی (۱۹۶۶) بر اصولی نظیر حق حیات، کرامت ذاتی انسان، عدم تبعیض و حق بر حریم خصوصی تأکید دارند.[۱] این اصول، گرچه در حوزه حقوق بشر تعریف شده‌اند، اما در مواجهه با فناوری‌های نوین مانند هوش مصنوعی، کاملاً قابل اعمال‌اند. برای مثال، اصل «عدم تبعیض» مستقیماً با موضوع سوگیری الگوریتم‌ها و تحلیل داده‌های آموزشی در ارتباط است، و اصل «حریم خصوصی» می‌تواند در برابر جمع‌آوری بی‌ضابطه داده‌های شخصی توسط سیستم‌های هوشمند، سپر حقوقی مهمی فراهم آورد. بنابراین، رعایت مفاد این اسناد بین‌المللی نه‌تنها در چارچوب اخلاقی، بلکه از حیث تعهدات الزام‌آور دولت‌ها در قبال حقوق بنیادین افراد اهمیت دارد. این موضوع به‌ویژه زمانی جدی‌تر می‌شود که سامانه‌های هوش مصنوعی در فرایندهای دادرسی کیفری یا امنیتی وارد شده و نقش تصمیم‌ساز یا حتی تصمیم‌گیرنده پیدا می‌کنند.

در کشورهای مختلف، نحوه نظارت بر داده‌های شخصی و صیانت از حریم خصوصی با یکدیگر تفاوت دارد. به‌عنوان نمونه، در اتحادیه اروپا، مقررات عمومی حفاظت از داده‌ها (GDPR)به‌طور خاص با هدف صیانت از حقوق فردی در برابر تهدیدات ناشی از کاربرد هوش مصنوعی تدوین شده‌اند. هرچند این مقررات به‌طور مستقیم به هوش مصنوعی اشاره ندارند، اما مفاد آن‌ها در بسیاری از کاربردهای این فناوری قابل اعمال و گاه چالش‌برانگیز است. اصول سنتی مانند محدودیت هدف، کمینه‌سازی داده و محدودیت تصمیم‌گیری خودکار، در مواجهه با کاربردهای نوین و گسترده هوش مصنوعی و کلان‌داده‌ها، تحت فشار قرار گرفته‌اند. با این حال، تفسیر و اجرای انعطاف‌پذیر این اصول می‌تواند امکان بهره‌گیری از مزایای هوش مصنوعی را بدون نقض مقررات

[۱] ویکی فقه، «اسناد بین‌المللی حقوق بشر»، بازیابی‌شده در ۱۴۰۴، از :
https://fa.wikifeqh.ir /اسناد_بین‌المللی_حقوق_بشر

حقوقی فراهم آورد. البته باید توجه داشت که این قوانین صرفاً در حوزه جغرافیایی اتحادیه اروپا نافذ هستند و هنوز در سطح جهانی چارچوب‌های حقوقی یکپارچه و روشنی برای حفاظت از حریم خصوصی و آزادی‌های فردی در برابر استفاده از هوش مصنوعی وجود ندارد. افزون بر این، خلأها و ابهامات قانونی در برخی حوزه‌های خاص از کاربرد هوش مصنوعی ممکن است به بروز هزینه‌های حقوقی قابل توجه و کند شدن روند توسعه این فناوری منجر شود. بنابراین، تهیه دستورالعمل‌های روشن و چندسطحی برای تطبیق هوش مصنوعی با مقررات حفاظت از داده، امری ضروری به شمار می‌آید (Sartor & Lagioia, 2020, II-III).

۴ .بازتولید تبعیض نژادی و اجتماعی در الگوریتم‌های کیفری

بهره‌گیری از هوش مصنوعی در فرآیندهای کیفری، به‌ویژه در پیش‌بینی جرم و تحلیل داده‌های رفتاری، می‌تواند به بازتولید تبعیض‌های نژادی، اجتماعی و جنسیتی منجر شود؛ به‌ویژه زمانی که داده‌های آموزشی این الگوریتم‌ها، خود متأثر از نابرابری‌های ساختاری موجود در نظام‌های پلیسی و قضائی باشند. در بسیاری از کشورها، داده‌های تاریخی ثبت‌شده از عملکرد نیروهای پلیس یا دادگاه‌ها، منعکس‌کننده برخوردهای ناعادلانه با اقلیت‌های قومی یا طبقات پایین جامعه هستند. اگر چنین داده‌هایی بدون پالایش و اصلاح وارد سامانه‌های هوشمند شوند، سیستم‌های هوش مصنوعی نیز همان تبعیض‌ها را بازتولید می‌کنند. برای نمونه، نتایج پژوهش‌ها نشان داده‌اند که سامانه‌های پیش‌بینی خطر مانند COMPAS در ایالات متحده، افراد سیاه‌پوست را حتی در صورت نداشتن سابقه کیفری، بیشتر در گروه‌های پرخطر طبقه‌بندی می‌کنند (Larson, Angwin, Mattu , Kirchner, 3,2016). همچنین، عملکرد ناعادلانه برخی سامانه‌های شناسایی چهره در قبال افراد با رنگ پوست تیره نیز گزارش شده است (Frankle , Bedoya, Garvie, 12,2016). چنین نتایجی بیانگر آن است که بدون تدوین استانداردهای نظارتی و اخلاقی برای پالایش داده‌ها و طراحی الگوریتم‌ها، عدالت کیفری هوشمند در معرض آسیب‌های جدی خواهد بود.

ب. تهدیدات جدید و چالش‌های هوش مصنوعی در حقوق جزای بین‌الملل

ورود هوش مصنوعی به عرصه حقوق جزای بین‌الملل، تهدیدات نوظهور و چالش‌هایی را به همراه داشته که مستقیماً اصول بنیادین عدالت کیفری و حقوق بشر را تحت‌تأثیر قرار می‌دهد. این تهدیدات صرفاً جنبه‌های فنی و تکنولوژیکی ندارند، بلکه ابعاد اخلاقی، اجتماعی و حقوقی را نیز دربر می‌گیرند. در ادامه، به مهم‌ترین تهدیدات و چالش‌های ناشی از به‌کارگیری هوش مصنوعی در این حوزه می‌پردازیم (حسینی، واحدیاریجان و یزدانی، ۱۴۰۳: ۳-۵). تهدیدات ناشی از هوش مصنوعی ماهیتی چندلایه دارند و معمولاً آثار آن‌ها از مرزهای فنی فراتر می‌رود. در حوزه‌هایی نظیر تحلیل داده‌های رفتاری، امنیت سایبری و اقتصاد، این تهدیدات می‌توانند به شکل زنجیره‌وار موجب اخلال در ساختارهای قانونی، نقض آزادی‌های فردی و تضعیف نظام عدالت کیفری شوند. همین چندبعدی بودن، ظرفیت مداخله مؤثر را برای نهادهای قضائی و قانون‌گذار دشوار می‌سازد (نعمتی، گلچین‌راد و صادقیان لمراسکی، ۲۰۲۵، ۳۰۶).

