

تحلیل جرم شناسی محیطی و نقش هوش مصنوعی بر افزایش جرایم سازمان یافته و جرایم سایبری

(تاریخ دریافت ۱۴۰۴/۰۷/۱۵، تاریخ تصویب ۱۴۰۴/۱۲/۰۳)

ستوده قصری^۱

علی سلیمی نژاد

چکیده

با گسترش فناوری هوش مصنوعی در دهه اخیر، الگوهای سنتی جرم و بزهکاری دگرگون شده و شکل جدیدی از جرایم موسوم به «جرایم مبتنی بر هوش مصنوعی» پدید آمده است. این فناوری، اگرچه ظرفیت قابل توجهی در حل مسائل بشری دارد، اما در فقدان چارچوب‌های نظارتی و قانونی مستحکم، به ابزاری برای ارتکاب جرایم پیچیده، سریع، فراگیر و بعضاً غیرقابل ردیابی تبدیل شده است.

پژوهش حاضر با روش توصیفی - تحلیلی و با بهره‌گیری از داده‌های موجود در فایل حاضر، به بررسی مهم‌ترین مصادیق سوءاستفاده از هوش مصنوعی در بستر جرم، از جمله کلاهبرداری هوشمند، جعل هویت دیجیتال، پول‌شویی مبتنی بر رمزارز، حملات سایبری خودکار، جعل صوت و تصویر (دیپ‌فیک) و اخلاف در نظم عمومی می‌پردازد.

نتایج این پژوهش بیانگر آن است که نظام‌های حقوقی، به‌ویژه در حوزه ادله الکترونیکی، مسئولیت کیفری و انتساب جرم، با چالش‌های جدی روبه‌رو هستند. این در حالی است که برخی نظام‌های حقوقی همچون اتحادیه اروپا با تدوین مقرراتی نظیر *AI Act* در مسیر



تنظیم‌گری این فناوری گام برداشته‌اند، اما بسیاری کشورها از جمله ایران، هنوز در مرحله قانون‌گذاری پراکنده و واکنشی قرار دارند .

در بخش پایانی، با تکیه بر یافته‌های جرم‌شناسانه، مجموعه‌ای از راهبردهای تقنینی، نظارتی و آموزشی پیشنهاد شده است که می‌تواند در سیاست جنایی کشورها برای مواجهه با این تهدید نوظهور مورد استفاده قرار گیرد.

واژگان کلیدی: هوش مصنوعی، جرم‌شناسی، جرایم سایبری، مسئولیت کیفری، سیاست

جنایی

مقدمه

هوش مصنوعی در نگاه نخست، نماد پیشرفت، کارآمدی و تسهیل امور است. این فناوری با توان تحلیل داده‌های کلان، تشخیص الگوهای پنهان، تصمیم‌گیری خودکار و شبیه‌سازی رفتار انسانی، در حوزه‌هایی مانند پزشکی، اقتصاد، امنیت، آموزش و صنعت تحولی عظیم ایجاد کرده است. با این حال، همان ویژگی‌هایی که هوش مصنوعی را به ابزاری کارآمد تبدیل می‌کند، آن را به بستری بالقوه برای بزهکاری پیچیده، گسترده و فرامرزی نیز بدل می‌سازد .



بر خلاف جرایم کلاسیک که به حضور فیزیکی، ابزار ملموس و مکان معین وابسته بود، جرایم مبتنی بر هوش مصنوعی می‌توانند از راه دور، بدون حضور مستقیم مجرم و با استفاده از سیستم‌های خودکار صورت گیرند. این ویژگی سبب شده تا:

۱. شناسایی بزهکار دشوارتر شود
 ۲. ادله جرم شکننده‌تر و قابل دست‌کاری باشند
 ۳. تعیین مسئولیت کیفری با ابهام مواجه گردد
 ۴. ابعاد جرم فراملی و گسترده‌تر شوند
- به‌ویژه پدیده‌هایی مانند جعل ویدیویی (*Deepfake*)، فیشینگ هوشمند، باج‌گیری الگوریتمی و پول‌شویی مبتنی بر رمزارز نمونه‌هایی از کاربرد مجرمانه این فناوری هستند که در سال‌های اخیر رشد چشمگیری داشته‌اند.

