فصلنامه پژوهش های نوین در علوم انسانی و حقوق دوره ۲- شماره ۱ – صفحات۱۳۹-۱۲۳
Journal of new Researches in Humanities and Law
ISSN 3060-6101

تحول جرم‌یابی در عصر داده‌های کلان و هوش مصنوعی با تأکید بر چالش‌های حریم خصوصی و مشروعیت ادله دیجیتال

کیمیا شکوهی [1*] ، نجمه دارنجانی شیرازی[2]

۱- کارشناسی رشته حقوق، واحد شیراز، دانشگاه آزاد اسلامی، شیراز، ایران.

۲- پژوهشگر دوره دکتری حقوق‌خصوصی، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران. (مدرس دانشگاه آزاد).

چکیده :

تحول فناوری‌های دیجیتال و ظهور داده‌های کلان و هوش مصنوعی، ساختار سنتی جرم‌یابی را دچار تغییرات بنیادین کرده است. در عصر حاضر، تحلیل داده‌های گسترده و الگوریتم‌های هوشمند امکان شناسایی الگوهای رفتاری، پیش‌بینی وقوع جرم و تسهیل جمع‌آوری ادله را فراهم کرده‌اند، اما در عین حال مجموعه‌ای از چالش‌های حقوقی، اخلاقی و اجتماعی را ایجاد کرده‌اند. هدف پژوهش حاضر بررسی تاثیرات داده‌های کلان و هوش مصنوعی بر جرم‌یابی، شناسایی چالش‌های حریم خصوصی و مشروعیت ادله دیجیتال و ارائه راهکارهای قانونی و تنظیم‌گری است. روش پژوهش مبتنی بر تحلیل حقوقی، مرور ادبیات بین‌المللی و تطبیقی، و بررسی نظام‌های قضایی نوین است که امکان استخراج الگوها، شناسایی چالش‌ها و ارائه پیشنهادات کاربردی را فراهم می‌سازد. یافته‌های مقاله نشان می‌دهد ورود هوش مصنوعی به فرآیندهای جرم‌یابی موجب افزایش دقت، سرعت و کارآمدی تحقیقات جنایی شده، اما همزمان خطرات جدی برای حریم خصوصی شهروندان، سوگیری الگوریتمی، فقدان شفافیت و پیچیدگی در مشروعیت ادله دیجیتال ایجاد می‌کند. علاوه بر این، نبود استانداردهای قانونی بومی و رویه‌های قضایی روشن، استفاده از ادله دیجیتال را با ابهام و چالش مواجه ساخته است. مقاله نتیجه‌گیری می‌کند که تحقق جرم‌یابی هوشمند نیازمند چارچوب‌های قانونی، استانداردهای فنی، شفافیت الگوریتمی، نظارت مستقل و همسویی با اصول حقوق بشر است. تنها با ایجاد چنین چارچوبی، امکان بهره‌برداری از ظرفیت‌های فناوری برای افزایش عدالت کیفری و پیشگیری مؤثر از جرم فراهم می‌شود، بدون آنکه حقوق بنیادین شهروندان یا کرامت انسانی تهدید گردد. نتایج این پژوهش می‌تواند مبنای تدوین سیاست‌های حقوقی، تنظیم‌گری هوش مصنوعی و توسعه ادله دیجیتال در نظام قضایی ایران و سایر کشورها قرار گیرد.

واژگان کلیدی: داده‌های کلان، هوش مصنوعی، ادله دیجیتال، چالش‌های حریم خصوصی، عدالت کیفری

مقدمه :

تحقیقات جنایی در دهه‌های اخیر شاهد یکی از بزرگ‌ترین دگرگونی‌های تاریخی خود بوده است (نجفی و همکاران، ۱۴۰۴)؛ دگرگونی‌ای که نه‌تنها روش‌ها و ابزارهای جرم‌یابی را تغییر داده، بلکه بنیان‌های نظری و هنجاری عدالت کیفری را نیز با چالش‌های بنیادین مواجه ساخته است. ظهور فناوری‌های نوینی همچون کلان‌داده‌ها (Big Data)، هوش مصنوعی، یادگیری ماشین، تحلیل الگوریتمی رفتار، سیستم‌های تشخیص چهره، شنود هوشمند، ردیابی بلادرنگ و پلیس پیش‌بینانه، مفهوم سنتی «کشف جرم» را از فرآیندی انسانی، تجربه‌محور و واکنشی، به کنش هوشمندانه، داده‌محور و پیش‌نگر تبدیل کرده است (Oatley, ۲۰۲۲). امروزه حجم عظیمی از داده‌هایی که پیش‌تر تصور ثبت و تحلیل آن ممکن نبود، با سرعتی بی‌سابقه جمع‌آوری، ذخیره و پردازش می‌شود و به پلیس و دستگاه قضایی امکان می‌دهد الگوهای رفتاری، روابط پنهان، پیش‌بینی ارتکاب جرم و تشخیص مظنونین بالقوه را با دقتی چشمگیر استخراج کنند (موسوی و همکاران، ۱۴۰۰). این تحولات درحالی صورت می‌گیرد که مرزهای سنتی میان «زندگی خصوصی»، «اطلاعات عمومی» و «حوزه امنیت عمومی» به‌شدت در حال فروریختن است و بسیاری از داده‌هایی که در بسترهای دیجیتال تولید می‌شود، در عمل بدون آگاهی افراد، به‌عنوان ماده خام جرم‌یابی مدرن مورد استفاده قرار می‌گیرد.

با وجود مزایای بی‌تردید این فناوری‌ها در ارتقای سرعت کشف جرم، کاهش هزینه‌های پلیسی، افزایش امنیت عمومی، کاهش خطای انسانی و تسهیل تصمیم‌گیری قضایی، گسترش داده‌کاوی و هوش مصنوعی در نظام عدالت کیفری پرسش‌های اساسی و پیچیده‌ای را در حوزه حقوق کیفری، آیین دادرسی، حقوق بشر و اخلاق فناوری مطرح کرده است (Ushakov et al., ۲۰۲۱).

نخست آنکه، افزایش توان نظارتی پلیس و نهادهای امنیتی، به‌ویژه در قالب نظارت‌های دائمی، تراکمی و مبتنی بر کلان‌داده‌ها، اساس حق بنیادین حریم خصوصی و حق بر داده‌های شخصی را در معرض تهدید قرار می‌دهد. جامعه‌ای که در آن هر کنش روزمره ـ از خرید اینترنتی تا جست‌وجوی ساده، از حضور در فضای شهری تا تعاملات مجازی ـ به‌صورت مداوم رصد، تحلیل و ذخیره می‌شود، به‌تدریج از فضای آزاد شهروندی فاصله گرفته و به سمت جامعه‌ای نظارتی، شبه‌پان‌اپتیکونی و مبتنی بر کنترل رفتاری سوق می‌یابد. این امر پرسش مهمی را ایجاد می‌کند: آیا امنیت بیشتر، می‌تواند مجوزی کافی برای نفوذ گسترده در زندگی خصوصی افراد باشد؟

دوم آنکه، مشروعیت ادله دیجیتال در عصر هوش مصنوعی با چالش‌های متعددی مواجه است. هرچند ادله دیجیتال ظرفیت عظیمی برای اثبات جرم، بازسازی صحنه جرم، تحلیل ترافیک داده، ردیابی مخابراتی، کشف ارتباطات مجرمانه و تعیین رفتارهای مشکوک دارد، اما ماهیت الکترونیکی، قابلیت دستکاری، امکان ایجاد داده‌های جعلی، تغییرپذیری اَبرساختارهای دیجیتال، وابستگی به الگوریتم‌های پیچیده و عملاً غیرشفاف بودن فرآیند تحلیل الگوریتمی، اعتبار و پذیرش ادله را در دادگاه‌ها با تردیدهای جدی روبه‌رو می‌سازد (Wankhade et al., ۲۰۲۲). مسئله «زنجیره حفاظت» (Chain of Custody) در ادله دیجیتال نسبت به ادله سنتی چندین برابر حساس‌تر است، چراکه کوچک‌ترین خلل در ثبت، ضبط یا انتقال داده می‌تواند نتیجه تحلیل را به‌طور کامل غیرقابل اعتماد سازد. افزون بر آن، تحولاتی همچون Deepfake، تولید تصاویر و ویدئوهای هوش مصنوعی، جعل صوت و بازتولید رفتار دیجیتال، معادلات سنتی اصالت و حجیت دلیل را به‌طور اساسی دگرگون کرده و آینده فرآیند دادرسی را با پرسش‌های نوپدید مواجه ساخته است (موسوی‌فرد و همکاران، ۱۴۰۴).