۱.مسئولیت کیفری یکی از پیچیده‌ترین چالش‌های حقوقی مرتبط با هوش مصنوعی، ابهام در تعیین

«صاحب اثر» یا «خالق» در مواردی است که هوش مصنوعی به‌تنهایی یا با حداقل مداخله انسانی، اثری را خلق می‌کند. حقوق مالکیت فکری به‌طور سنتی بر مبنای «خلاقیت انسانی» و «اصالت» اثر بنا شده است. اما زمانی که یک الگوریتم، آهنگی می‌سازد یا تابلویی نقاشی می‌کند، سؤال اصلی این است که آیا این اثر دارای «اصالت» و «خلاقیت» به معنای حقوقی آن است و چه کسی باید حقوق ناشی از آن را دریافت کند؟ آیا هوش مصنوعی را می‌توان «خالق» دانست و در صورت لزوم، «مسئول» اقدامات آن شناخت؟ (اسدپور، پهلوان‌زاده و خندانی، ۱۴۰۲، ۵).

در این زمینه، سه رویکرد اصلی برای تعیین تکلیف آفرینش‌های هوش مصنوعی مطرح شده است: نخست، فرض بر این است که انسان برنامه‌نویس یا اپراتور، خالق اصلی است و هوش مصنوعی صرفاً ابزاری در دست او محسوب می‌شود. دوم، قائل شدن به نوعی شخصیت حقوقی جدید برای هوش مصنوعی به دلیل قابلیت‌های خودمختاری و یادگیری آن، که این رویکرد به معنای شناسایی توانایی‌های تصمیم‌گیری مستقل برای AI است و پیامدهای گسترده‌ای در سایر حوزه‌های حقوقی، از جمله مسئولیت کیفری، دارد. سوم، ایجاد یک سیستم حقوقی کاملاً جدید برای آفرینش‌های هوش مصنوعی که نه به انسان و نه به هوش مصنوعی به‌تنهایی، بلکه به یک نهاد ترکیبی یا صندوق اختصاصی، حقوق را واگذار کند. در نهایت، فقدان چارچوب‌های حقوقی مناسب و یکپارچه در سطح بین‌المللی برای پاسخ‌گویی به این سؤالات، نیازمند همکاری‌های گسترده برای تدوین اصول و مقررات جدید است (همان، ۶). مسئولیت کیفری یکی از اساسی‌ترین چالش‌های حقوقی در مواجهه با فناوری هوش مصنوعی، مسئله‌ی تعیین مسئولیت کیفری است. در سیستم‌های سنتی، مسئولیت کیفری همواره متوجه فردی بود که مرتکب جرم می‌شد؛ اما با ظهور سامانه‌های هوشمند و خودمختار، این پرسش مطرح می‌شود که در صورت وقوع جرم توسط یک سیستم هوش مصنوعی، چه کسی باید پاسخگو باشد؟ آیا همچنان افراد (مانند توسعه‌دهندگان یا کاربران) باید مسئول شناخته شوند یا اینکه به علت توان تصمیم‌گیری مستقل این سامانه‌ها، خود آن‌ها باید مشمول مسئولیت حقوقی قرار گیرند؟ (حسینی، واحدیاریجان و یزدانی، ۱۴۰۳، ۴-۶). در حقوق ایران، قانون‌گذار در «قانون جرایم رایانه‌ای»، فصل ششم را به موضوع مسئولیت کیفری اختصاص داده است. مهم‌ترین نوآوری این قانون در حوزه مسئولیت کیفری، شناسایی و پذیرش مسئولیت کیفری برای اشخاص حقوقی است. مواد ۲۰ و ۲۱ این قانون به‌صراحت به مسئولیت کیفری اشخاص حقوقی پرداخته‌اند. بر اساس ماده ۲۰، در مواردی که جرایم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن صورت گیرد، شخص حقوقی نیز دارای مسئولیت کیفری خواهد بود. مصادیق این ماده عبارت‌اند از:

الف) زمانی که مدیر شخص حقوقی خود مرتکب جرم رایانه‌ای شود .

ب) زمانی که مدیر دستور ارتکاب جرم را صادر کرده باشد و جرم واقع شود .

ج) زمانی که یکی از کارکنان شخص حقوقی با آگاهی مدیر یا بر اثر اهمال و عدم نظارت او مرتکب جرم رایانه‌ای گردد .

د) زمانی که تمام یا بخشی از فعالیت شخص حقوقی به ارتکاب جرایم رایانه‌ای اختصاص یافته باشد (رضوی‌فرد و موسوی، ۱۳۹۵، ۱۱).

ماده ۲۱ نیز مجازات‌هایی را برای اشخاص حقوقی مجرم در نظر گرفته و مقرر می‌دارد: با در نظر گرفتن شرایط جرم، اوضاع و احوال ارتکاب، میزان درآمد و نتایج حاصل از آن، اشخاص حقوقی مشمول ماده ۲۰، علاوه بر پرداخت سه تا شش برابر حداکثر جزای نقدی مقرر برای جرم، به مجازات‌های زیر محکوم می‌شوند:

الف) اگر حداکثر مجازات جرم ارتکابی تا پنج سال حبس باشد، شخص حقوقی به تعطیلی موقت از یک تا نه ماه محکوم می‌شود و در صورت تکرار، این تعطیلی موقت می‌تواند تا پنج سال ادامه یابد .

ب) اگر حداکثر مجازات جرم بیش از پنج سال حبس باشد، تعطیلی موقت از یک تا سه سال در نظر گرفته می‌شود و در صورت تکرار، شخص حقوقی منحل خواهد شد (رضوی‌فرد و موسوی، ۱۳۹۵، ۱۲).

نکته قابل توجه آن‌که تأکید قانون‌گذار بر مسئولیت کیفری اشخاص حقوقی به معنای نفی یا نادیده گرفتن مسئولیت کیفری اشخاص حقیقی نیست. در تبصره ۲ ماده ۲۰ به‌صراحت آمده است که مسئولیت کیفری شخص حقوقی مانع از مجازات فرد مرتکب نخواهد بود. در واقع، این دو نوع مسئولیت، ریشه‌ای مشترک دارند و هر دو به‌منظور پاسخ‌گویی به نقض جدی تعهداتی که در برابر جامعه وجود دارد، ایجاد می‌شوند (همان، ۱۲).