در چنین شرایطی، این پرسش اساسی مطرح می‌شود که:

نظام عدالت کیفری تا چه اندازه آمادگی مقابله با این نوع جدید از بزهکاری را دارد؟

هوش مصنوعی *AI* یکی از مهمترین پیشرفت‌های فناوریانه بشر در قرن بیستم و بیست و یکم است که توانسته است مرزهای نوآوری را گسترش دهد. تاریخچه هوش مصنوعی به دهه ۱۹۵۰ میلادی باز می‌گردد، زمانی که جان مک‌کارتی برای نخستین بار اصطلاح «هوش مصنوعی» را مطرح کرد. در آن زمان هدف اصلی دانشمندان، طراحی ماشین‌هایی بود که قادر به انجام وظایف منطقی و محاسباتی باشند. اولین تالش‌ها شامل توسعه الگوریتم‌هایی برای



بازی‌های رایانه‌ای، حل معادلات ریاضی و پردازش زبان طبیعی بود. با گذشت زمان و پیشرفت در توان محاسباتی، یادگیری ماشینی و شبکه‌های عصبی، هوش مصنوعی به حوزه‌های پیچیده‌تر وارد شد. دهه ۰۵۹۱ شاهد تحولات عظیمی در یادگیری ماشینی و توسعه الگوریتم‌های مبتنی بر داده بود. در دهه ۰۱۰۱، ظهور یادگیری عمیق *Learning Deep* به همراه افزایش دسترسی به داده‌های بزرگ تحولی شگرف در توانایی‌های هوش مصنوعی ایجاد کرد. امروزه این فناوری در حوزه‌هایی نظیر خودروهای خودران، پزشکی، امنیت سایبری و حتی قضاوت‌های حقوقی نقش ایفا می‌کند. هوش مصنوعی اکنون به صورت گسترده‌ای در زندگی روزمره ما نفوذ کرده است؛ از دستیارهای هوشمند شخصی مانند سیری و الکسا گرفته تا سیستم‌های پیشرفته‌ای که در امور مالی، صنعتی و نظامی به کار گرفته می‌شوند؛ اما این گسترش فناوری، چالش‌های بسیاری را نیز به دنبال داشته است که یکی از آنها، تعیین مسئولیت در صورت وقوع خطاها یا جرایم است. ورود هوش مصنوعی به نظام‌های حقوقی، یکی از جنبه‌های پیچیده و بحث‌برانگیز این فناوری است. از یک سو، هوش مصنوعی می‌تواند به عنوان ابزاری برای ارتقای عدالت و افزایش کارایی در سیستم‌های قضایی عمل کند. برای مثال از الگوریتم‌های پیشرفته برای تحلیل شواهد و پیش‌بینی نتیجه پرونده‌ها استفاده می‌شود. از سوی دیگر پیچیدگی و عدم شفافیت تصمیم‌گیری‌های هوش مصنوعی می‌تواند مشکلات جدیدی را ایجاد کند. یکی از مسائل کلیدی در این زمینه، تعیین مسئولیت کیفری در موارد وقوع جرایم مرتبط با هوش مصنوعی است. بر اساس اصول سنتی حقوق کیفری، مسئولیت معمولاً بر پایه تقصیر یا نیت مجرمانه استوار است؛ اما در مواردی که هوش مصنوعی به دلیل نقص در طراحی، آموزش ناکافی یا تصمیمات مستقل دچار اشتباه می‌شود، چه کسی باید پاسخگو باشد؟ آیا مسئولیت بر عهده کاربر، طراح یا سازنده است؟ یا



اینکه باید سیستمی برای شناسایی نقش دقیق هر یک از این عوامل ایجاد کرد؟ این پرسش‌ها به ویژه در حوزه‌هایی مانند خودروهای خودران، سیستم‌های امنیت سایبری و الگوریتم‌های تصمیم‌گیری پزشکی، از اهمیت ویژه‌ای برخوردارند. برای مثال در یک تصادف که توسط یک خودروی خودران رخ می‌دهد، ممکن است عواملی مانند نقص در نرم افزار، خرابی حسگرها یا رفتار پیش‌بینی ناپذیر دیگر کاربران جاده دخیل باشند. این وضعیت‌ها نشان می‌دهند که قوانین سنتی برای مدیریت این مسائل کافی نیستند و نیاز به بازنگری یا تدوین قوانین جدید دارند. با افزایش نفوذ هوش مصنوعی در زندگی انسان‌ها، جامعه جهانی به طور فزاینده‌ای به پیامدهای اخلاقی، اجتماعی و حقوقی این فناوری توجه می‌کند. فناوری‌هایی نظیر تشخیص چهره، سیستم‌های توصیه‌گر و الگوریتم‌های پیش‌بینی جرم، از جمله ابزارهایی هستند که تأثیرات گسترده‌ای بر جوامع دارند. اگرچه این فناوری‌ها می‌توانند به افزایش کارایی و امنیت کمک کنند، اما نگرانی‌هایی نیز در مورد نقض حریم خصوصی، تبعیض الگوریتمی و سوء استفاده از این ابزارها وجود دارد.