سومین چالش اساسی، مسئله تبعیض الگوریتمی و عدالت کیفری است. مدل‌های هوش مصنوعی به‌طور طبیعی بازتابی از داده‌هایی هستند که با آن آموزش دیده‌اند. اگر داده‌ها دارای سوگیری‌های طبقاتی، جنسیتی، قومیتی یا جغرافیایی باشند ـ که در اغلب موارد هستند ـ خروجی مدل نیز ناگزیر سوگیرانه خواهد بود. این خطر وجود دارد که تکنیک‌های تحلیل پیش‌بینانه، افراد متعلق به مناطق محروم را بیشتر در معرض نظارت قرار دهد، نسبت به رفتارهای خاص حساسیت بیش از حد نشان دهد، یا حتی برخی گروه‌ها را به‌صورت ناعادلانه مظنون بالقوه تلقی کند. این پدیده ـ که با عنوان Algorithmic Bias شناخته می‌شود ـ تهدیدی مستقیم برای اصل برائت، اصل منع تبعیض و اصول بنیادین دادرسی عادلانه محسوب می‌شود. بنابراین برخلاف تصور رایج، فناوری به‌تنهایی بی‌طرف نیست و می‌تواند خطا یا تبعیض را در مقیاسی بزرگ‌تر بازتولید یا تقویت کند (Ţical, ۲۰۲٤). از منظر حقوقی، مهم‌ترین مسئله این است که چارچوب‌های سنتی قانون‌گذاری و آیین دادرسی کیفری اساساً برای عصر داده‌های کلان طراحی نشده‌اند. قانون‌گذار در گذشته با نوعی ادله مواجه بود که ماهیت فیزیکی و انسانی داشت؛ اما امروز ادله نه‌تنها غیرملموس، بلکه پویا، وابسته به شبکه‌های پیچیده، حاصل پردازش الگوریتمی و تابع محاسباتی پیشرفته‌اند. پرسش‌هایی که مطرح می‌شود بسیار بنیادی است:

- آیا می‌توان نتیجه یک مدل هوش مصنوعی را به‌عنوان دلیل مستقل در دادگاه پذیرفت؟
- آیا ضابطان می‌توانند بدون حکم قضایی داده‌های کلان را تحلیل کنند؟
- حد و مرز «رضایت ضمنی» کاربران در فضای مجازی چیست؟
- آیا قاضی می‌تواند از الگوریتمی استفاده کند که فرایند درونی آن برای او قابل فهم نیست؟

در عرصه تطبیقی نیز، چالش‌های مشابهی در نظام‌های حقوقی مختلف دیده می‌شود. آمریکا با رویکرد امنیت‌محور، اروپا با رویکرد مبتنی بر حفاظت حداکثری از حریم خصوصی و کشورهای آسیایی با سیاست‌گذاری‌های متفاوت، هرکدام تلاش کرده‌اند تعادلی میان امنیت و آزادی ایجاد کنند؛ اما هیچ نظام حقوقی هنوز مدلی کامل و بی‌نقص ارائه نکرده است. در ایران نیز، هرچند اسناد پراکنده‌ای درباره ادله دیجیتال، جرائم رایانه‌ای و شنود مخابراتی وجود دارد، اما تحول فناوری از سرعت رشد قانون‌گذاری پیشی گرفته و نیاز به بازنگری مبانی اصولی جرم‌یابی بیش از هر زمان احساس می‌شود. بنابراین، مسئله اصلی این مقاله بررسی این است که جرم‌یابی در عصر داده‌های کلان و هوش مصنوعی چگونه دگرگون شده، و این تحول چه چالش‌هایی برای حریم خصوصی، مشروعیت ادله دیجیتال و اصول عدالت کیفری به‌وجود آورده است؟ هدف این پژوهش آن است که با تحلیل نظری و تطبیقی، ضمن تبیین فرصت‌ها و تهدیدهای فناوری‌های نوین در فرآیند کشف جرم، چارچوبی حقوقی و عملی برای تنظیم‌گری جرم‌یابی هوشمند ارائه دهد؛ چارچوبی که بتواند ضمن بهره‌گیری از ظرفیت‌های فناوری، از اصول بنیادین حقوق کیفری، حقوق بشر و دادرسی عادلانه پاسداری کند.

۲. تحول جرم‌یابی و گذار از روش‌های سنتی به فناوری‌های هوشمند

جرم‌یابی در معنای کلاسیک همواره بر مشاهده مستقیم، تجربه میدانی، شهود حرفه‌ای مأموران، اظهارات شهود، آثار فیزیکی و روش‌های آزمایشگاهی متکی بود. این مدل سنتی، گرچه طی دهه‌ها کارآمدی نسبی خود را نشان داده و همچنان در بسیاری از حوزه‌ها غیرقابل جایگزین است، اما در جهان امروز با چالش‌هایی روبه‌روست که آن را از پاسخ‌گویی کافی به پیچیدگی‌های جرم در عصر دیجیتال بازمی‌دارد. رشد سریع شبکه‌های اجتماعی، جابه‌جایی‌های گسترده مالی، توسعه زیرساخت‌های الکترونیکی، افزایش

تعاملات مجازی و گسترش سبک زندگی دیجیتال سبب شده است بخش عمده‌ای از نشانه‌های ارتکاب جرم نه در صحنه فیزیکی بلکه در فضاهای مجازی، تراکنش‌ها، ردپاهای داده‌ای، لاگ‌های سیستم‌ها و ارتباطات الکترونیکی پنهان باشد (محمدی‌نیا و همکاران، ۱۴۰۲). از همین‌رو روش‌های سنتی که عمدتاً به «آثار مشهود» و «شواهد عینی فیزیکی» محدود بود، قادر نیست با سرعت و پیچیدگی جرائم نوپدید هماهنگ شود. در چنین بستری، فناوری‌های نوین به تدریج ساختار جرم‌یابی را متحول کرده و آن را وارد مرحله‌ای کرده‌اند که می‌توان آن را «جرم‌یابی هوشمند» نامید.

گام نخست این تحول، ورود فناوری اطلاعات به فرآیند کشف جرم بود؛ فناوری‌ای که با ایجاد امکان ثبت و ذخیره حجم عظیمی از داده‌ها، مدیریت پرونده‌ها، تحلیل الگوهای رفتاری و ردیابی الکترونیکی مظنونین، به پلیس امکان داد تصمیمات دقیق‌تر و علمی‌تری اتخاذ کند. اما تحولی که امروز با آن مواجهیم، فراتر از کاربرد ساده ابزارهای دیجیتال است. اکنون هوش مصنوعی و کلان‌داده‌ها نه‌تنها ابزارهای کمکی تحقیق نیستند، بلکه عملاً «شریک تصمیم‌ساز» و گاهی «تصمیم‌گیر» شده‌اند. این فناوری‌ها به کمک یادگیری ماشین قادرند رفتار مجرمانه را بر اساس داده‌های گذشته پیش‌بینی کنند، ارتباطات پنهان افراد را آشکار سازند، چهره‌ها را در کسری از ثانیه از میان میلیون‌ها تصویر شناسایی کنند، و حتی الگوهای غیرعادی در تراکنش‌های مالی یا حرکت‌های شهری را تشخیص دهند. این دگرگونی، جرم‌یابی را از حالتی پسینی و واکنشی به حالتی «پیش‌نگر» و حتی «پیش‌دستانه» تبدیل می‌کند؛ یعنی پیش از وقوع جرم، احتمال وقوع آن سنجیده شده و مکان، زمان و افراد مورد ریسک شناسایی می‌شوند. چنین تغییری، بنیان معرفت‌شناسی سنتی جرم‌یابی را کاملاً دگرگون کرده است (محمد نعمتی و همکاران، ۱۴۰۴).

در روش‌های کلاسیک، «انسان» محور اصلی فرآیند کشف جرم بود؛ مأمور جرم‌شناس با مشاهده صحنه جرم، جمع‌آوری آثار مادی و تحلیل منطقی به نتیجه می‌رسید. اما در روش‌های نوین مبتنی بر هوش مصنوعی، «داده» و «الگوریتم» در مرکز فرآیند قرار گرفته‌اند و مأمور انسانی بیشتر نقش تحلیل‌گر یا ناظر بر عملکرد سیستم را ایفا می‌کند. این گذار از انسان‌محوری به داده‌محوری، تبعات گسترده‌ای در حقوق کیفری و آیین دادرسی دارد. وقتی تصمیمات اولیه و حتی برخی تحلیل‌های کلیدی مبتنی بر خروجی الگوریتم‌ها اتخاذ می‌شود، پرسش‌هایی درباره مسئولیت، اعتبار تحلیل، احتمال خطا، سوگیری و شفافیت مطرح می‌گردد. به بیان دیگر، فناوری نه‌تنها ابزار، بلکه «عامل» تأثیرگذار در فرایند عدالت کیفری می‌شود و همین امر ضرورت بازتعریف برخی مفاهیم سنتی مانند دلیل، ظن، کشف، تفتیش و حتی قضاوت را به‌وجود می‌آورد. نقطه عطف دیگر در تحول جرم‌یابی، قدرت بی‌سابقه کلان‌داده‌هاست. در جهان دیجیتال، هر فرد روزانه هزاران داده تولید می‌کند؛ از موقعیت مکانی گرفته تا تعاملات آنلاین، علایق، خریدها، فعالیت‌های روزمره، تصاویر، پیام‌ها و حتی الگوهای زیستی. این داده‌ها که در ابتدا صرفاً محصول جانبی فعالیت‌های دیجیتال بودند، امروز به ماده خام جرم‌یابی مدرن تبدیل شده‌اند. تحلیل این حجم از داده، تنها با ابزارهایی ممکن است که بتوانند در زمانی بسیار کوتاه، الگوهای پنهان را استخراج و رفتارها را طبقه‌بندی کنند. اینجاست که یادگیری ماشین، شبکه‌های عصبی، تحلیل خوشه‌ای، تشخیص آنومالی، مدل‌های پیش‌بینی و سیستم‌های رتبه‌بندی ریسک وارد عرصه می‌شوند. نتیجه آن است که مأموران تحقیق اکنون قادرند مواردی را شناسایی کنند که در روش‌های سنتی کاملاً غیرقابل تشخیص بود. برای مثال، تشخیص الگوی رفت‌وآمد یک فرد خاص در شهری شلوغ، تحلیل ارتباطات مجرمانه میان گروه‌های پنهان، کشف پول‌شویی در میان هزاران تراکنش، یا شناسایی نقشه‌برداری‌های مشکوک شهری، تنها به کمک تحلیل هوشمند ممکن است.