پیچیدگی این مسئله زمانی بیشتر می‌شود که سامانه‌های هوش مصنوعی به‌طور خودکار و بدون نظارت مستقیم انسان عمل می‌کنند و تصمیماتی می‌گیرند که می‌توانند پیامدهای کیفری جدی داشته باشند. یکی از دشوارترین چالش‌ها، تطبیق مسئولیت کیفری سنتی با رفتارهای خودکار و پیش‌بینی‌ناپذیر سامانه‌های هوشمند است. در نظام کیفری کلاسیک، عناصر روانی چون قصد مجرمانه، علم و اراده، اساس انتساب مسئولیت هستند. اما فناوری‌های نوین ممکن است بدون آگاهی یا نیت انسانی، موجب وقوع رفتارهای مجرمانه شوند؛ ازاین‌رو، چارچوب‌های فعلی حقوق کیفری برای پاسخ‌گویی به این وضعیت کافی به نظر نمی‌رسند و بازنگری جدی می‌طلبند (نعمتی، گلچین‌راد و صادقیان لمراسکی، ۲۰۲۵، ۳۰۷).

برخی صاحب‌نظران بر این باورند که مسئولیت باید متوجه طراحان، برنامه‌نویسان و شرکت‌های توسعه‌دهنده باشد، چراکه آن‌ها داده‌ها و ساختار تصمیم‌گیری این سیستم‌ها را طراحی کرده‌اند. اما اشکال کار اینجاست که حتی این افراد نیز ممکن است قادر به پیش‌بینی رفتار دقیق سیستم در شرایط خاص نباشند (لرکی بختیاری‌نژاد، ۱۴۰۳، ۱۰).

نمونه بارز این مسئله، حادثه‌ی سال ۲۰۱۸ است که طی آن یک خودروی خودران شرکت «اوبر» در آریزونا با یک عابر پیاده برخورد کرد و منجر به مرگ وی شد. این رویداد بحث‌هایی گسترده درباره‌ی تعیین مسئولیت میان طراح، شرکت، راننده پشتیبان و الگوریتم هوش مصنوعی را برانگیخت (طلیات، ۲۰۲۲، ۱۵).

ابهام در نسبت میان تصمیم‌گیری خودکار و مسئولیت حقوقی با پیشرفت سریع فناوری‌های هوشمند، بسیاری از تصمیماتی که پیش‌تر به‌طور کامل در اختیار انسان بودند، اکنون توسط سامانه‌های خودکار اتخاذ می‌شوند. این تحول در ظاهر موجب افزایش دقت، سرعت و کارایی شده، اما در بطن خود پرسشی جدی درباره نسبت بین تصمیم و مسئولیت پدید آورده است. به‌ویژه در حوزه حقوق کیفری، جایی که اساس مسئولیت بر پایه آگاهی، اراده و قصد شکل می‌گیرد، عملکرد هوش مصنوعی می‌تواند این اصول بنیادین را به چالش بکشد.

یکی از مسائل محوری در این زمینه آن است که در صورت بروز خطا یا خسارت ناشی از تصمیم‌گیری الگوریتمی، چه شخص یا نهادی باید پاسخگو باشد؟ آیا می‌توان توسعه‌دهنده، شرکت سازنده یا بهره‌بردار نهایی را مسئول دانست؟ یا باید به‌سوی شناسایی نوعی شخصیت حقوقی محدود برای سامانه‌های هوشمند حرکت کرد؟ این پرسش‌ها وقتی اهمیت بیشتری می‌یابند که بدانیم بسیاری از این سامانه‌ها نه‌تنها بر اساس داده‌های گذشته تصمیم می‌گیرند، بلکه با استفاده از یادگیری ماشینی، رفتارشان ممکن است در طول زمان تغییر کند. از همین رو، پاسخ‌گویی حقوقی در چنین سیستمی صرفاً از مسیر سنتی تقصیر یا قصد قابل حل نیست و نیاز به بازتعریف مسئولیت در بستر فناوری‌های نوین دارد. به بیان دیگر، شکاف موجود میان قدرت تصمیم‌گیری هوش مصنوعی و ساختارهای حقوقی فعلی، یکی از چالش‌های اساسی نظام عدالت کیفری در دهه آینده خواهد بود.

از طرفی، برخی نظریات جدید بر لزوم ایجاد نوعی «شخصیت حقوقی» برای سامانه‌های هوش مصنوعی تأکید دارند تا این سیستم‌ها در برابر تصمیماتشان پاسخگو باشند. اما این رویکرد همچنان در مراحل نظری و آزمایشی قرار دارد و مستلزم تدوین چارچوب‌های حقوقی جدید برای تعریف دقیق مسئولیت قانونی این سامانه‌هاست (صلح‌چی، بیگلربیگی و کینگستون، ۱۴۰۲، ۱۰۹).

۲.نقض حریم خصوصی هوش مصنوعی به دلیل توانایی‌های بالا در تحلیل و پردازش حجم انبوهی از داده‌ها، پتانسیل بالایی در شناسایی الگوهای رفتاری و تحلیل اطلاعات شخصی دارد. این توانایی در شرایطی که بدون اطلاع یا رضایت فرد انجام شود، به یکی از جدی‌ترین تهدیدات حقوق بشر و به‌ویژه حق بر حریم خصوصی تبدیل می‌شود (حسینی، واحدیاریجان و یزدانی، ۱۴۰۳، ۳-۴).

در مواردی مشاهده شده که جمع‌آوری داده‌های رفتاری افراد از شبکه‌های اجتماعی یا فعالیت‌های آنلاین، به‌منظور پیش‌بینی رفتار مجرمانه مورد استفاده قرار می‌گیرد. اگر داده‌های جمع‌آوری شده ناقص، اشتباه یا غیرقانونی باشند، ممکن است به تعقیب افراد بی‌گناه یا برداشت‌های نادرست منجر شود (صوفی و صالح‌نژاد بهرستاقی، ۱۴۰۲، ۵).

در این زمینه، اتحادیه اروپا با وضع مقررات عمومی حفاظت از داده‌ها (GDPR) تلاش کرده تا چارچوب‌های سخت‌گیرانه‌ای برای حفظ حریم خصوصی وضع کند. این قوانین، اگرچه نقاط قوت قابل توجهی دارند، اما تنها در محدوده کشورهای عضو این اتحادیه قابل اجرا هستند. در سطح بین‌المللی، هنوز نظام جامع و هماهنگی برای محافظت از داده‌های شخصی در برابر سوءاستفاده‌های

احتمالی هوش مصنوعی تدوین نشده است (Bygrave, 2017, 21).

۳.بی‌طرفی و عدالت یکی دیگر از چالش‌های جدی، مسئله بی‌طرفی و عدالت در عملکرد الگوریتم‌های هوش مصنوعی است. این الگوریتم‌ها، بسته به داده‌هایی که دریافت می‌کنند، ممکن است دچار سوگیری شوند؛ به‌ویژه در مواقعی که برای پیش‌بینی جرم یا شناسایی مظنونین مورد استفاده قرار می‌گیرند (شیخوند، کردعلیوند، مینایی، آشوری و مهدوی ثابت، ۱۴۰۲، ۱۴۳).