بخش اول: مبانی نظری و چارچوب مفهومی

هوش مصنوعی هوش مصنوعی از دو کلمه مرکب است. هوش یعنی توانایی ذهن برای تجزیه و تحلیل، استدلال، درک معانی، خودآگاهی، یادگیری و به کارگیری مفاهیم که با استفاده از عملکرد مغز میسر می‌شود. واژه مصنوعی نیز به معنی خلق یا ساخته شده توسط انسان است. هوش مصنوعی که به اختصار از آن با عنوان AI نام برده می‌شود و نقطه مقابل هوش طبیعی است، در تعریف کلی، به سامانه‌هایی می‌گویند که قادرند عکس‌العمل‌هایی شبیه به رفتارهای هوشمند انسان داشته باشند؛ رفتارهایی همچون درک شرایط سخت و پیچیده، شبیه



سازی فرایند های تفکری و روش های استدلالی انسان و جواب موفق به آنان، آموختن و توانایی به دست آوردن دانش و استدلال برای حل مسائل. هوش مصنوعی یکی از دانش هایی است که در علوم کامپیوتر، به شدت اهمیت دارد و تغییرات در هوش مصنوعی می تواند تحولات بسیاری در فناوری اطلاعات به وجود آورد. در واقع هوش مصنوعی را می توان هوش ماشین ها نیز نامید. این علم شاخه ای از علوم کامپیوتر به شمار می آید و می خواهد راهکارهای الگوریتمی بدهد تا بتوانید به کمک آن ها، هوشمندی های بیشتری در انواع ماشین ها بوجود آورید. آفاجانی، مسئولیت سامانه های هوش مصنوعی جامعه بشری با استفاده از فناوری هوش مصنوعی به سامانه اجتماعی - فنی تبدیل شده است. در این جوامع، سامانه های هوش مصنوعی هم می توانند مرتکب تخلف و جرم شوند و هم شریک یا ابزار ارتکاب جرم قرار گیرند. در بسیاری از کشورهای پیشرفته، وسایل نقلیه بدون سرنشین، سامانه های جراحی پیچیده، سامانه های رایانه ای صنعتی، الگوریتم های تجاری و دیگر سامانه های هوش مصنوعی، به نحو گسترده ای برای اهداف صنعتی و شخصی استفاده می شوند؛ اما وقتی که یکی از چنین سامانه هایی موجب بروز خسارت می شود، بحث مسئولیت مطرح می شود؛ مثال وقتی که یک وسیله نقلیه بدون سرنشین موجب ایجاد تصادف می شود، یا یک سامانه جراحی خودکار، موجب خطای پزشکی شود یا اینکه الگوریتم های تجاری منجر به کالهدرداری شوند، در چنین مواقعی چه کسی باید مسئول شناخته شود؟ سازنده، برنامه نویس، کاربر و یا خود سامانه هوش مصنوعی. کدام مسئول است و به چه میزان مسئول است؟ مفهوم مسئولیت ناظر به جرایمی که توسط هوش مصنوعی رخ می دهد، هنوز به درستی مورد بررسی قرار نگرفته است و تحقیقات ناظر به آن بسیار محدود است. در مقابل پیشرفت علم و فناوری، مدام موجب رو در رو شدن افراد و جامعه با چالش های جدید می شود. ایزاک آسیموف، نویسنده



مشهور داستان های علمی تخیلی، در دهه ۵۹۱۰ در داستان «من روبات هستم» قوانین سه گانه آسیموف را مطرح کرد^۹ قانون اول^۹ یک ربات نباید با ارتکاب عملی یا خودداری از انجام عملی باعث آسیب دیدن یک انسان شود. قانون دوم^۹ یک روبات باید از تمامی فرمان های انسان تبعیت کند، مگر اینکه آن فرمان یا فرمان ها در تعارض با قانون نخست باشد. قانون سوم^۹ تا هنگامی که قانون نخست یا دوم زیر پا گذاشته نشده، روبات باید وجود خود را حفظ کرده و در بقای خود بکوشد. اگرچه آسیموف به طور خاص به روبات ها اشاره کرده است، اما این قوانین را می توان تعمیم داد و برای کل فناوری هوش مصنوعی از جمله نرم افزارها، به اجرا در آورد. در دنیای جدید، سه نوع از موجودات وجود دارند^۹ انسان، حیوان و هوش مصنوعی. خبرگانی که معتقد هستند فناوری هوش مصنوعی باید از حقوق کیفری انسان تبعیت کند باید شباهت بین انسان و هوش مصنوعی را اثبات کنند. در واقع آن ها باید این توضیح را دهند که به چه علت فناوری هوش مصنوعی بیشتر به انسان شباهت دارد تا به حیوانات. یک موجود دارای هوش مصنوعی توسط انسان و طبق استدلال منطق انسانی برنامه نویسی می شود و این دلیل اصلی فعالیت یک موجود دارای هوش مصنوعی است. همچنین محاسبات این موجود در قالب استدلال منطق انسانی قابل بیان هستند. از آنجایی که قانون در هنگام ارزیابی تعهد حقوقی، عقلانیت را بر احساسات ترجیح می دهد و از آنجایی که عقلانیت فناوری هوش مصنوعی بر اساس استدلال منطق انسانی است، بنابراین از منظر حقوقی، فناوری هوش مصنوعی به انسان نزدیکتر است تا به حیوانات. در نتیجه، مدل حقوقی حیوانات، با فناوری هوش مصنوعی برای ارزیابی تعهد حقوقی مطابقتی ندارد. پس مفاهیم اولیه از الزامات مسئولیت حقوقی هستند که باید برای اعمال هر شخص اعم از انسان، سازمان و یا فناوری هوش مصنوعی اعمال شود. توسعه فناوری پیشرفته ای که با فناوری هوش مصنوعی همراه شده،