با این‌حال، این تحول صرفاً جنبه فنی و تکنیکی ندارد؛ بلکه پیامدهای حقوقی و اخلاقی گسترده‌ای نیز دارد. یکی از مهم‌ترین پیامدها، تغییر نسبت میان «حق فرد» و «قدرت دولت» است. در گذشته، جمع‌آوری اطلاعات درباره افراد مستلزم حضور فیزیکی، روش‌های سنتی تفتیش و کسب مجوزهای قضایی بود، اما امروز بسیاری از داده‌ها بدون هیچ‌گونه مداخله مستقیم، توسط پلتفرم‌ها و سرویس‌های دیجیتال ثبت و ذخیره می‌شود. بنابراین، دسترسی دولت به اطلاعات شهروندان بالقوه افزایش یافته و این امر در صورت نبود چارچوب قانونی روشن، می‌تواند منجر به نقض سیستماتیک حریم خصوصی شود. این مسأله اهمیت زیادی دارد، زیرا جرم‌یابی هوشمند مرزهای سنتی میان «اطلاعات عمومی» و «اطلاعات خصوصی» را کمرنگ می‌کند و نوعی نظارت دائمی و فراگیر ایجاد می‌نماید.

از سوی دیگر، فناوری‌های هوشمند موجب شده‌اند که دقت و صحت برخی روش‌های جرم‌یابی افزایش یابد. تشخیص چهره، تحلیل تصاویر دوربین‌های شهری، پردازش بیومتریک، تحلیل صوت و ردیابی دیجیتال، همگی باعث شده‌اند که فرآیند کشف جرم سریع‌تر و مبتنی بر اطلاعات دقیق‌تر انجام شود. این پیشرفت‌ها به‌ویژه در مواردی مانند کشف جرائم سازمان‌یافته، تروریسم، جرائم سایبری، قاچاق انسان و مواد مخدر اهمیت دارد، زیرا این دسته از جرائم معمولاً گسترده، پیچیده و فراملی هستند. با این وجود، تکیه بیش‌ازحد بر فناوری ـ بدون در نظر گرفتن خطاهای احتمالی ـ می‌تواند خطرناک باشد. فناوری‌های تشخیص چهره ممکن است در تشخیص افراد از اقلیت‌های خاص دقت کمتری داشته باشند، مدل‌های پیش‌بینی ممکن است ریسک برخی افراد را بر اساس داده‌های ناقص یا سوگیرانه بیش از حد برآورد کنند، و الگوریتم‌ها ممکن است تحلیل‌هایی انجام دهند که برای انسان قابل فهم یا قابل بررسی نباشد.

تحول جرم‌یابی از سنتی به هوشمند، درواقع نمایانگر گذار از «فردمحوری» به «الگوریتم‌محوری»، از «دلیل مستقیم» به «دلیل داده‌محور»، از «تحلیل انسانی» به «تحلیل محاسباتی» و از «واکنش به جرم» به «پیش‌بینی جرم» است. این گذار، همان‌قدر که فرصت‌زا و ضروری به‌نظر می‌رسد، به همان اندازه نیازمند تنظیم‌گری حقوقی، نظارت قضایی، چارچوب‌های اخلاقی و استانداردهای شفاف است تا فناوری به ابزاری برای کشف جرم و نه ابزاری برای نقض آزادی‌های بنیادین تبدیل شود. به‌بیان دیگر، تحول جرم‌یابی در عصر داده‌های کلان و هوش مصنوعی یک ضرورت انکارناپذیر است، اما این تحول باید درون چارچوبی صورت گیرد که بتواند بین امنیت عمومی و احترام به حقوق شهروندان تعادل ایجاد کند (لطیف‌زاده، ۱۴۰۳).

جدول ۱: مقایسه رویکرد سنتی و هوشمند در جرم‌یابی

جنبه	جرم‌یابی سنتی	جرم‌یابی مبتنی بر داده‌های کلان و هوش مصنوعی
رویکرد	واکنشی، پرونده‌محور	پیش‌بینانه، تحلیل‌محور
ابزارها	تحقیقات میدانی، شهادت، ادله فیزیکی	الگوریتم‌های یادگیری ماشین، کلان‌داده، تحلیل الگو
سرعت و کارآمدی	پایین، زمان‌بر	بالا، پردازش سریع حجم عظیم داده‌ها
قابلیت پیش‌بینی جرم	محدود	توانایی پیش‌بینی بر اساس الگوهای رفتاری

خطرات و چالش‌ها	خطاهای انسانی، محدودیت داده‌ها	سوگیری الگوریتمی، تهدید حریم خصوصی، پیچیدگی ادله دیجیتال

۳. داده‌های کلان و هوش مصنوعی در تحقیقات جنایی

رشد بی‌وقفه فناوری‌های دیجیتال سبب شده است که هر فعالیت انسانی ـ خواه آگاهانه و خواه ناخواسته ـ به تولید داده منجر شود؛ داده‌هایی که در قالب موقعیت مکانی، تعاملات شبکه‌های اجتماعی، تراکنش‌های مالی، جست‌وجوهای اینترنتی، تصاویر دوربین‌ها، پیام‌های متنی، سوابق سلامت، تاریخچه مرورگر، تماس‌ها و حتی الگوهای رفتاری و زیستی ثبت و ذخیره می‌شوند. این حجم عظیم و متنوع از داده‌ها، که در ادبیات علمی با عنوان «کلان‌داده» شناخته می‌شود، چنان گسترده، پویا و پیچیده است که تحلیل آن با روش‌های کلاسیک تقریباً ناممکن است. اما همین شرایط، نقطه آغاز ورود هوش مصنوعی به تحقیقات جنایی است؛ جایی که الگوریتم‌ها می‌توانند آنچه را ذهن انسان قادر به تشخیص آن نیست، از میان انبوه داده‌ها بیرون بکشند و تحلیل کنند. داده‌های کلان ماهیت جرم‌یابی را دگرگون کرده‌اند؛ زیرا اطلاعات مربوط به رفتار مجرمانه یا مظنونانه دیگر صرفاً در صحنه جرم یا میان اشخاص محدود نمی‌شود، بلکه در تاروپود زندگی دیجیتال کاربران پراکنده است و قابلیت استخراج الگوهای رفتاری را فراهم می‌سازد.

ویژگی‌های کلیدی کلان‌داده‌ها، یعنی حجم بالا (Volume)، سرعت تولید و پردازش سریع (Velocity)، تنوع انواع داده‌ها (Variety)، عدم قطعیت و نادقیق‌بودن برخی داده‌ها (Veracity)، و ارزش‌افزوده‌ی استخراجی (Value)، موجب شده است که پلیس و نهادهای امنیتی قادر باشند به جای تمرکز بر نمونه‌های محدود، رفتارهای گسترده و الگوهای کلانی را شناسایی کنند که پیش‌تر امکان رصد آن وجود نداشت. برای مثال، تحلیل رفتار جمعیتی در مناطق شهری می‌تواند نشان دهد که در چه خیابان‌هایی پتانسیل وقوع جرم بیشتر است؛ بررسی حجم بزرگی از داده‌های مالی می‌تواند ارتباطات مشکوک یا الگوهای پول‌شویی را آشکار سازد؛ ردیابی داده‌های موقعیت جغرافیایی گوشی‌ها می‌تواند حرکت مظنونین را در نقاط مختلف شهر با دقتی بی‌نظیر ترسیم کند؛ و تحلیل شبکه‌ای ارتباطات مجازی می‌تواند گروه‌های مجرمانه پنهان را که در ظاهر هیچ ارتباطی با یکدیگر ندارند، افشا کند. این ظرفیت‌ها، نظام تحقیقات جنایی را از حالت محدود و واکنشی به حالتی فراگیر، تحلیلی و داده‌محور تبدیل کرده است (شریف‌زاده و همکاران، ۱۴۰۳).

در این میان هوش مصنوعی نقش بنیادی‌تری ایفا می‌کند؛ زیرا کلان‌داده‌ها بدون دخالت الگوریتم‌های یادگیری ماشین (Machine Learning)، یادگیری عمیق (Deep Learning) و تحلیل محاسباتی قابل استفاده نیستند. الگوریتم‌های هوشمند قادرند مجموعه‌های داده بسیار بزرگ را در زمانی کوتاه پردازش کرده و الگوهایی را استخراج کنند که برای انسان غیرقابل تشخیص است. برای مثال، سامانه‌های تشخیص چهره که بر پایه شبکه‌های عصبی عمیق کار می‌کنند می‌توانند چهره افراد را حتی از میان میلیون‌ها تصویر با احتمال خطای بسیار کم شناسایی کنند. همین فناوری در ترکیب با داده‌های ویدئویی دوربین‌های شهری، امکان ردیابی مستمر افراد در سطح کلانشهرها را فراهم می‌سازد. هوش مصنوعی همچنین قادر است الگوهای رفتاری غیرعادی را در میان داده‌ها تشخیص دهد؛ الگوریتم‌های تشخیص آنومالی (Anomaly Detection) می‌توانند رفتارهای غیرطبیعی یک حساب بانکی، الگوهای مشکوک سفر، تغییرات ناگهانی فعالیت‌های آنلاین، یا پیام‌های غیرعادی در شبکه‌های اجتماعی را شناسایی کرده و هشدارهای لازم را صادر کنند. یکی از ابزارهای مهم هوش مصنوعی در تحقیقات جنایی، «پلیس پیش‌بینانه» (Predictive Policing) است؛ مدلی که بر اساس

تحلیل داده‌های تاریخی جرم، الگوهای زمانی و مکانی، ویژگی‌های رفتاری و عوامل اجتماعی، احتمال وقوع جرم در آینده را پیش‌بینی می‌کند. این سیستم‌ها می‌توانند مناطق دارای ریسک بالا را مشخص کنند، زمان‌های محتمل ارتکاب جرم را تعیین کنند، یا حتی فهرستی از افراد دارای احتمال ارتکاب جرم را ارائه دهند. گرچه این روش در ظاهر کارآمد به‌نظر می‌رسد و برخی کشورها از آن برای تخصیص منابع پلیسی بهره می‌برند، اما همین فناوری با پرسش‌های دشوار حقوقی مواجه است:

- آیا می‌توان فردی را به صرف «احتمال بالای ارتکاب جرم» تحت نظر قرار داد؟
- آیا این الگوریتم‌ها داده‌های سوگیرانه و تبعیض‌آمیز را بازتولید نمی‌کنند؟
- مرز میان پیشگیری مشروع و نقض آزادی‌های فردی کجاست؟

این پرسش‌ها نشان می‌دهد که هرچند هوش مصنوعی کارآمدی تحقیقات جنایی را افزایش می‌دهد، اما اگر فاقد تنظیم‌گری مناسب باشد می‌تواند زمینه‌ساز نقض اصول بنیادین حقوق کیفری و حقوق بشر شود.