الگوریتم‌هایی مانند «پرسیتی (PredPol)» که در ایالات متحده استفاده می‌شوند، از داده‌های تاریخی برای پیش‌بینی مناطق جرم‌خیز استفاده می‌کنند. اما اگر این داده‌ها حاوی تبعیض‌های نژادی یا طبقاتی باشند، نتایج حاصل نیز احتمالاً دارای همان سوگیری‌ها خواهند بود. این امر به‌طور بالقوه می‌تواند منجر به افزایش دستگیری‌های ناعادلانه علیه اقلیت‌ها و گروه‌های آسیب‌پذیر شود (بینا و حبیبی، ۱۴۰۲، ۲-۳). یافته‌های پژوهش‌های اولیه نظیر مطالعه ProPublica (2016)، از وجود نوعی سوگیری نژادی در الگوریتم‌های پیش‌بینی خطر خبر می‌دادند؛ اما تحلیل اصلی این پیامدها، در ادامه مقاله و در بخش چالش‌های حقوقی مرتبط با بی‌طرفی و تبعیض بررسی خواهد شد.

۴.تبعیض نژادی و اجتماعی هوش مصنوعی، به‌ویژه در فرآیندهای قضائی، ممکن است به بازتولید تبعیض‌های نژادی و اجتماعی موجود در داده‌های آموزشی منجر شود. این امر به‌ویژه زمانی رخ می‌دهد که داده‌های ورودی به الگوریتم‌ها از منابعی باشند که خود دچار نابرابری‌های ساختاری هستند (سوشینا، سوبنین و صادقی، ۱۴۰۲، ۹۵).

به‌عنوان مثال، در بسیاری از کشورها، داده‌های پلیسی و قضائی تاریخی نشان‌دهنده برخوردهای سخت‌گیرانه‌تر با اقلیت‌های قومی و طبقات پایین جامعه است. اگر این داده‌ها بدون بررسی و اصلاح به الگوریتم‌ها داده شوند، سیستم‌های هوش مصنوعی نیز همان تبعیض‌ها را بازتولید می‌کنند.

برای جلوگیری از چنین پیامدهایی، تدوین قوانین و دستورالعمل‌های بین‌المللی جهت پایش عملکرد الگوریتم‌ها، تضمین شفافیت در طراحی و اجرای آن‌ها، و همچنین کنترل کیفیت داده‌های ورودی، کاملاً ضروری است. بدون چنین نظارتی، خطر تحمیل نابرابری‌های ساختاری از سوی فناوری‌هایی که اساساً برای عدالت طراحی شده‌اند، بسیار جدی خواهد بود.

هوش مصنوعی در مخاصمات مسلحانه و پیامدهای کیفری آن در سال‌های اخیر، فناوری هوش مصنوعی نه‌تنها زندگی روزمره بلکه میدان‌های نبرد را نیز دستخوش تغییر کرده است. از سامانه‌های تحلیل‌گر پیشرفته گرفته تا پهپادهای خودکار، ابزارهای هوشمند اکنون می‌توانند تصمیم‌هایی بگیرند که پیش‌تر تنها انسان‌ها قادر به آن بودند. همین تحول موجب شده که مرز میان «تصمیم انسانی» و «رفتار خودکار سیستم» در درگیری‌های مسلحانه کم‌رنگ شود؛ و این پرسش اساسی مطرح گردد که اگر چنین سامانه‌هایی مرتکب خطا یا حتی جنایت جنگی شوند، مسئولیت آن با کیست؟ طراح، فرمانده، اپراتور یا خود سامانه؟ در حقوق بشردوستانه بین‌المللی،

اصولی مانند تناسب، تمایز میان اهداف نظامی و غیرنظامی، و احتیاط در حمله اهمیت بالایی دارند. اما وقتی الگوریتم‌ها به‌جای انسان تصمیم می‌گیرند، تضمین پایبندی به این اصول با چالش‌هایی جدی روبه‌رو می‌شود. به‌ویژه آنکه این سامانه‌ها ممکن است بدون دخالت مستقیم انسان، حمله‌ای را آغاز کنند یا در تحلیل موقعیت دچار اشتباه شوند. در چنین شرایطی، برخی حقوقدانان پیشنهاد داده‌اند تا مفهوم جدیدی از مسئولیت کیفری معرفی شود؛ مفهومی که در آن نه فقط شخص حقیقی، بلکه طراحی، برنامه‌ریزی، و حتی شیوه آموزش داده‌های سامانه نیز در زنجیره مسئولیت در نظر گرفته شود. این رویکرد می‌تواند امکان پاسخ‌گویی را در مواردی فراهم کند که با ساختارهای سنتی حقوق کیفری قابل مدیریت نیستند. در مجموع، ورود هوش مصنوعی به مخاصمات مسلحانه تنها یک تحول فناورانه نیست، بلکه یک آزمون جدی برای نظام مسئولیت کیفری بین‌الملل است. آزمونی که اگر برای آن چارچوب مشخصی تعریف نشود، نه‌تنها عدالت، بلکه امنیت انسانی نیز در خطر قرار خواهد گرفت[1].

پ. راهکارها و رویکردهای مقابله با تهدیدات

برای مقابله مؤثر با تهدیدات ناشی از کاربرد هوش مصنوعی در حوزه حقوق جزای بین‌الملل، ضرورت دارد که نظام‌های حقوقی به‌روز شده و مقررات جدیدی تدوین شوند تا بتوانند امنیت حقوقی، عدالت کیفری و حقوق بشر را تضمین کنند.

در این راستا، راهکارهای زیر از جمله مهم‌ترین پیشنهادها به شمار می‌آیند:

تعیین مسئولیت کیفری هوش مصنوعی یکی از گام‌های اساسی در مدیریت پیامدهای حقوقی هوش مصنوعی، تدوین سازوکاری روشن برای تعیین مسئولیت کیفری در صورت وقوع جرائم مرتبط با این فناوری است. برخی از رویکردهای پیشنهادی بر آن تأکید دارند که طراحان، برنامه‌نویسان و توسعه‌دهندگان سامانه‌های هوش مصنوعی باید در قبال سوءاستفاده‌ها یا پیامدهای ناشی از عملکرد این سیستم‌ها پاسخگو شناخته شوند (کاوه و بارانی، ۱۴۰۳، ۵۸-۵۹). این امر می‌تواند نقش بازدارنده‌ای در برابر طراحی الگوریتم‌هایی داشته باشد که فاقد نظارت کافی یا استانداردهای اخلاقی و حقوقی هستند.

تدوین مقررات دقیق برای حفظ حریم خصوصی از دیگر اقدامات ضروری، تصویب و اجرای قوانینی است که نحوه جمع‌آوری، ذخیره‌سازی و بهره‌برداری از داده‌های شخصی توسط سامانه‌های هوش مصنوعی را به‌شدت کنترل و محدود کنند. این مقررات باید مبتنی بر اصول شفافیت، رضایت آگاهانه و حفظ کرامت انسانی باشند تا از نقض حریم خصوصی افراد جلوگیری شود.