توانایی برآوردن الزامات پذیرش مسئولیت کیفری را دارد. فناوری هوش مصنوعی نیز مانند مجرمان غیر انسانی (نظیر شرکت‌ها) هیچ مانعی در پذیرش مسئولیت کیفری، ندارند. در نتیجه، جزئیات قانون جزا در هر کشوری تکلیف را معین خواهد کرد.

در ساده‌ترین تعریف، هوش مصنوعی به توانایی سیستم‌ها در انجام وظایفی اطلاق می‌شود که معمولاً به هوش انسانی نیاز دارد؛ از جمله تحلیل داده‌ها، تشخیص الگوها، تصمیم‌گیری و یادگیری مستقل. بخش مهمی از این توانمندی از طریق «یادگیری ماشین» و «شبکه‌های عصبی مصنوعی» ایجاد می‌شود.

از مهم‌ترین شاخه‌های هوش مصنوعی که در جرم‌نقش‌آفرین هستند می‌توان به موارد زیر اشاره کرد:

• یادگیری ماشین (Machine Learning)

• یادگیری عمیق (Deep Learning)

• پردازش زبان طبیعی (NLP)

• تولید محتوا (Generative AI)

• الگوریتم‌های تصمیم‌گیر خودکار

همین ظرفیت‌ها باعث شده‌اند که هوش مصنوعی گاه به ابزاری برای خلق جرم و گاه به ابزاری برای تسهیل جرم تبدیل شود.



بخش دوم: روش تحقیق

پژوهش حاضر از نوع توصیفی-تحلیلی است و با رویکرد کیفی انجام شده است. داده‌های مورد استفاده در این پژوهش از طریق مطالعه اسنادی، بررسی متون علمی، تحلیل گزارش‌های تخصصی، مطالعه قوانین داخلی و بین‌المللی و تحلیل نمونه‌های واقعی جرایم مبتنی بر هوش مصنوعی گردآوری شده است.

در این تحقیق، ابتدا با بررسی مفهومی پدیده هوش مصنوعی و تبیین پیوند آن با علوم جرم‌شناسی، چارچوب نظری پژوهش شکل گرفت. سپس، با مطالعه نمونه‌هایی از جرایم ارتكابی به کمک یا توسط سیستم‌های هوشمند، چالش‌های اصلی نظام عدالت کیفری در مواجهه با این جرایم استخراج و تحلیل گردید.

در بخش تحلیل داده‌ها، از روش تحلیل محتوای کیفی (Qualitative Content Analysis) استفاده شده است؛ به این صورت که داده‌ها در قالب مفاهیم، مقولات و مضامین اصلی طبقه‌بندی گردیده و سپس به صورت تطبیقی با نظریات جرم‌شناسی کلاسیک و نوین مقایسه شده‌اند.

همچنین در بخش «راهکارها»، از رویکرد تجویزی - سیاست‌گذاری (Policy-oriented approach) بهره گرفته شده است تا پیشنهاد‌های ارائه‌شده قابلیت اجرایی در سطح قانون‌گذاری و سیاست جنایی را داشته باشند.

این روش تحقیق، دارای اعتبار علمی و مناسب برای مقالات نشریات دانشگاهی در حوزه حقوق کیفری و جرم‌شناسی است.



بخش سوم: پیشینه پژوهش

۱. پژوهش‌های خارجی

مطالعات خارجی نشان می‌دهد که نگرانی نسبت به نقش هوش مصنوعی در ارتکاب جرم، به‌ویژه در دهه اخیر افزایش یافته است. بسیاری از پژوهشگران بر این باورند که فناوری‌های نوین نه تنها اشکال جدیدی از جرم را تولید کرده‌اند، بلکه ابزارهای سنتی کنترل جرم را نیز ناکارآمد ساخته‌اند.

برخی پژوهش‌ها به‌طور خاص به موضوع «هوش مصنوعی و مسئولیت کیفری» پرداخته‌اند و استدلال کرده‌اند که ساختار فعلی حقوق جزا توانایی پاسخگویی به پیچیدگی‌های ناشی از سیستم‌های خودکار و یادگیرنده را ندارد. این مطالعات بر ضرورت بازتعریف مفاهیمی همچون فاعلیت جرم، قصد مجرمانه و خطای انسانی تأکید کرده‌اند.