نکته مهم دیگری که در حوزه ادله دیجیتال اهمیت یافته، قابلیت دستکاری داده‌هاست. برخلاف ادله سنتی که ماهیت فیزیکی داشته و امکان جعل آن محدودتر بود، داده‌های دیجیتال به‌راحتی تغییر می‌کنند، حذف می‌شوند یا بدون بر جای گذاشتن اثر قابل توجهی بازنویسی می‌شوند. این امر نیاز به سازوکارهای دقیق برای حفظ زنجیره حفاظت، تضمین اصالت، مستندسازی فرآیند جمع‌آوری و جلوگیری از دخالت انسانی یا سیستمی در داده‌ها را افزایش می‌دهد. هوش مصنوعی نیز در این حوزه دو نقش متضاد دارد: از یک‌سو ابزار قدرتمندی برای تشخیص جعل، دستکاری یا تغییر داده‌هاست و می‌تواند با مدل‌های تشخیص اصالت تصاویر، ویدئوها و فایل‌ها، جعل دیجیتال را تشخیص دهد؛ اما از سوی دیگر، خود هوش مصنوعی می‌تواند ابزاری برای تولید ویدئوهای جعلی، تصاویر ساختگی، صداهای بازتولیدی و Deepfake باشد. این دوگانگی، مبارزه میان ادله دیجیتال و جعل دیجیتال را پیچیده‌تر کرده و چالش‌های مشروعیت دلیل را دوچندان ساخته است.

یکی از مهم‌ترین عرصه‌های کاربرد هوش مصنوعی در تحقیقات جنایی، تحلیل شبکه اجتماعی (Social Network Analysis) است. این روش به کمک الگوریتم‌های گراف‌محور، ارتباطات افراد را ـ چه واقعی و چه مجازی ـ تحلیل می‌کند و می‌تواند رهبران پنهان شبکه‌های مجرمانه، نقش‌های کلیدی، واسطه‌ها، و مسیرهای انتقال اطلاعات را استخراج کند. این نوع تحلیل در کشف جرائم سازمان‌یافته، تروریسم و قاچاق انسان اهمیت فراوانی دارد. اما این تحلیل نیز مستلزم دسترسی به حجم عظیمی از داده‌های خصوصی کاربران است که در صورت نبود ضمانت اجراهای قانونی، می‌تواند منجر به نقض گسترده حریم خصوصی شود. به‌طور کلی، ورود داده‌های کلان و هوش مصنوعی به تحقیقات جنایی دو پیامد هم‌زمان داشته است: نخست افزایش چشمگیر کارآمدی در کشف جرم و دوم افزایش خطر نقض حقوق شهروندان. از این‌رو ضرورت دارد که ابزارهای هوشمند در چهارچوبی شفاف، قانونمند و مبتنی بر اصول حقوق کیفری و حقوق بشر به کار گرفته شوند. در غیر این صورت، جامعه در معرض شکل‌گیری «عدالت الگوریتمی» قرار می‌گیرد؛ عدالتی که اگرچه ظاهراً مبتنی بر داده‌هاست، اما در عمل می‌تواند سوگیرانه، ناعادلانه و مغایر با کرامت انسانی باشد. بنابراین کلان‌داده‌ها و هوش مصنوعی نه‌تنها امکانات جدیدی برای کشف جرم فراهم می‌کنند، بلکه نیازمند بازاندیشی در مبانی حقوقی و اخلاقی تحقیقات جنایی‌اند (حیدرپور و همکاران، ۱۴۰۲).

۴. چالش‌های حریم خصوصی در عصر جرم‌یابی هوشمند

جرم‌یابی در عصر داده‌های کلان و هوش مصنوعی با وجود افزایش دقت، سرعت و کارآمدی، یکی از عمیق‌ترین چالش‌های حقوقی را در حوزه حریم خصوصی ایجاد کرده است. تحول در سازوکارهای کشف جرم مبتنی بر الگوریتم‌ها و تحلیل‌های کلان‌داده، مرزهای کلاسیک بین «نظارت مشروع» و «مداخله ناموجه» را به‌شدت مبهم کرده و باعث شده است توازن سنتی میان امنیت عمومی و حقوق بنیادین شهروندان دچار تنش‌های جدی شود (El-Din et al., ۲۰۲۲). حریم خصوصی که در حقوق بشر به‌عنوان حق کنترل فرد بر اطلاعات شخصی و حوزه زندگی خصوصی تعریف می‌شود، در مواجهه با فناوری‌هایی که توان ثبت، ذخیره، استخراج و تحلیل داده‌های ظریف و چندلایه را دارند، در معرض تغییر ماهیت قرار گرفته است. امروزه نهادهای امنیتی و کیفری قادرند از طریق تحلیل موقعیت مکانی، الگوهای تردد، تراکنش‌های مالی، فعالیت‌های شبکه‌های اجتماعی و حتی نشانه‌های زیستی استخراج‌شده از تجهیزات هوشمند، تصویری دقیق و سابقاً ناممکن از رفتار روزمره افراد ترسیم کنند؛ تصویری که نه بر مبنای داده‌های افشاشده بلکه بر پایه استنباط‌های الگوریتمی تولید می‌شود و این امر، نوعی نقض حریم خصوصی استنباطی (Inferential Privacy Violation) محسوب می‌شود.

یکی از مهم‌ترین چالش‌ها در این میان، گسترش نظارت فراگیر و بدون مرز است. بسیاری از فناوری‌های نوین جرم‌یابی، برخلاف ابزارهای کلاسیک همچون بازرسی، شنود یا تفتیش، ماهیتاً «مداخله‌گر» محسوب نمی‌شوند و در نتیجه، نیازمند مجوز قضایی مستقیم نیز نیستند. به‌عنوان نمونه، تحلیل خودکار تصاویر دوربین‌های شهری یا استخراج الگوهای رفتاری کاربران شبکه‌های اجتماعی در مقیاس میلیون‌ها داده، بدون آنکه ضرورتی برای هدف‌گیری فرد مشخصی وجود داشته باشد، انجام می‌شود. چنین سازوکارهایی باعث شکل‌گیری «نظارت بی‌وقفه بر جمعیت» می‌شود؛ نظارتی که اگرچه با هدف پیشگیری از جرم صورت می‌گیرد، اما مرز میان «نظارت عمومی بر محیط» و «نظارت بر تک‌تک افراد بدون ظن معین» را از بین می‌برد. این شرایط، خطر ایجاد جامعه‌ای شبیه به مدل پان‌اپتیکون فوکو را در دل خود دارد؛ جامعه‌ای که در آن افراد دائماً احساس می‌کنند تحت نظارت هستند و این امر آزادی‌های فردی، رفتارهای اجتماعی و حتی سبک زندگی را نیز تحت تأثیر قرار می‌دهد (AL-Marghilani et al., ۲۰۲۲).

چالش دوم، ابهام در مالکیت، کنترل و چرخه عمر داده‌ها است. داده‌هایی که توسط سامانه‌های جرم‌یابی جمع‌آوری می‌شوند، اغلب از منابع متعدد و ناهمگون به‌دست می‌آیند و این پراکندگی باعث می‌شود مسئولیت حقوقی در قبال جمع‌آوری، نگهداری و پردازش آن‌ها نامشخص شود. بسیاری از داده‌ها مانند اطلاعات مکانی تلفن همراه یا داده‌های زیستی ساعت‌های هوشمند، اساساً برای اهداف غیرکیفری تولید می‌شوند اما بعدها در فرآیند جرم‌یابی مورد استفاده قرار می‌گیرند. این استفاده ثانویه، بدون رضایت مستقیم و آگاهانه صاحب داده، برخلاف اصول بنیادین حفاظت داده و اصل «جمع‌آوری حداقلی» است. افزون بر آن، نگهداری بلندمدت این داده‌ها در پایگاه‌های متمرکز، خطر حملات سایبری، دسترسی غیرمجاز و سوءاستفاده داخلی را افزایش می‌دهد و می‌تواند منجر به نقض گسترده حقوق شهروندان شود. حتی در مواردی که داده‌ها به‌طور رسمی حذف می‌شوند، خطر بازشناسایی مجدد از طریق ترکیب با داده‌های دیگر همچنان وجود دارد؛ چالشی که در ادبیات حقوق داده به‌عنوان «توهم ناشناس‌سازی» شناخته می‌شود.

چالش سوم، تبعیض الگوریتمی و اثرات غیرمستقیم بر حریم خصوصی گروه‌ها است. الگوریتم‌های مورد استفاده در جرم‌یابی هوشمند، بر مبنای داده‌های تاریخی آموزش می‌بینند و این داده‌ها خود حامل سوگیری‌های اجتماعی، نژادی، اقتصادی یا جغرافیایی هستند.