جرایم سایبری به‌عنوان یکی از مهم‌ترین تهدیدات امنیتی در جهان دیجیتال امروز، چالش‌های متعددی را در حوزه‌های اجتماعی، اقتصادی و حقوقی ایجاد کرده‌اند. مقابله مؤثر با این

[1] انجمن ایرانی مطالعات سازمان ملل متحد، «نقش هوش مصنوعی در مخاصمات مسلحانه و پیامدهای حقوقی آن»، منتشرشده در وب‌سایت رسمی انجمن، ۱۴۰۳، قابل بازیابی در : https://unstudies.ir/iauns-forum/نقش-هوش-مصنوعی-در-مخاصمات-مسلحانه-و-پی/ (تاریخ بازدید: ۱۱ تیر ۱۴۰۳).

جرائم مستلزم رویکردی چندوجهی است که از آموزش عمومی گرفته تا تدوین چارچوب‌های حقوقی دقیق را دربر می‌گیرد. ارتقاء آگاهی عمومی نسبت به تهدیدات سایبری و آموزش رفتارهای ایمن در فضای دیجیتال، گامی بنیادی در پیشگیری از حملات محسوب می‌شود. از سوی دیگر، تدوین و اجرای قوانین شفاف، به‌روز و الزام‌آور برای شناسایی، پیگرد و مجازات مرتکبین جرایم سایبری، از الزامات حیاتی نظام حقوقی است. همکاری میان نهادهای دولتی، بخش خصوصی و مراکز علمی می‌تواند زمینه‌ساز توسعه فناوری‌های نوین حفاظتی و راهکارهای خلاقانه در این حوزه باشد. در نهایت، تقویت زیرساخت‌های امنیتی، حفاظت از داده‌ها و اطلاعات حساس، و به‌کارگیری ابزارهای پیشرفته برای مقابله با حملات سایبری، از ارکان اساسی برای صیانت از حریم خصوصی و امنیت دیجیتال در عصر نوین فناوری به شمار می‌رود (انصاری مهیاری،خلیلی سامانی،پوالدیان،احمدی، ۴۴۲۰، ۵۳۵).

آموزش و استانداردسازی الگوریتم‌ها ضروری است الگوریتم‌هایی که در فرآیندهای قضائی، پیش‌بینی جرم یا شناسایی مظنونین مورد استفاده قرار می‌گیرند، تحت نظارت دقیق علمی و حقوقی قرار گیرند. همچنین ایجاد استانداردهای بین‌المللی برای طراحی الگوریتم‌های عادلانه و بی‌طرف امری حیاتی است تا از بروز سوگیری‌های نژادی، جنسیتی یا طبقاتی جلوگیری شود (مصطفوی اردبیلی، تقی‌زاده انصاری و رحمتی‌فر، ۱۴۰۱، ۲۶). در مسیر تحقق عدالت کیفری در بستر فضای سایبری، یکی از تحولات مهم در حقوق ایران، به رسمیت شناختن مسئولیت کیفری اشخاص حقوقی است؛ موضوعی که پیش از تصویب قانون جرایم رایانه‌ای کمتر مورد توجه قانون‌گذار قرار گرفته بود. با تصویب این قانون، به‌ویژه در ماده ۱۹، برای نخستین‌بار چارچوبی قانونی جهت پاسخ‌گویی کیفری نهادهای حقوقی در قبال جرایم رایانه‌ای فراهم شد. به‌موجب این ماده، چنانچه جرمی در فضای سایبری به‌واسطه اشخاص حقوقی و در راستای منافع آن‌ها رخ دهد، در صورت احراز شرایطی نظیر سهل‌انگاری در نظارت یا سوءاستفاده از ساختار سازمانی، شخص حقوقی نیز در کنار فرد مرتکب، مسئول شناخته می‌شود. به تعبیر رضوی‌فرد و موسوی‌الهی، این اقدام گامی نخستین در جهت انطباق سیاست جنایی ایران با تحولات جهانی در حوزه مسئولیت کیفری نهادهاست؛ تحولی که از دهه ۱۹۹۰ میلادی در نظام‌های حقوقی پیشرو، به‌ویژه در اروپا و شرق آسیا، مورد توجه قرار گرفته است (رضوی‌فرد و موسوی‌الهی، ۱۳۹۵، ۴۷–۴۹). با توجه به پیچیدگی و قدرت فزاینده اشخاص حقوقی در بهره‌گیری از فناوری‌های نوین، تقویت ضمانت‌های کیفری علیه آن‌ها، ضرورتی انکارناپذیر در مواجهه با جرایم سایبری است. بنابراین پیشنهاد می‌شود با بهره‌گیری از تجربیات تطبیقی، از جمله نظام‌های حقوقی ژاپن و اتحادیه اروپا، ابزارهای شناسایی، اثبات و اجرای مسئولیت کیفری اشخاص حقوقی در حقوق ایران توسعه یابد.

ج. بازاندیشی در مفهوم مسئولیت کیفری در بستر سایبری

با توسعه فناوری‌های نوین و گسترش تعاملات دیجیتال، مفاهیم سنتی مسئولیت کیفری نیز دچار دگرگونی شده‌اند. در فضای سایبری، برخلاف بسترهای فیزیکی، بسیاری از افعال مجرمانه فاقد نمود عینی‌اند، و همین امر احراز عناصر جرم را با چالش مواجه می‌سازد. برخی معتقدند که «در فضای سایبری، مفاهیم کلاسیک مسئولیت کیفری مانند مباشرت، معاونت، و عنصر مادی جرم باید بازتعریف شوند؛ چرا که با جرایمی مواجهیم که بدون تماس مستقیم، بدون خسارت

فیزیکی آنی، اما با نتایج فاجعه‌بار شکل می‌گیرند» (رضوی‌فرد، ۱۳۹۵،۲۷). در چنین شرایطی، تحلیل مسئولیت کیفری تنها با تکیه بر مدل‌های سنتی پاسخ‌گو نیست. آنچه در فضای سایبری اهمیت می‌یابد، ردیابی رفتار دیجیتال، تحلیل نیت در محیط غیرفیزیکی، و بررسی ساختارهای نهادیِ مرتبط با جرم است. همین مسأله، توجه به مسئولیت کیفری ناشی از «سهل‌انگاری فناورانه» یا «اشکالات سیستمی در الگوریتم‌ها» را نیز ضروری می‌سازد. به تعبیر نویسندگان، مسئولیت کیفری در فضای مجازی نه تنها به شخص مرتکب، بلکه به نهادها، مدیران سیستم‌های اطلاعاتی، و حتی طراحان نرم‌افزارهایی که امکان بزهکاری دیجیتال را فراهم می‌کنند، نیز قابل تسری است. در این فضا، مرز میان «فاعل» و «ابزار» در حال بازتعریف است، و همین موضوع، پرسش‌های بنیادینی را درباره قلمرو و حدود مسئولیت کیفری در عصر هوش مصنوعی و اینترنت اشیاء مطرح می‌سازد.