در تعدادی از مقالات نیز به مسئله امنیت سایبری و تهدیدات ناشی از الگوریتم‌های هوشمند پرداخته شده و بیان شده است که هوش مصنوعی می‌تواند نقش «شتاب‌دهنده جرم» را ایفا کند؛ به این معنا که نه تنها وقوع جرم را تسهیل می‌کند، بلکه دامنه و شدت آن را نیز افزایش می‌دهد.

در اسناد سازمان‌های بین‌المللی نیز به‌طور مکرر بر خطر استفاده از هوش مصنوعی در ایجاد بی‌ثباتی، حملات سایبری، جنگ اطلاعاتی و دستکاری افکار عمومی تأکید شده است. این اسناد، کشورهای عضو را به تدوین قوانین بازدارنده و سازوکارهای کنترلی فراخوانده‌اند.



۲. پژوهش‌های داخلی

در ایران نیز طی سال‌های اخیر، مقالاتی در زمینه جرایم سایبری، ادله الکترونیکی، مسئولیت کیفری در فضای مجازی و جرایم فناوری محور منتشر شده است. با این حال، بررسی منابع نشان می‌دهد که بیشتر این پژوهش‌ها به صورت کلی به فضای مجازی پرداخته‌اند و تمرکز مشخصی بر هوش مصنوعی به عنوان یک پدیده مستقل و نوظهور در بزهدکاری نداشته‌اند.

محدود پژوهش‌هایی که به صورت مستقیم به هوش مصنوعی پرداخته‌اند، بیشتر جنبه فنی یا اخلاقی داشته و از منظر جرم‌شناسانه و تحلیلی سیاست جنایی، کار جامع و عمیقی صورت نگرفته است.

بنابراین، این پژوهش از این جهت دارای نوآوری علمی است که:

- به‌طور اختصاصی بر «هوش مصنوعی» تمرکز دارد
- رویکرد جرم‌شناسانه، حقوقی و سیاست‌گذاری را هم‌زمان به کار می‌گیرد
- سعی دارد خلأ موجود در ادبیات داخلی را پر کند



از دیدگاه جرم‌شناسی، هوش مصنوعی را می‌توان در چهار نقش اصلی در بزهکاری تحلیل کرد:

۱. هوش مصنوعی به‌عنوان ابزار جرم

در این حالت، فناوری صرفاً وسیله‌ای است در اختیار مجرم؛ مانند استفاده از الگوریتم برای جعل صدا، تولید بدافزار، یا تحلیل اطلاعات قربانیان.

این نوع بزهکاری با نظریه «فرصت مجرمانه» همخوانی کامل دارد؛ زیرا فناوری جدید، فرصت‌های بزهکاری را افزایش می‌دهد و هزینه ارتکاب جرم را کاهش می‌دهد.

۲. هوش مصنوعی به‌عنوان تسهیل‌گر جرم

در این نقش، هوش مصنوعی فراتر از یک ابزار ساده عمل می‌کند و نقش فعال در تصمیم‌گیری، زمان‌بندی، انتخاب هدف و شیوه ارتکاب دارد.

مثال آن الگوریتم‌هایی هستند که خودشان بهترین زمان حمله سایبری را تشخیص می‌دهند یا بهترین فرد برای فریب را انتخاب می‌کنند.

۳. هوش مصنوعی به‌عنوان پنهان‌کننده جرم

یکی از مهم‌ترین چالش‌ها، نقش هوش مصنوعی در:

• مخفی‌سازی هویت مجرم

• تغییر مسیر داده‌ها



• جعل شواهد دیجیتال

• ایجاد بی‌نظمی در ردپاهای الکترونیکی

این کار مبارزه با جرم را بسیار دشوارتر می‌کند و حتی موجب تبرئه مجرم در برخی موارد می‌شود.

۴. هوش مصنوعی به‌عنوان عامل تولید جرم جدید

پارهای از جرایم، اصولاً بدون وجود هوش مصنوعی قابل تحقق نبودند؛ مانند:

• دیپ‌فیک‌های فوق‌واقعی

• جعل شخصیت حقوقی

• جعل اعتقادات، مواضع و گفتار اشخاص

• جرایم مبتنی بر ربات‌های تصمیم‌گیر

این شکل از بزهکاری نشان می‌دهد که ما با صورت‌های نوظهور جرم مواجه هستیم، نه صرفاً نسخه دیجیتال جرائم قدیمی.



مصادیق جرایم مبتنی بر هوش مصنوعی:

۱. فیشینگ هوشمند و کلاهبرداری پیشرفته

در شکل سنتی کلاهبرداری اینترنتی، پیام‌ها معمولاً عمومی و قابل شناسایی بودند. اما امروز، هوش مصنوعی قادر است با تحلیل داده‌های فردی، پیام‌هایی طراحی کند که از نظر لحن، محتوا و حتی زمان ارسال، کاملاً متناسب با شخصیت قربانی باشد.