نتیجه آن است که سیستم‌های پیش‌بینی جرم یا تشخیص چهره ممکن است رفتارهای افراد یا گروه‌های خاص را بیش از حد پرخطر تحلیل کنند و این امر موجب افزایش نظارت و جمع‌آوری داده از آن‌ها می‌شود. در این حالت، افراد صرفاً به دلیل تعلق به یک منطقه، طبقه اجتماعی یا الگوی رفتاری آماری، بدون سابقه مجرمانه، تحت سطحی از نظارت تبعیض‌آمیز قرار می‌گیرند که نقض آشکار حریم خصوصی و کرامت انسانی است. این نوع نقض، نه مستقیم بلکه ساختاری و جمعی است و به همین دلیل، کشف و مقابله با آن دشوارتر است. در کنار چالش‌های ماهوی، چالش‌های هنجاری و حقوقی نیز مطرح می‌شوند. بسیاری از نظام‌های حقوقی، از جمله ایران، چارچوب کاملی برای تنظیم جمع‌آوری و استفاده از داده‌ها در جرم‌یابی هوشمند ندارند. قوانین سنتی مانند مقررات مربوط به بازرسی، تفتیش، شنود و ادله الکترونیک، برای وضعیت‌هایی طراحی شده‌اند که داده به‌صورت محدود، معین و در کنترل مستقیم پلیس است. اما در عصر داده‌های کلان، داده‌ها بخشی از زیست دیجیتال افراد هستند و در شبکه‌ای از تعاملات اجتماعی تولید می‌شوند. بنابراین پرسش اصلی آن است که آیا نظارت بر محیط دیجیتال بدون ظن قوی، با اصول قانونی بودن جرم‌وجزا، ضرورت، تناسب و کرامت اجتماعی سازگار است؟ پاسخ به این پرسش، نیازمند بازنگری عمیق در اصول حاکم بر حریم خصوصی و تطبیق آن با ویژگی‌های فناوری‌های نوین است (Apene et al., ۲۰۲٤).

از همه مهم‌تر، در جرم‌یابی هوشمند، مرز میان «داده‌های عمومی» و «داده‌های خصوصی» نیز دچار دگرگونی شده است. در گذشته، داده‌های عمومی مانند تصاویر خیابان‌ها یا پست‌های شبکه‌های اجتماعی حریم خصوصی محدودتری داشتند. اما امروزه الگوریتم‌ها قادرند از همین داده‌های عمومی، شناخت عمیقی از وضعیت سیاسی، اقتصادی، رفتاری و حتی عواطف افراد استخراج کنند. در چنین شرایطی، حتی داده‌ای که عموم مردم به آن دسترسی دارند، ممکن است در فرآیند الگوریتمی به داده‌ای بشدت خصوصی تبدیل شود. این تغییر ماهیت، نیازمند توسعه مفهومی جدید از حریم خصوصی است که علاوه بر داده خام، نتایج استنباطی و مدل‌های پیش‌بینی‌کننده را نیز تحت حمایت قرار دهد. در مجموع، چالش‌های حریم خصوصی در عصر جرم‌یابی هوشمند نشان می‌دهد که افزایش ظرفیت‌های نظارتی، بدون ایجاد سازوکارهای قویِ پاسخگویی، شفافیت، محدودیت هدف، نظارت قضایی دقیق و تضمین‌های فنی و حقوقی، می‌تواند به تضعیف بنیادین حقوق شهروندان منجر شود. بنابراین لازم است قوانین کیفری و آیین دادرسی، همگام با تحولات فناورانه، بازنگری و تکمیل شوند تا توازن میان امنیت عمومی و آزادی‌های فردی حفظ گردد.

جدول ۲: چالش‌های حریم خصوصی و حقوقی در جرم‌یابی هوشمند

نوع چالش	توضیح	پیامدها
نظارت فراگیر	جمع‌آوری داده بدون هدف مشخص	محدودیت آزادی فرد، ایجاد احساس پایش دائم
مالکیت و کنترل داده‌ها	داده‌ها از منابع مختلف و بدون مجوز ثانویه جمع‌آوری می‌شوند	نقض حریم خصوصی، امکان سوءاستفاده
تبعیض الگوریتمی	الگوریتم‌ها بر داده‌های سوگیری‌آلود آموزش می‌بینند	نظارت نامتناسب بر گروه‌ها یا افراد

مشروعیت ادله دیجیتال	پیچیدگی انتساب و تغییرپذیری داده‌ها	تردید در حجیت قضایی، مشکل در دفاع متهم
تغییر ماهیت داده‌های عمومی	داده‌های عمومی در تحلیل الگوریتمی خصوصی می‌شوند	تهدید حقوق شهروندی و آزادی‌های فردی

۵. چالش‌های مشروعیت ادله دیجیتال در نظام عدالت کیفری

مشروعیت ادله دیجیتال در نظام‌های عدالت کیفری یکی از چالش‌برانگیزترین مباحث حقوق فناوری در دهه اخیر است. هرچند گسترش فناوری، فرصت‌های بی‌سابقه‌ای را برای کشف جرم، اثبات اتهام و بازسازی صحنه جنایت فراهم کرده است، اما ماهیت «دیجیتال» بودن این ادله، پرسش‌هایی بنیادین درباره اصالت، تمامیت، قابلیت انتساب، حجیت قضایی و استانداردهای جمع‌آوری و تحلیل ایجاد کرده است. برخلاف ادله سنتی که غالباً دارای ماهیت فیزیکی، ملموس و قابل مشاهده هستند، ادله دیجیتال در قالب داده‌های نامرئی، قابل تغییر، وابسته به محیط نرم‌افزاری و فناوری، و مستعد دست‌کاری یا تفسیر نادرست می‌باشند. این ویژگی‌ها موجب شده است که نظام‌های حقوقی برای پذیرش چنین ادله‌ای، نیازمند توسعه استانداردهای چندلایه و ترکیبی باشند؛ استانداردهایی که هم ناظر بر اصول سنتی دادرسی عادلانه باشند و هم پیچیدگی‌های فنی ادله دیجیتال را پوشش دهند.

یکی از بنیادی‌ترین چالش‌ها، مسئله قابلیت انتساب داده دیجیتال به شخص معین است. در ادله کلاسیک، انتساب معمولاً از طریق امضا، اثر انگشت، سند مکتوب یا شهادت صورت می‌گیرد. اما در فضای دیجیتال، داده‌ها در شبکه‌ای از دستگاه‌ها، حساب‌ها، بسترهای ابری و پروتکل‌های رمزنگاری تولید و منتقل می‌شوند. یک پیام، فایل، تراکنش یا فعالیت آنلاین ممکن است از طریق ابزارهای ناشناس‌ساز، VPNها، ربات‌ها یا حساب‌های جعلی انجام شده باشد و تشخیص هویت واقعی فاعل، نیازمند تحلیل‌های پیچیده فنی است. حتی در مواردی که داده به دستگاه یا حساب کاربری خاصی متصل است، همچنان امکان ادعای نفوذ، دسترسی غیرمجاز، مالکیت اشتراکی دستگاه یا سوءاستفاده توسط شخص ثالث وجود دارد. بنابراین اصل «نسبت‌دادن مستقیم» که در ادله فیزیکی پذیرفته است، در حوزه دیجیتال به‌شدت تضعیف می‌شود و این امر نیازمند سطوح جدیدی از اثبات انتساب، مبتنی بر زنجیره شواهد دیجیتال است (Dai et al., ۲۰۲۲).

چالش دوم، مسئله تمامیت (Integrity) و عدم تغییرپذیری داده‌ها است. داده دیجیتال برخلاف ادله فیزیکی که تغییر آن به‌طور معمول قابل مشاهده است، می‌تواند بدون باقی‌گذاشتن آثار آشکار دست‌کاری شود. حذف یا افزودن بخشی از یک فایل، تغییر ابرداده‌ها (Metadata)، اصلاح زمان‌بندی‌ها، بازنویسی لاگ‌ها، جعل تصاویر و ویدئوها توسط ابزارهای هوش مصنوعی یا ایجاد داده‌های ساختگی (Synthetic Data) نمونه‌هایی از این خطرات هستند. ظهور فناوری‌های دیپ‌فیک نیز به این چالش ابعاد جدیدی بخشیده است، زیرا اکنون امکان تولید تصاویر و ویدئوهایی وجود دارد که از لحاظ بصری با واقعیت تفاوتی ندارند و این موضوع مفهوم سنتی «ادله بصری» را به چالش می‌کشد. بنابراین دادگاه‌ها برای اطمینان از تمامیت داده دیجیتال، نیازمند استانداردهای سخت‌گیرانه مانند زنجیره حفاظتی دیجیتال (Digital Chain of Custody)، استفاده از هش‌کدها، ثبت دقیق فرآیندهای جمع‌آوری، و تضمین امنیت ابزارهای ذخیره‌سازی هستند؛ اموری که در بسیاری از پرونده‌ها رعایت نمی‌شوند و زمینه اعتراض‌های جدی حقوقی را فراهم می‌کنند.