د. نقش سازمان‌های بین‌المللی در تنظیم قوانین هوش مصنوعی

با توجه به گستره جهانی تأثیرات هوش مصنوعی بر حقوق بشر، عدالت کیفری و ساختارهای حکمرانی، نقش سازمان‌های بین‌المللی در تنظیم، تدوین و نظارت بر اجرای مقررات در این زمینه بسیار حائز اهمیت است. این نهادها می‌توانند استانداردهای جهانی مشترکی برای استفاده مسئولانه از هوش مصنوعی ارائه دهند و سازوکارهای لازم برای تضمین رعایت این اصول را طراحی و پیاده‌سازی کنند (Gray, Zhong, Imperial, McKinlay, & Cremen, 2023, 4–7).

۱.سازمان ملل متحد **(UN)** سازمان ملل متحد طی سال‌های اخیر تلاش‌هایی جدی در جهت بررسی تأثیرات هوش مصنوعی بر نظام‌های عدالت کیفری و حقوق بشر انجام داده است. از مهم‌ترین اقدامات این سازمان، تدوین اسناد بین‌المللی و پروژه‌هایی است که به بررسی چالش‌های حقوقی، اخلاقی و اجتماعی ناشی از توسعه این فناوری می‌پردازند. به‌طور خاص، «کنوانسیون چارچوب شورای اروپا درباره هوش مصنوعی، حقوق بشر، دموکراسی و حاکمیت قانون» از جمله اسناد برجسته‌ای است که اصولی مانند عدالت، شفافیت، پاسخگویی، برابری، عدم تبعیض و حفاظت از حریم خصوصی را به‌عنوان معیارهایی بنیادین برای استفاده از هوش مصنوعی مطرح می‌کند (مشرفیان، ۱۴۰۴، ۱۳۸-۱۴۳).

۲.اتحادیه اروپا **(EU)** اتحادیه اروپا در سال ۲۰۲۴ نخستین چارچوب قانونی جامع جهانی در حوزه هوش مصنوعی با عنوان مقررات هوش مصنوعی (AI Act) را تصویب کرد. این قانون سامانه‌های هوش مصنوعی را بر اساس میزان ریسک در چهار طبقه قرار می‌دهد و برای سیستم‌های پرخطر الزاماتی نظیر ارزیابی ریسک، نظارت انسانی، شفافیت و مستندسازی را مقرر می‌دارد. هدف اصلی این قانون، کاهش خطرات احتمالی و تضمین حفاظت از حقوق بنیادین بشر است. اتحادیه اروپا همچنین با تأکید بر همکاری فرامرزی، سایر کشورها را به پیوستن به این چارچوب و ایجاد استانداردهای جهانی

دعوت کرده است (پژوهشکده حقوقی شهر دانش، ۱۴۰۳)[1].

۳.سازمان همکاری اقتصادی و توسعه **(OECD)** سازمان همکاری اقتصادی و توسعه نیز با ارائه «اصول هوش مصنوعی «OECD در سال ۲۰۱۹، رویکردی بین‌المللی به تنظیم فناوری‌های هوش مصنوعی اتخاذ کرد. این اصول تأکید ویژه‌ای بر عدالت اجتماعی، شفافیت، پاسخگویی و حفظ حقوق بشر دارند و از دولت‌ها می‌خواهند تا با وضع چارچوب‌های حقوقی مناسب، نظارتی مؤثر بر توسعه و استفاده از این فناوری‌ها اعمال کنند (بیگی و اقبالی، ۱۴۰۲، ۳۲).

۴.مثال‌ها و چالش‌ها در پیاده‌سازی قوانین بین‌المللی اجرای قوانین جهانی در زمینه هوش مصنوعی با موانع متعددی روبه‌روست؛ از جمله مهم‌ترین این چالش‌ها می‌توان به تفاوت‌های فرهنگی، حقوقی و سیاسی میان کشورها اشاره کرد. برای نمونه، در حالی که اتحادیه اروپا بر حفاظت از داده‌ها و حقوق فردی تمرکز دارد به‌ویژه از طریق قانون(GDPR)، برخی کشورها مانند چین رویکردی مبتنی بر نظارت دولتی را اتخاذ کرده‌اند (Miazi, 2023, 4–7).چین با ایجاد بزرگ‌ترین سامانه نظارت تصویری جهان که از فناوری‌های تشخیص چهره بهره می‌برد، نگرانی‌های گسترده‌ای را در زمینه نقض حریم خصوصی و حقوق اقلیت‌ها، به‌ویژه در منطقه سین‌کیانگ، برانگیخته است (Kurdistan TV, 2023, 1).این موضوع ضرورت نقش فعال‌تر سازمان‌های بین‌المللی در نظارت و وضع مقررات محدودکننده را دوچندان می‌سازد.

۵.لزوم همکاری‌های بین‌المللی با توجه به ماهیت فرامرزی جرائم نوظهور و پیچیده، همکاری میان کشورها و نهادهای بین‌المللی امری حیاتی است. آژانس‌هایی مانند Eurojust و eu-LISA در اتحادیه اروپا، با هدف مدرن‌سازی ساختارهای دیجیتال قضائی و تسهیل تبادل امن داده‌ها، اقدام به تدوین دستورالعمل‌های مشترک کرده‌اند. این دستورالعمل‌ها تأکید دارند که به‌کارگیری فناوری‌های هوش مصنوعی باید منطبق با اصول قانونی حفاظت از داده‌ها و احترام به حریم خصوصی باشد و صرفاً در شرایطی مورد استفاده قرار گیرد که ایمن، مفید و اخلاق‌مدار باشد (Eurojust & eu-LISA, 2022, 6–8).