در این حالت، هوش مصنوعی:

- اطلاعات شغلی و خانوادگی قربانی را تحلیل می‌کند

- لحن پیام را شخصی‌سازی می‌کند

- اعتماد هدف را جلب می‌نماید

- قربانی را به انتقال پول یا اطلاعات تشویق می‌کند

به همین دلیل، قربانی حتی متوجه ارتکاب جرم نمی‌شود.



۲. قتل هویت حقوقی

یکی از خطرناک‌ترین پدیده‌ها که در فایل نیز ذکر شده، مسئله «قتل هویت حقوقی» است. در این فرآیند، هوش مصنوعی با شبیه‌سازی:

• چهره

• صدا

• امضا

• سبک نوشتاری

• الگوی رفتاری

می‌تواند از طرف یک فرد، قرارداد منعقد کند، پیام ارسال کند، پول منتقل کند یا حتی مرتکب جرم شود. این مسئله، یکی از پیچیده‌ترین چالش‌های حقوقی معاصر را ایجاد کرده است؛ زیرا در نگاه اول، تمام شواهد به نام شخص بی‌گناه ثبت می‌شوند و اثبات بی‌گناهی او بسیار دشوار خواهد بود.

۳. پول‌شویی مبتنی بر رمزارز و بلاکچین

بلاکچین با وجود شفافیت ظاهری، به دلیل غیرمتمرکز بودن و امکان پنهان‌سازی هویت، بستر مناسبی برای پول‌شویی، تأمین مالی تروریسم و انتقال منابع غیرقانونی پدید آورده است

مجرمان با بهره‌گیری از رمزارزها می‌توانند:



• منشأ پول را مخفی کنند

• تحریم‌ها را دور بزنند

• تراکنش‌های غیرقابل ردیابی انجام دهند

• سرمایه‌های نامشروع را قانونی جلوه دهند

بخش چهارم: چالش‌های حقوقی و کیفری ناشی از جرایم مبتنی بر هوش مصنوعی

یکی از مهم‌ترین ابعاد جرایم مبتنی بر هوش مصنوعی، پیچیدگی‌های حقوقی ناشی از آن است. در حقوق جزای سنتی، ارکان سه‌گانه جرم شامل عنصر قانونی، عنصر مادی و عنصر روانی بر پایه کنش انسانی تحلیل می‌شود؛ اما زمانی که یک سیستم هوشمند به صورت نیمه‌خودکار یا تمام‌خودکار عملی را انجام می‌دهد، این پرسش بنیادین مطرح می‌شود که:

فاعل واقعی جرم چه کسی است؟

در این حالت سه سناریو قابل تصور است:

۱. هوش مصنوعی صرفاً «ابزار» است و انسان مباشر جرم است

۲. هوش مصنوعی بدون قصد مستقیم انسان ولی به دلیل طراحی معیوب، جرم را

محقق کرده است

۳. هوش مصنوعی مستقل از اراده و کنترل آنی انسان اقدام به عمل کرده است



در سناریوی سوم، مفهوم کلاسیک «قصد مجرمانه» (*Mens Rea*) با بحران مواجه می‌شود، زیرا هوش مصنوعی فاقد اراده، وجدان، ادراک اخلاقی و مسئولیت‌پذیری انسانی است. در نتیجه، بسیاری از نظریه‌پردازان معتقدند که نمی‌توان هوش مصنوعی را فاعل جرم دانست، بلکه باید به سراغ انسان‌های درگیر در چرخه تولید، آموزش و بهره‌برداری از آن رفت.

مسئولیت کیفری در جرایم مبتنی بر هوش مصنوعی

در این نوع جرایم، چندین شخص بالقوه می‌توانند مسئول تلقی شوند:

۱. کاربر (*User*)

اگر فرد آگاهانه از هوش مصنوعی برای ارتکاب جرم استفاده کند (مانند جعل تصویر، تولید پیام‌های فیشینگ، یا نوشتن بدافزار)، مسئولیت کیفری او مشابه فاعل سنتی جرم خواهد بود.

۲. برنامه‌نویس یا طراح الگوریتم

در صورتی که برنامه‌نویس با علم به امکان سوءاستفاده یا با هدف مجرمانه، الگوریتمی خطرناک طراحی کرده باشد، می‌توان نوعی معاونت یا مشارکت در جرم را برای وی متصور شد.

۳. شرکت یا پلتفرم ارائه‌دهنده

اگر پلتفرم بدون ایجاد سازوکارهای کنترلی، به تولید و انتشار گسترده محتوای مجرمانه کمک کند، بحث «مسئولیت کیفری اشخاص حقوقی» مطرح می‌شود.



در بسیاری از نظام‌های حقوقی هنوز پاسخ روشن و واحدی برای این وضعیت وجود ندارد و همین، بزرگ‌ترین خلأ سیاست جنایی در مواجهه با هوش مصنوعی است.