چالش سوم، مسئله مشروعیت روش‌های جمع‌آوری داده است. ادله دیجیتال در بسیاری از مواقع بدون رضایت فرد، بدون مجوز قضایی کافی یا از طریق سامانه‌های نظارت گسترده به‌دست می‌آیند. پرسش اساسی این است که آیا بهره‌گیری از داده‌های حاصل از پایش‌های مستمر، ردیابی‌های الگوریتمی، شنودهای شبکه‌ای یا تحلیل داده‌های عمومی شبکه‌های اجتماعی، منطبق با اصول «قانونی بودن»، «ضرورت»، «تناسب» و «احترام به کرامت انسانی» است؟ در برخی نظام‌های حقوقی، جمع‌آوری داده بدون حکم قضایی حتی از محیط‌های عمومی نیز ممنوع تلقی می‌شود؛ زیرا فناوری‌های نوین قابلیت استخراج اطلاعات بسیار فراتر از آنچه در ظاهر دیده می‌شود، دارند. از این رو، داده عمومی در ذات خود خصوصی تلقی نمی‌شد، اما در فرآیند تحلیل الگوریتمی تبدیل به داده خصوصی می‌شود و این تحول، وضعیت مشروعیت آن را پیچیده می‌سازد. در چارچوب نظام حقوقی ایران نیز مقررات جامع و مانع برای جمع‌آوری ادله دیجیتال، به‌ویژه در حوزه کلان‌داده‌ها و هوش مصنوعی، هنوز به‌طور کامل توسعه نیافته است و همین خلأ می‌تواند مشروعیت ادله دیجیتال را در محاکم با تردید مواجه سازد.

مسئله دیگر، ابهام در قابلیت فهم‌پذیری و ارزیابی قضایی ادله دیجیتال است. برخی از ادله دیجیتال مبتنی بر الگوریتم‌هایی هستند که برای قضات، وکلا و حتی کارشناسان غیر قابل فهم یا پیچیده‌اند. فناوری‌هایی همچون یادگیری عمیق (Deep Learning) قادرند الگوها را تشخیص دهند بدون اینکه سازوکار تصمیم‌گیری آن‌ها قابل توضیح باشد. این وضعیت که به «جعبه سیاه الگوریتمی» مشهور است، چالشی جدی برای حق دفاع متهم ایجاد می‌کند. اگر متهم نداند الگوریتم بر چه اساسی او را در دسته پرریسک، مظنون یا مرتبط با جرم قرار داده است، امکان اعتراض مؤثر، بررسی انتقادی و نقد کارشناسانه از او سلب می‌شود. به همین دلیل، بحث «توضیح‌پذیری الگوریتم» به یکی از اصول کلیدی در مشروعیت ادله دیجیتال تبدیل شده است؛ اصلی که در بسیاری از سیستم‌های فعلی محقق نشده و همین امر موجب ابهام در حجیت قضایی چنین ادله‌ای می‌شود. از سوی دیگر، ادله دیجیتال گاه به‌صورت انبوه، متنوع و چندمنبعی ارائه می‌شوند که خود باعث چالش در قضاوت می‌شود. داده‌های شبکه‌های اجتماعی، پیام‌رسان‌ها، تصاویر دوربین‌ها، داده‌های مکانی، سوابق جست‌وجو، تراکنش‌های مالی و ارتباطات رمزنگاری‌شده، همگی ممکن است در یک پرونده مورد استفاده قرار گیرند. این تنوع، ارزیابی قاضی را دشوار می‌کند؛ زیرا هر نوع داده دارای ماهیت، سطح خطا، امکان دست‌کاری و استاندارد تحلیل ویژه‌ای است. در نبود دستورالعمل‌های دقیق برای ارزیابی، ترکیب یا وزن‌دهی به این انواع داده، امکان صدور آرای ناهماهنگ یا غیرمنطقی افزایش می‌یابد.

نهایتاً یکی از مهم‌ترین چالش‌ها، فقدان استانداردهای بومی و هماهنگ در نظام حقوقی ایران است. هرچند قانون جرایم رایانه‌ای و آیین‌نامه‌های مربوط به ادله الکترونیک برخی اصول کلی را تعیین کرده‌اند، اما نظام جامع و منسجمی برای نظارت قضایی، معیارهای پذیرش، شیوه‌های جمع‌آوری، مستندسازی، حفظ و تحلیل داده‌های دیجیتال در مقیاس کلان وجود ندارد. این خلأ موجب می‌شود محاکم در برخورد با ادله دیجیتال با رویه‌های متفاوت، تفاسیر متنوع و گاه متعارض مواجه شوند و همین امر، اصل قابلیت پیش‌بینی دادرسی را تضعیف می‌کند. در نتیجه، مشروعیت ادله دیجیتال مستلزم بازتعریف اصول سنتی دادرسی در چارچوب واقعیت‌های نوین دیجیتال است. این مشروعیت تنها زمانی تحقق می‌یابد که ادله دیجیتال تحت رژیمی از شفافیت، قابلیت راستی‌آزمایی، احترام به حقوق دفاعی، نظارت قضایی سخت‌گیرانه و استانداردهای فنی دقیق قرار گیرد. تا زمانی که چنین سازوکاری به‌طور کامل استقرار نیافته باشد، استفاده گسترده از ادله دیجیتال در نظام کیفری می‌تواند چالش‌هایی جدی برای عدالت کیفری، اعتماد عمومی و اصول بنیادین حقوق بشر ایجاد کند.

۶. پیامدهای اخلاقی و حقوق بشری جرم‌یابی مبتنی بر هوش مصنوعی

ورود هوش مصنوعی به فرآیندهای جرم‌یابی، علاوه بر فرصت‌های گسترده برای کشف جرم و افزایش کارآمدی نظام قضایی، مجموعه‌ای از پیامدهای اخلاقی و حقوق بشری را نیز به همراه دارد. یکی از مهم‌ترین ابعاد این پیامدها، تأثیر مستقیم بر کرامت انسانی و حقوق بنیادین شهروندان است (Ekundayo, ۲۰۲٤). فناوری‌های هوشمند قادرند داده‌های فردی و جمعی را بدون آگاهی و رضایت شهروندان جمع‌آوری، تحلیل و حتی پیش‌بینی کنند. چنین وضعیت‌هایی می‌توانند به شکل غیرمستقیم، آزادی‌های فردی را محدود کرده، افراد را بر اساس الگوهای رفتاری آماری مورد پیش‌داوری قرار دهند و رفتارها و تصمیمات آنان را تحت تأثیر قرار دهند. از این منظر، جرم‌یابی مبتنی بر هوش مصنوعی می‌تواند به ایجاد نوعی «عدالت الگوریتمی» منجر شود که اگرچه ظاهراً عینی و بی‌طرفانه به نظر می‌رسد، اما در عمل ممکن است تبعیض‌آمیز، غیرشفاف و فاقد امکان اعتراض واقعی برای شهروندان باشد.

یکی دیگر از چالش‌های اخلاقی، پیش‌داوری و سوگیری الگوریتمی است. الگوریتم‌های یادگیری ماشین بر اساس داده‌های تاریخی آموزش می‌بینند و این داده‌ها ممکن است حاوی سوگیری‌های نژادی، جنسیتی، اقتصادی یا جغرافیایی باشند. در نتیجه، حتی الگوریتم‌هایی که به‌ظاهر بی‌طرف طراحی شده‌اند، ممکن است گروه‌های خاصی را به شکل نامتناسب تحت نظارت یا ارزیابی ریسک قرار دهند. این امر نه تنها عدالت کیفری را تهدید می‌کند، بلکه با اصول حقوق بشر، از جمله اصل برابری و منع تبعیض، در تضاد است. پیامدهای این سوگیری می‌تواند دامنه وسیعی داشته باشد؛ از افزایش نظارت و محدودیت آزادی‌ها گرفته تا محرومیت غیرموجه از خدمات و فرصت‌های اجتماعی و اقتصادی (Iguodala et al., ۲۰۲٥).

چالش دیگر، مسئله شفافیت و توضیح‌پذیری تصمیمات هوش مصنوعی است. بسیاری از مدل‌های پیشرفته هوش مصنوعی، به ویژه مدل‌های یادگیری عمیق، به شکل «جعبه سیاه» عمل می‌کنند؛ یعنی سازوکار داخلی تصمیم‌گیری آنها برای انسان‌ها قابل درک نیست. در نظام قضایی، این امر چالشی جدی ایجاد می‌کند، زیرا متهمان و وکلا باید بتوانند فرآیند تحلیل ادله و استنتاج تصمیمات قضایی یا پلیسی را بررسی کنند. فقدان شفافیت باعث می‌شود حق دفاع، حق اعتراض و امکان بررسی منصفانه پرونده‌ها به شدت محدود شود و اعتماد عمومی به نظام عدالت کاهش یابد. یکی دیگر از ابعاد اخلاقی، تناسب و ضرورت استفاده از فناوری‌های نظارتی است. استفاده گسترده از هوش مصنوعی در جرم‌یابی، به ویژه در پیش‌بینی جرم یا نظارت بر جمعیت، می‌تواند منجر به اعمال محدودیت‌های پیشگیرانه علیه افرادی شود که هنوز جرم مرتکب نشده‌اند. این نوع اقدامات پیشگیرانه، اگر بدون سازوکارهای قانونی، شفاف و قابل بررسی انجام شوند، با اصول سنتی حقوق کیفری مانند «اصل قانونی بودن جرم و مجازات»، «اصل جرمیت شخصی» و «اصل بی‌گناهی تا اثبات جرم» مغایرت دارند و چالشی جدی برای مشروعیت اخلاقی و حقوقی نظام کیفری ایجاد می‌کنند.