نتیجه‌گیری و پیشنهادات

هوش مصنوعی با تمام ظرفیت‌هایی که برای بهبود عملکرد نظام‌های کیفری دارد، چالش‌های تازه و پیچیده‌ای را هم به‌وجود آورده است؛ چالش‌هایی که مستقیماً عدالت، حقوق بشر و اصول بنیادین دادرسی را تحت‌تأثیر قرار می‌دهند. در حال حاضر، قوانین موجود، که عمدتاً برای شرایط سنتی طراحی شده‌اند، پاسخ‌گوی ویژگی‌های خاص و پیچیده این

[1] پژوهشکده حقوقی شهر دانش.(۱۴۰۳) .قانون اتحادیه اروپا در مورد هوش مصنوعی (AI Act):تحلیل و بررسی چارچوب قانونی .بازیابی شده از https://sdil.ac.ir/قانون-اتحادیه-اروپا-در-مورد-هوش-مصنوعی/

فناوری نیستند. به‌عنوان مثال، اگر یک سامانه هوش مصنوعی مرتکب اشتباه یا تخلفی شود، مشخص نیست چه کسی باید پاسخگو باشد: طراح؟ توسعه‌دهنده؟ کاربر؟ یا خود سیستم؟ همچنین، وقتی تصمیم‌گیری‌ها در بستر الگوریتم‌های نامرئی و بدون شفافیت انجام می‌شود، اعتماد عمومی به نظام قضایی آسیب می‌بیند. از طرفی، اگر داده‌های آموزشی این سیستم‌ها سوگیرانه باشند، تبعیض‌هایی که در گذشته وجود داشته‌اند، ممکن است دوباره در تصمیم‌های امروز بازتولید شوند.برای اینکه بتوانیم از فرصت‌های هوش مصنوعی استفاده کنیم، بدون آنکه به اصول عدالت لطمه وارد شود، پیشنهادهای زیر ارائه می‌شود:

۱.بازنگری درمفهوم باید چارچوبی طراحی شود که مشخص کند در صورت بروز خطا از سوی یک سامانه هوشمند، چه کسانی مسئول هستند. شاید نیاز باشد مسئولیت میان طراح، شرکت توسعه‌دهنده و کاربران تقسیم شود یا حتی در برخی موارد، سامانه‌ها شخصیت حقوقی محدود پیدا کنند.

۲.شفاف‌سازی فرآیندهای الگوریتمی کاربران، قضات و حتی متهمان باید بدانند تصمیمات سیستم بر چه اساسی گرفته شده است. الگوریتم‌ها نباید جعبه‌های سیاه باشند. لازم است فرآیندها قابل‌بررسی، قابل‌اعتراض و قابل‌درک باشند.

۳.کنترل و کاهش سوگیری‌ها باید مراقب باشیم که داده‌های سوگیرانه گذشته، در سیستم‌های جدید تکرار نشوند. این کار نیازمند نظارت مستقل، تنوع در داده‌های آموزشی و ممیزی‌های منظم است.

۴.تدوین مقررات بین‌المللی یکپارچه چون بسیاری از جرائم در فضای دیجیتال فرامرزی هستند، ضروری است سازمان‌هایی مانند سازمان ملل و اتحادیه اروپا برای تنظیم چارچوب‌های مشترک اقدام کنند. الگویی مانند قانون «AI Act» اتحادیه اروپا می‌تواند الهام‌بخش سایر کشورها باشد.

۵.آموزش تخصصی و تقویت دانش قضات و وکلا برای بهره‌گیری درست از هوش مصنوعی، فعالان حوزه حقوق باید آموزش ببینند؛ هم درباره فناوری، هم درباره پیامدهای اخلاقی و حقوقی آن. ایجاد دوره‌های تخصصی و مراکز مطالعاتی در دانشگاه‌ها و نهادهای قضایی، در این مسیر بسیار مؤثر خواهد بود.

در پایان، تحقق عدالت در دوران فناوری‌های هوشمند، بدون نوسازی قوانین و ارتقای آگاهی حقوقی ممکن نیست. همکاری‌های بین‌المللی و توجه به ابعاد انسانی و اخلاقی این تحولات، رمز موفقیت در مواجهه با چالش‌های روبه‌رشد هوش مصنوعی خواهد بود.

سپاسگزاری

از معاونت محترم پژوهشی به خاطر حمایت حمایت معنوی در اجرای پژوهش حاضر سپاسگزاری می‌شود.
از آقای دکتر عبدالله علیزاده به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.
از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.
نگارندگان بر خود لازم می‌دانند از آقای دکتر محمد رسول آهنگران به خاطر مطالعه متن مقاله حاضر و ارائه نظرهای ارزشمند سپاسگزاری نمایند.

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

منابع

۱. عباسی کلیمانی، عاطفه. (۱۴۰۲). نقش هوش مصنوعی در پیشگیری از جرم. سخنرانی علمی، دانشگاه امام صادق (ع)، پردیس خواهران. https://isuw.ac.ir/file/download/news/1669449921-.pdf

۲. پور قصاب امیری، علی، و علوی‌تبار، مجید. (۱۴۰۳). آسیب‌پذیری حقوق بشر از کاربردهای هوش مصنوعی. فصلنامه علمی پژوهشی نی نودرآموزش وپرورش، ۵(۲)، ۲۰۱–۲۱۰. https://esjournal.ir/fa/paper.php?pid=214

۳. طلیات، سید محمدحسین. (۲۰۲۲). توسعه یک شبکه باور بیزی برای ارزیابی ریسک تصادف خودروهای متصل و خودران در محیط‌های شهری: یک سنتز جامعه‌شناختی–فنی (رساله دکتری، دانشکده علوم اجتماعی، مدرسه کسب‌وکار ساوتهمپتون، دانشگاه ساوتهمپتون، انگلستان). https://eprints.soton.ac.uk/472451/1/Thesis.pdf

٤. کینگستون، جی. کی. سی. (نویسنده)، صلحچی، سارا، و بیگلربیگی، کیان (مترجمان). (۱۴۰۲). هوش مصنوعی و مسئولیت قانونی. تمدن حقوقی، ۶(۱۸)، ۱۰۳–۱۲۰. https://www.pzhfars.ir/article_191091.html

۵. صوفی، سارا، و صالح‌نژاد بهرستاقی، صابر. (۱۴۰۲). تأثیر هوش مصنوعی در ارتکاب جرایم سایبری. مجله مطالعات حقوق، ۱۱(۵۱)، ۱–۱۸. https://jlawst.ir/article-1-1069-en.pdf

٦. بینا، مرتضی، و حبیبی، مسعود. (۱۴۰۲). مطالعه بین‌رشته‌ای بیم‌ها و امیدها: خطر سوگیری هوش مصنوعی در حوزه حقوق. وب‌سایت فردای اقتصاد. https://www.fardayeeghtesad.com/news/28290

۷. سوشینا، تاتیانا، و سوبنین، آندری. (نویسندگان)، صادقی، سالار. (مترجم). (۱۴۰۲). هوش مصنوعی در نظام عدالت کیفری: روندها و احتمالات پیشرو. تمدن حقوقی، ۶(۱۸)، ۹۱–۱۰۲. https://www.pzhfars.ir/article_191090.html

۸. کاوه، محمدهادی، و بارانی، محمد. (۱۴۰۳). مسؤولیت کیفری هوش مصنوعی در حقوق کیفری ایران با نگاهی به قوانین اتحادیه اروپا. فصلنامه فقه جزای تطبیقی، ۴(۳)، ۵۱–۶۱. https://www.jccj.ir/article_201974.html