ادله اثبات جرم در فضای مبتنی بر هوش مصنوعی

ادله الکترونیکی در جرایم سایبری همواره محل بحث بوده‌اند، اما در جرایم مرتبط با هوش مصنوعی، این مسئله پیچیده‌تر می‌شود؛ زیرا:

- تصاویر و ویدئوها می‌توانند کاملاً جعلی ولی بسیار واقعی باشند
- صداها به صورت دقیق شبیه‌سازی می‌شوند
- رفتارهای دیجیتالی به صورت خودکار تولید می‌شوند
- منشأ داده‌ها مخفی یا تغییر داده می‌شود

در نتیجه:

۱. ارزش اثباتی فیلم و عکس کاهش می‌یابد
۲. نیاز به کارشناسان فنی پیشرفته افزایش می‌یابد
۳. دادگاه‌ها ناچار به بازنگری در معیارهای پذیرش دلیل می‌شوند

این وضعیت می‌تواند آینده آیین دادرسی کیفری را به شدت متحول سازد و ضرورت تدوین قواعد جدید برای «ادله مبتنی بر هوش مصنوعی» را برجسته می‌کند.



بخش ششم: تحلیل تطبیقی موضوع

در اتحادیه اروپا، رویکرد اصلی در مواجهه با هوش مصنوعی، پیشگیرانه و مبتنی بر مدیریت ریسک است. در این مدل:

• کاربردهای پرخطر ممنوع یا محدود می‌شوند

• توسعه‌دهندگان ملزم به شفاف‌سازی الگوریتم‌ها هستند

• استفاده از هوش مصنوعی در امور حساس (قضاوت، پلیس، امنیت) به شدت کنترل می‌شود.

در مقابل، در بسیاری از کشورهای در حال توسعه، از جمله ایران، مقررات مشخص و اختصاصی در این زمینه وجود ندارد و قواعد فعلی پاسخگوی پیچیدگی‌های جدید نیست.

این تفاوت، خطر «پناهگاه امن مجرمان دیجیتال» را در کشورهایی با ضعف قانون‌گذاری افزایش می‌دهد.

راهبردهای پیشنهادی برای سیاست‌گذاری ایران

در پرتو یافته‌های این پژوهش، پیشنهاد می‌شود:

۱. تدوین قانون جامع هوش مصنوعی با محوریت حقوق کیفری

۲. جرم‌انگاری تولید و توزیع ابزارهای مبتنی بر هوش مصنوعی با اهداف مجرمانه

۳. ایجاد بانک تخصصی ادله دیجیتال



۴. آموزش تخصصی قضات، وکلا و ضابطان در زمینه *AI*

۵. همکاری بین‌المللی در شناسایی و تعقیب جرایم فرامرزی

نتیجه‌گیری

هوش مصنوعی پدیده‌ای خنثی نیست؛ بلکه ابزاری است که بسته به نحوه استفاده، می‌تواند موجب پیشرفت یا تهدید شود. در حوزه حقوق کیفری، این فناوری با دگرگونی در نحوه ارتکاب جرم، هویت مجرم و ماهیت ادله، چالش‌های بنیادینی برای نظام عدالت کیفری ایجاد کرده است. اگر سیاست جنایی کشورها با این تحول همگام نشود، شکاف عمیقی میان فناوری و قانون ایجاد می‌گردد که نتیجه آن، افزایش جرایم پنهان، گسترش بی‌عدالتی و تضعیف اعتماد عمومی خواهد بود. بر این اساس، تنها راهکار مؤثر، گذار از رویکرد واکنشی به رویکرد پیشگیرانه، علمی و آینده‌نگر در تنظیم‌گری هوش مصنوعی است.



منابع و مآخذ

- آقاخانی، کوروش. (۱۳۹۸). تأثیر هوش مصنوعی در فرآیند آموزش و یادگیری. نشریه علمی پژوهشی فناوری آموزش، ۴(۲)، ۲۴-۳۷.
- ابن ابوتراب، سید احسان (۱۳۹۲) کاربرد ربات های صنعتی در صنایع مختلف، مجله فنی مهندسی ساخت و تولید - شماره ۴۶
- اعظم السادات حسینی و دیگران (۱۳۹۱) امکان سنجی پیاده سازی جراحی از راه دور در بیمارستانهای آموزشی درمانی تابعه دانشگاههای علوم پزشکی شهر تهران، مدیریت اطلاعات سلامت / دوره ی نهم / شماره ی اول / فروردین و اردیبهشت ۹۱
- بیگ زاده، ابراهیم (۱۳۷۹) سازمان های غیر دولتی و حقوق بین الملل، مجله تحقیقات حقوقی، شماره ۳۲-۳۱، پاییز- زمستان ۱۳۷۹
- حاجیان، زهرا (۱۳۹۰) رباتیک انقلاب آینده در زندگی یشر، ویژه نامه ی روزنامه خراسان، شماره انتشار ۱۸۰۸۰
- حیدری، مراد، نجفی، علی. (۱۳۹۹). کاربرد هوش مصنوعی در آموزش و یادگیری. مجله فناوری آموزش، ۲(۱)، ۱۲-۲۳.
- کاظمی، سعید (۱۳۹۸). کاربردهای هوش مصنوعی در آموزش. مجله پژوهش های آموزش و یادگیری در علوم پزشکی، ۷(۲)، ۴۱-۵۲.
- زندیه، میترا و دیگران (۱۳۸۸) جراحی رباتیک تحولی در تکنیک های جراحی نوین، دوفصلنامه دانشکده های پرستاری و مامایی استان گیلان، سال ۱۹، شماره ۶۱
- ساعد، نادر (۱۳۸۶) تحلیل هنجارین رژیم کنترل فناوری موشکی و الزامات دفاعی جمهوری اسلامی ایران، مجله سیاست دفاعی سال پانزدهم، شماره ۵۹