پیامد دیگر، خطر انباشت قدرت و اطلاعات در دست نهادهای اجرایی است. فناوری‌های هوشمند، امکان دسترسی به حجم عظیمی از داده‌های شخصی، تحلیل الگوهای رفتاری و پیش‌بینی اقدامات افراد را فراهم می‌کنند. این تمرکز اطلاعاتی، اگر بدون نظارت مستقل و کنترل‌های شفاف صورت گیرد، می‌تواند به سوءاستفاده، محدودیت آزادی‌های فردی و حتی نقض گسترده حقوق بشر منجر شود. بنابراین، لازم است چارچوب‌های نظارتی، شفافیت در تصمیم‌گیری، استانداردهای اخلاقی و راهکارهای پاسخگویی در سطح قانونی و اجرایی ایجاد شود تا استفاده از هوش مصنوعی محدود به اهداف مشروع و با رعایت کرامت انسانی باشد. در آخر، پیامدهای

اخلاقی و حقوق بشری جرم‌یابی مبتنی بر هوش مصنوعی بر لزوم تطبیق اصول سنتی حقوق کیفری با واقعیت‌های فناوری دیجیتال تأکید دارند. ضرورت دارد نظام حقوقی و آیین دادرسی کشور، با تدوین مقررات دقیق، ایجاد سازوکارهای نظارت، تضمین شفافیت، حفاظت از حریم خصوصی، امکان اعتراض مؤثر و تضمین بی‌طرفی الگوریتم‌ها، توازن میان امنیت عمومی و حقوق بنیادین شهروندان را حفظ کند. تنها در چنین چارچوبی است که جرم‌یابی هوشمند می‌تواند با رعایت موازین اخلاقی و حقوق بشری، به یک ابزار کارآمد و مشروع برای ارتقای عدالت کیفری تبدیل شود، بدون آنکه حقوق و آزادی‌های اساسی شهروندان قربانی پیشرفت فناوری گردد.

۷. راهکارهای قانونی و تنظیم‌گری برای جرم‌یابی مبتنی بر هوش مصنوعی

با توجه به چالش‌های گسترده‌ای که هوش مصنوعی و داده‌های کلان در فرآیند جرم‌یابی ایجاد کرده‌اند، نظام‌های حقوقی نیازمند تدوین چارچوب‌های قانونی و سیاست‌های تنظیم‌گری جامع هستند که بتوانند توازن میان امنیت عمومی و حقوق بنیادین شهروندان را حفظ کنند. این چارچوب‌ها باید هم به جنبه‌های فنی و عملیاتی فناوری توجه داشته باشند و هم اصول حقوقی کلاسیک مانند قانونیت جرم و مجازات، حق دفاع متهم، اصل بی‌گناهی، مشروعیت ادله و حریم خصوصی را تضمین کنند. تدوین چنین سازوکاری مستلزم بررسی دقیق چند حوزه کلیدی است: جمع‌آوری داده، تحلیل و استفاده از آن، نظارت قضایی و پاسخگویی در صورت بروز خطا یا سوءاستفاده.

۱. نخستین حوزه، محدودیت هدفمند جمع‌آوری داده‌ها است. قوانین باید مشخص کنند که داده‌ها صرفاً برای اهداف جنایی و امنیتی قابل جمع‌آوری هستند و نباید برای مقاصد دیگر مانند تبلیغات، پروفایل‌سازی اجتماعی یا پیش‌بینی رفتار شهروندان به‌کار گرفته شوند. همچنین، جمع‌آوری داده باید حداقل و متناسب با ضرورت باشد؛ یعنی تنها داده‌های ضروری برای کشف جرم و با رعایت اصل کمترین مداخله جمع‌آوری شوند. به این ترتیب، از ایجاد نظارت فراگیر و نقض بی‌ضابطه حریم خصوصی جلوگیری می‌شود. علاوه بر این، مشخص شدن مسئولیت جمع‌آوری، صحت‌سنجی و نگهداری داده‌ها برای هر نهاد یا شخص حقیقی و حقوقی، به ایجاد زنجیره پاسخگویی شفاف کمک می‌کند.

۲. دومین حوزه، استانداردهای پذیرش و ارزیابی ادله دیجیتال است. برای تضمین مشروعیت ادله، قوانین باید چارچوب مشخصی برای اعتبارسنجی، حفظ تمامیت و قابلیت انتساب داده‌ها تعیین کنند. این شامل استفاده از تکنیک‌هایی مانند هش‌کدها، امضای دیجیتال، زنجیره حفاظت دیجیتال، ثبت لاگ‌های دقیق و مستندسازی فرآیند جمع‌آوری و پردازش است. همچنین، استانداردهای حقوقی باید مشخص کنند که چه نوع داده‌هایی به عنوان ادله قابل قبول هستند، چگونه می‌توان اصالت و صحت آن‌ها را تأیید کرد، و چه پروتکل‌هایی برای جلوگیری از دستکاری، جعل یا سوءاستفاده وجود دارد. چنین مقرراتی، اطمینان می‌دهد که فناوری‌های هوشمند نه تنها کارآمد بلکه قابل اعتماد و مشروع باشند.

۳. سومین حوزه، شفافیت و توضیح‌پذیری الگوریتم‌ها است. قوانین و دستورالعمل‌های تنظیم‌گری باید الزام کنند که الگوریتم‌های مورد استفاده در جرم‌یابی، به ویژه سیستم‌های پیش‌بینی جرم و تحلیل داده‌های پیچیده، قابل توضیح و بررسی برای مقامات قضایی، کارشناسان مستقل و وکلای مدافع باشند. این اقدام امکان نظارت قضایی موثر، حق دفاع متهم و کنترل خطاهای الگوریتمی را فراهم می‌کند. در این راستا، ایجاد دفاتر مستقل بررسی الگوریتم‌ها، مستندسازی فرآیندهای تصمیم‌گیری و الزام

به گزارش شفاف از معیارهای ارزیابی ریسک و تحلیل داده‌ها می‌تواند اعتماد عمومی به کاربرد هوش مصنوعی در عدالت کیفری را افزایش دهد.

٤. چهارمین حوزه، نظارت و پاسخگویی مستقل است. قوانین باید مرزهای نظارت، مسئولیت‌ها و مکانیسم‌های پاسخگویی در صورت نقض حقوق شهروندان یا خطای سیستم را مشخص کنند. این شامل ایجاد مراجع مستقل نظارت بر کاربرد هوش مصنوعی، کمیته‌های اخلاق فناوری و کمیسیون‌های بررسی شکایات شهروندان است. این سازوکارها می‌توانند تضمین کنند که استفاده از داده‌های کلان و هوش مصنوعی با رعایت حقوق بشر، اصول دادرسی عادلانه و استانداردهای اخلاقی انجام شود و در صورت بروز سوءاستفاده یا خطای سیستم، اقدامات اصلاحی سریع و مؤثر اتخاذ گردد.

٥. پنجمین حوزه، همسویی با استانداردهای بین‌المللی است. تنظیم‌گری داخلی باید با اصول پذیرفته‌شده بین‌المللی در زمینه حقوق دیجیتال، حریم خصوصی، حفاظت داده و عدالت کیفری تطابق داشته باشد. به‌کارگیری دستورالعمل‌هایی مانند GDPR اتحادیه اروپا، اصول OCED در داده‌های شخصی و توصیه‌های شورای اروپا در زمینه هوش مصنوعی و عدالت کیفری می‌تواند چارچوبی قوی برای حفاظت از حقوق شهروندان فراهم آورد. هم‌زمان، توسعه مقررات بومی و منعطف که متناسب با شرایط اجتماعی، فرهنگی و قانونی ایران باشد، الزامی است تا قوانین نه صرفاً تقلید از مقررات خارجی، بلکه پاسخگوی نیازهای داخلی و شرایط اجرایی کشور باشند.

بنابرین، ترکیب این حوزه‌ها می‌تواند به ایجاد یک چارچوب قانونی جامع، اخلاقی و عملیاتی برای جرم‌یابی مبتنی بر هوش مصنوعی منجر شود. چنین چارچوبی هم امنیت عمومی و توان کشف جرم را تقویت می‌کند و هم حریم خصوصی، کرامت انسانی و مشروعیت ادله دیجیتال را تضمین می‌کند. علاوه بر این، تنظیم‌گری موفق باید پویا و سازگار با پیشرفت فناوری باشد؛ زیرا تحولات هوش مصنوعی و کلان‌داده‌ها بسیار سریع هستند و هرگونه قانون‌گذاری ایستا، به سرعت ناکارآمد می‌شود. بدین ترتیب، راهکارهای قانونی و تنظیم‌گری نه تنها ضرورت حقوقی بلکه شرط اساسی تحقق عدالت هوشمند، اخلاقی و قابل اعتماد در عصر دیجیتال محسوب می‌شوند.

جدول ۳: راهکارهای قانونی و تنظیم‌گری برای جرم‌یابی مبتنی بر هوش مصنوعی

حوزه راهکار	اقدام پیشنهادی	هدف
جمع‌آوری داده‌ها	حداقل‌گرایی در جمع‌آوری، محدودیت استفاده ثانویه	حفاظت از حریم خصوصی و رعایت اصل ضرورت
استانداردهای ادله دیجیتال	حفظ تمامیت، قابلیت انتساب، زنجیره حفاظتی دیجیتال	تضمین مشروعیت و اعتماد به ادله دیجیتال
شفافیت الگوریتمی	توضیح‌پذیری تصمیمات، مستندسازی فرآیندها	امکان نظارت قضایی و حق دفاع مؤثر
نظارت و پاسخگویی مستقل	مراجع نظارتی مستقل و کمیته‌های اخلاق	پیشگیری از سوءاستفاده و تبعیض الگوریتمی

همسویی با استانداردهای بین‌المللی	تطبیق مقررات با GDPR و توصیه‌های شورای اروپا	ایجاد چارچوب حقوقی مطمئن و هماهنگ جهانی