۹. مصطفوی اردبیلی، سید محمدمهدی، تقی‌زاده انصاری، مصطفی، و رحمتی‌فر، سمانه. (۱۴۰۱). کارکردها و بایسته‌های هوش مصنوعی از منظر دادرسی منصفانه. دوفصلنامه علمی حقوق فناوری‌های نوین، ۳(۶)، ۴۷–۶۰. https://doi.org/10.22133/MTLJ.2022.360802.1121

۱۰. مشرفیان، محمدرضا. (۱۴۰۴). ترجمه کنوانسیون چارچوب شورای اروپا در مورد هوش مصنوعی و حقوق بشر، دموکراسی و حاکمیت قانون. مجله حقوقی بین‌المللی، دوره ۴۲(شماره ۷۷)، ۱۳۸–۱۴۳. https://www.cilamag.ir/article_723523_1b80213646532b83e783ea00346940c0.pdf

۱۱. بیگی، جمال، و اقبالی، زهرا. (۱۴۰۲). جایگاه هوش مصنوعی و چالش‌های حقوق بشری آن در ارتباطات بین‌المللی. نشریه مدیریت فرهنگ و توسعه اقتصادی، ص. ۳۲. بازیابی از https://doi.org/10.52547/rcmde.1.2.32

۱۲. حسینی، الهه سادات؛ واحدیاریجان، یونس؛ و یزدانی، سمانه. (۱۴۰۳). چالش‌های هوش مصنوعی و مبانی مسئولیت مدنی آن در فقه. پژوهش‌های تطبیقی فقه، حقوق و سیاست، ۶(۵)، ۱–۲۰. https://doi.org/10.61838/csjlp.6.5.1

۱۳. شیخوند، محمدصادق؛ کردعلیوند، روح‌الدین؛ مینایی، بهروز؛ آشوری، محمد؛ و مهدوی ثابت، محمدعلی. (۱۴۰۲). هوش مصنوعی و صدور احکام کیفری؛ تصمیم‌سازی یا تصمیم‌گیری؟ فصلنامه پژوهش‌های حقوق تطبیقی، ۲۷(۴)، ۱۳۸–۱۶۷. https://clr.modares.ac.ir/article-20-72285-fa.html

۱٤. مکی، اکرم‌السادات؛ مکی، زهراالسادات؛ کشکولیان، اسماعیل. (۱۴۰۳). بررسی مسئولیت ناشی از اعمال هوش مصنوعی در نظام حقوقی ایران. نشریه علمی فقه، حقوق و علوم جزا، ۸(۳۲)، ۷۱–۷۹. بازیابی شده از https://www.magiran.com/paper/2799036

۱۵. انصاری مهیاری، علیرضا، خلیلی سامانی، کیمیا، پوالدیان، مهناز، &احمدی، ملینا. (۱۴۰۲). راه‌کارهای مبارزه با جرایم سایبری از دیدگاه حقوق بین‌الملل. نشریه علمی مطالعات نوین علوم انسانی در جهان، ۴(۴)، ۲۳۵–۲۴۹. بازیابی شده از https://hujournal.ir/fa/paper.php?pid=213

۱٦. نعمتی، محمد؛ گلچین‌راد، عارفه؛ صادقیان لمراسکی، نگار. (۲۰۲۵). جرائم اقتصادی هوش مصنوعی: تهدیدها و راهکارها. دومین کنفرانس ملی چالش‌های نوظهور حقوق کیفری در فضای سایبری. دانشگاه آزاد اسلامی واحد مشهد. بازیابی از :https://civilica.com/doc/1789238

۱۷. ذاکری‌نیا، حانیه. (۲۰۲۵). جایگاه مسئولیت مدنی در حقوق کیفری ایران (با تأکید بر قانون مجازات اسلامی ۱۳۹۲). همایش بین‌المللی حقوق تطبیقی و نوآوری‌های قانونی. دانشگاه تهران. بازیابی از : https://clicl.ut.ac.ir/articles?_action=article&au=79566&_au=ذاکری+حانیه

۱۸. رضوی‌فرد، بهزاد، و موسوی، سید نعمت‌الله. (۱۳۹۶). مسئولیت کیفری در فضای سایبر در حقوق ایران. فصلنامه پژوهش حقوق کیفری، ۵(۱۶)، ۵۱–۸۳. ***https://jclr.atu.ac.ir/article_6753.html***

۱۹. اسدپور، فرشته، پهلوان‌زاده، عباس، و خندانی، پدرام. (۱۴۰۲). تأثیر تحولات حقوقی هوش مصنوعی در حوزه حقوقی مالکیت فکری. تحقیقات حقوق خصوصی و کیفری، ۱۹(۴)، ۱۳۱–۱۴۷. ***https://www.magiran.com/p2701996***

20. Binns, R. (2018). Algorithmic accountability and public reason. Philosophy & Technology, 31, 543–556. https://doi.org/10.1007/s13347-017-0263-5

21. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). Machine bias. ProPublica.

justice (pp. 6–8). European Union Agency for Criminal Justice Cooperation & European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice. https://www.eurojust.europa.eu/sites/default/files/assets/artificial-intelligence-cross-border-cooperation-criminal-justice-report.pdf

31. Gray, Charlotte, Zhong, Han, Imperial, Joseph Marvin, McKinlay, Jack, & Cremen, Eoin. (2023). Promoting global cooperation on AI regulation: ART-AI submission to the Global Digital Compact (Supplementary Report) (pp. 4–7). University of Bath. https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/GDC-submission_ART-AI_University-of-Bath.pdf

https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

22. Zarsky, T. Z. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. Science, Technology, & Human Values, 41(1), 118–132. https://doi.org/10.1177/0162243915605575

23. Jouini, E. (2016). Algorithmic bias: Sources and solutions. Journal of Ethics and Information Technology, 18(2), 123–135. https://doi.org/10.1007/s10676-016-9395-2

24. Garvie, C., Bedoya, A., & Frankle, J. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology. https://www.perpetuallineup.org/

25. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, May 23). *Machine bias: There's software used across the country to predict future criminals. And it's biased against Blacks*. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

26. Raji, I. D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., & Denton, E. (2020). Saving face: Investigating the ethical concerns of facial recognition auditing. In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (pp. 145–151). Association for Computing Machinery. https://doi.org/10.1145/3375627.3375820

27. Miazi, M. A. N. (2023). Interplay of legal frameworks and artificial intelligence (AI): A global perspective. Law and Policy Review, 2(2), 1–25. https://doi.org/10.32350/lpr.22.01

28. Sartor, Giovanni, & Lagioia, Francesca. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (pp. II–III). European Parliamentary Research Service, Panel for the Future of Science and Technology (STOA). https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

29. Kurdistan TV. (2023). Chin bozorgtarin system-e nezarati-ye jahan ra darad [China has the world's largest surveillance system]. Retrieved from https://kurdistantv.net/fa/news/199314

30. Eurojust & eu-LISA. (2022). Artificial intelligence supporting cross-border cooperation in criminal