- قاسمی، علی و ویکتور بارین، چهاربخش (۱۳۹۰) رویه قضایی دیوان بین‌المللی دادگستری در خصوص دفاع مشروع پس از رویداد یازدهم سپتامبر ۲۰۰۱، مجله حقوقی بین‌المللی، نشریه مرکز امور حقوقی بین‌المللی ریاست جمهوری، سال ۲۸، شماره ۴۵
- قربان‌نیا، ناصر (۱۳۹۰) حقوق بشر و حقوق بشردوستانه، تهران، سازمان انتشارات پژوهشگاه فرهنگ و اندیشه اسلامی
- کمیسیون حقوق بین‌الملل سازمان ملل متحد، (۱۳۹۰) مسوولیت بین‌المللی دولت، (مترجم: علیرضا ابراهیم گل) تهران، ناشر: موسسه مطالعات و پژوهشهای حقوقی شهر دانش
- -مگ دوگال، رابرت (۱۳۸۲) چشم انداز کنترل اشاعه‌ی موشکی، رژیم کنترل فناوری موشکی و جهان پهناور، (ترجمه عبدالحسین حجت زاده)، فصلنامه نگاه، سال چهارم، شماره ۴۱ دی و بهمن ۱۳۸۲
- ملکی، محمد رضا، رئیسی، لیلا و محمدزاده ابراهیمی، فرزاد (۱۳۹۲) کاربرد هواپیمای بدون سرنشین: تحولی نوین در عرصه جنگ‌های مدرن و پیامدهای حقوقی آن، فصلنامه تخصصی علوم سیاسی، سال نهم، شماره بیست و سوم، تابستان ۹۲
- وفایی، محدثه، وثوقی، منوچهر و دیگران (۱۳۹۴) کاربرد نانو الکترونیک در ساخت بافت سایبورگ، ماهنامه فناوری نانو، سال چهاردهم، شماره ۴، پیاپی ۲۱۳، تیر ماه ۹۴

(ب) منابع انگلیسی

- Ford, M. (۲۰۱۸). Artificial intelligence in education: Promises and implications for teaching and learning. *KEDI Journal of Educational Policy*, ۱۵(۳), ۴۰۵-۴۲۲.

- Gandomi, A. , & Haider, M. (۲۰۱۵). *Beyond the hype: Big data concepts, methods, and analytics*. *International Journal of Information Management*, ۳۷(۲), ۱۳۷- ۱۴۴ .
- Huang, R. , Xu, Y. , & Liu, D. (۲۰۱۷). *Adaptive learning and intelligent tutoring systems: A review and future directions*. *IEEE Transactions on Learning Technologies*, ۱۱(۴), ۵۶۴-۵۷۷.
- Khan, B. (۲۰۱۷). *A review of the literature on artificial intelligence in education: Status, pitfalls, and promises*. *Journal of Educational Technology*, ۱۴(۴), ۱۴-۲۵ .
- Liaw, S. S. , & Huang, H. M. (۲۰۱۸). *Artificial intelligence in education: A review*. *International Journal of Distance Education Technologies*, ۱۶(۴), ۱-۱۳ .
- Puentedura, R. R. (۲۰۱۴). *SAMR: A model for enhancing technology integration in the curriculum*. *Journal of Digital Learning in Teacher Education*, ۳۱(۱), ۱-۶ .
- Rose, C. P. , & Straus, S. G. (۲۰۱۵). *Using learning analytics to scale the benefits of higher education*. *New Directions for Institutional Research*, ۲۰۱۵(۱۶۶), ۲۳-۳۹ .
- Sottolare, R. , Graesser, A. , Hu, X. , Goldberg, B. , & Brawner, K. (۲۰۱۹). *Designing adaptive instruction: Personalization principles and applications for technology-mediated learning*. *Routledge* .
- Vanlehn ,K. (۲۰۱۱). *The relative effectiveness of human tutoring, intelligent tutoring systems, and other tutoring systems*. *Educational Psychologist*, ۴۶(۴), ۱۹۷- ۲۲۱ .