۸. نتیجه‌گیری و پیشنهادات

تحول جرم‌یابی در عصر داده‌های کلان و هوش مصنوعی، نشان‌دهنده چرخشی بنیادین در شیوه کشف جرم و اجرای عدالت کیفری است. فناوری‌های نوین، از جمع‌آوری و تحلیل کلان‌داده‌ها گرفته تا سامانه‌های یادگیری ماشین و هوش مصنوعی پیش‌بینی‌کننده، توانسته‌اند امکان دسترسی به اطلاعات دقیق، گسترده و زمان واقعی را فراهم کنند و مسیر کشف جرم را از حالت واکنشی به حالتی تحلیل‌محور و پیش‌نگرانه تغییر دهند. با این حال، این تحول همراه با مجموعه‌ای از چالش‌های حقوقی، اخلاقی و اجتماعی است که اگر به‌درستی مدیریت نشوند، می‌توانند باعث تضعیف حقوق بنیادین شهروندان، مشروعیت ادله و اعتماد عمومی به نظام قضایی شوند. از مهم‌ترین یافته‌ها می‌توان به چالش‌های حریم خصوصی، سوگیری الگوریتمی، فقدان شفافیت و توضیح‌پذیری، و مشکلات مشروعیت ادله دیجیتال اشاره کرد. فناوری‌های جرم‌یابی هوشمند، با توانایی استخراج اطلاعات دقیق از داده‌های ظاهراً عمومی، زمینه نظارت بی‌وقفه و پیش‌داوری آماری علیه افراد و گروه‌ها را فراهم می‌کنند. این وضعیت می‌تواند به محدودیت آزادی‌های فردی، افزایش بی‌عدالتی ساختاری و ایجاد تبعیض‌های پنهان منجر شود. افزون بر این، داده‌های دیجیتال مستعد دستکاری، جعل و تولید مصنوعی هستند و در صورت عدم رعایت زنجیره حفاظتی و استانداردهای فنی، مشروعیت ادله دیجیتال را به خطر می‌اندازند.

نتیجه‌گیری دوم، ضرورت تطبیق چارچوب‌های حقوقی و آیین‌دادرسی با واقعیت‌های فناوری دیجیتال است. قوانین سنتی که بر حریم خصوصی محدود، ادله ملموس و فرآیندهای دستی مبتنی هستند، قادر به پاسخگویی به پیچیدگی‌های هوش مصنوعی و کلان‌داده‌ها نیستند. از این رو، تدوین سیاست‌ها و مقررات بومی، استانداردهای فنی و حقوقی، و مکانیسم‌های نظارتی مستقل اهمیت فراوان دارد. این چارچوب‌ها باید به‌گونه‌ای طراحی شوند که ضمن حفظ اصل قانونی بودن جرم و مجازات، حق دفاع متهم، اصل بی‌گناهی و احترام به کرامت انسانی، امکان بهره‌برداری مؤثر و قانونی از فناوری‌های جرم‌یابی هوشمند فراهم گردد.

در همین راستا، چند پیشنهاد کلیدی برای آینده جرم‌یابی هوشمند قابل طرح است: نخست، ایجاد چارچوب جامع حفاظت از داده و حریم خصوصی که شامل الزامات حداقل جمع‌آوری داده، محدودیت استفاده ثانویه، و تضمین امنیت و تمامیت داده‌ها باشد. دوم، توسعه استانداردهای ارزیابی ادله دیجیتال و قابلیت انتساب که شامل روش‌های فنی تایید اصالت، زنجیره حفاظت دیجیتال و مستندسازی دقیق فرآیند جمع‌آوری است. سوم، شفافیت الگوریتمی و توضیح‌پذیری تصمیمات هوش مصنوعی تا متهمان، وکلا و قضات امکان بررسی و نقد فرآیندهای تصمیم‌گیری را داشته باشند و حق دفاع به طور مؤثر رعایت شود. چهارم، نظارت مستقل و پاسخگویی قضایی و سازمانی که تضمین کند سوءاستفاده، خطا یا تبعیض الگوریتمی قابل شناسایی و اصلاح باشد. و نهایتاً، تطبیق با استانداردهای بین‌المللی حقوق بشر و حفاظت داده در کنار توسعه مقررات بومی منعطف، که امکان همگرایی با تحولات جهانی و پاسخگویی به شرایط داخلی کشور را فراهم کند.

در پایان، آینده جرم‌یابی هوشمند نه صرفاً مسأله فناوری، بلکه مسأله حقوقی، اخلاقی و اجتماعی است. استفاده موفق و مشروع از هوش مصنوعی و داده‌های کلان در تحقیقات جنایی مستلزم تعامل میان فناوری، قانون، اخلاق و جامعه‌شناسی حقوقی است. تنها با ایجاد سازوکارهای قانونی، فنی و نظارتی منسجم، امکان تحقق عدالت هوشمند، کارآمد و قابل اعتماد فراهم می‌شود و فناوری می‌تواند به ابزاری برای تقویت عدالت، پیشگیری مؤثر از جرم و افزایش اعتماد عمومی بدل شود، بدون آنکه کرامت انسانی یا حقوق بنیادین شهروندان قربانی پیشرفت فناوری گردد.

منابع

- حیدرپور حمیدرضا, شهانقی محمد, مهرآرا ژیلا. (۱۴۰۲). کاربرد هوش مصنوعی در جرم یابی و تحقیقات جنایی؛ نمونه پژوهی: قتل های سریالی.
- شریف زاده, میرکوشش, امیرهوشنگ, حسینی. (۱۴۰۳). بررسی آثار سیاست‌های توسعهٔ فناوری‌های نوین و هوش مصنوعی در گسترش راهبردهای سیاسی کلان با رویکرد سیاست‌های کلی نظام. سیاست‌های راهبردی و کلان, ۱۲(۴۵), ۲۴-۴۷.
- لطیف زاده. (۱۴۰۳). تحلیل حقوقی فریب الگوریتمی در عصر هوش‌مصنوعی: چالش‌ها و راهکارها. سیاست علم و فناوری, ۱۷(۴), ۷۱-۸۸.
- محمد نعمتی, غلامرضا گلچین راد, محدثه صادقیان لمراسکی. (۱۴۰۴). جرائم اقتصادی هوش مصنوعی: تهدیدها و راهکارها. پژوهش‌های تطبیقی فقه، حقوق و سیاست, ۳۰۲-۳۲۵.
- محمدی‌نیا, امید, علی‌نژاد, آذر. (۱۴۰۲). نقش و تأثیر هوش مصنوعی در روند کشف جرم. کارآگاه, ۶۳(۱۷), ۸۵-۱۰۴.
- موسوی فرد, سیدمحمّدرضا, ابوالخیریان, محمد امین, عمیدی مهر, مراد پور. (۱۴۰۴). ضرورت های سیاست گذاری حقوقی در آستانه تحولات شگرف انقلاب چهارم صنعتی و هوش مصنوعی با تاکید بر چالش ها و اولویت ها. مطالعات فضای مجازی و رسانه‌های اجتماعی.
- موسوی, سیدمحسن, امیری عقدایی, سید فتح الله. (۱۴۰۰). تحقیقات بازاریابی در انقلاب صنعتی چهارم، استفاده از تحلیل کلان‌داده‌ها و «یادگیری ماشین» جهت ارائه ارزش به مشتری. تحقیقات بازاریابی نوین, ۱۰(۴), ۳۷-۵۴.
- نجفی, موسوی‌فر. (۱۴۰۴). تأملی در روند هوش مصنوعی در پیشگیری از جرم. فصلنامه تمدن حقوقی, ۸(۲۳).
- Ahmed Alaa El-Din, E. (۲۰۲۲). Artificial intelligence in forensic science: Invasion or revolution?. Egyptian Society of Clinical Toxicology Journal, ۱۰(۲), ۲۰-۳۲.
- AL-Marghilani, A. A. (۲۰۲۲). Target Detection Algorithm in Crime Recognition Using Artificial Intelligence. Computers, Materials Continua, ۷۱.(۱)
- Apene, O. Z., Blamah, N. V., Aimufua, G. I. O. (۲۰۲٤). Advancements in crime prevention and detection: From traditional approaches to artificial intelligence solutions. European Journal of Applied Science, Engineering and Technology, ۲(۲), ۲۸۵-۲۹۷.
- Dai, D., Boroomand, S. (۲۰۲۲). A review of artificial intelligence to enhance the security of big data systems: state-of-art, methodologies, applications, and challenges. Archives of Computational Methods in Engineering, ۲۹(۲), ۱۲۹۱-۱۳۰۹.
- Ekundayo, F. (۲۰۲٤). Big data and machine learning in digital forensics: Predictive technology for proactive crime prevention,'. Complexity, ۲٤(۲), ۲٦۹۲-۲۷۰۹.
- Iguodala, O., Oyiborhoro, A. (۲۰۲٥). AI-Powered Anti-Money Laundering (AML) and fraud detection-enhancing financial security through intelligent fraud detection. World Journal of Advanced Research and Reviews, ۲٦, ۳۷۰۲-۳۷۱٤.
- Oatley, G. C. (۲۰۲۲). Themes in data mining, big data, and crime analytics. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, ۱۲(۲), e۱٤۳۲.
- Ţical, G. M. (۲۰۲٤). Artificial intelligence technologies: a new era for crime prevention. Annals–Series on Military Sciences, ۱٦(۲), ۱۱٥-۱۲۸.
- Ushakov, R. M., Efremov, D. A., Gariga, O. A., Finogenov, N. A., Khametov, R. B. (۲۰۲۱). Information technology of Big Data in crime detection, investigation, and prevention. Theoretical and applied analysis of individual prospects and application problems. Turkish Journal of Computer and Mathematics Education, ۱۲(٦), ۱٦٤٥-۱٦٥۷.

- Wankhade, T. D., Ingale, S. W., Mohite, P. M., Bankar, N. J., Wankhade, T., Ingale, S., MOHITE, P. (۲۰۲۲). Artificial intelligence in forensic medicine and toxicology: the future of forensic medicine.