

فصلنامه پژوهش های حقوقی قانون یار

License Number: 80025 Article Cod: W54772715 ISSN-E: 6452-2588

فناوری های نوین نظارت کیفری (کلان داده، هوش مصنوعی، تشخیص چهره)

و چالش های آن در حوزه حقوق بشر و حریم خصوصی

(تاریخ دریافت ۱۴۰۵/۰۲/۱۱ تاریخ تصویب ۱۴۰۵/۰۳/۲۸)

میلاد حسین تبار

دانشجوی کارشناسی ارشد حقوق جزا و جرم شناسی دانشگاه پیام نور

چکیده

تحولات فناوری در سال های اخیر قلمرو نظارت کیفری را دگرگون کرده و شیوه های سنتی کنترل اجتماعی را با مدل های جدیدی جایگزین نموده است که بر پایه داده، تحلیل های محاسباتی و ابزارهای هوشمند عمل می کنند. این تحولات باعث شده است که پلیس و دستگاه قضایی اکنون به ابزارهایی دسترسی داشته باشند که نه تنها رفتار افراد را ثبت می کنند، بلکه می توانند رفتارهای احتمالی آینده را نیز پیش بینی کنند. این موضوع، هم ظرفیت هایی بزرگ برای مبارزه با جرم ایجاد کرده و هم نگرانی هایی مهم درباره حقوق بشر، آزادی های فردی و حریم خصوصی به همراه آورده است. بررسی دقیق این فناوری ها نشان می دهد که مزایای آنها به همان اندازه که چشم گیر است، خطرات پنهان و عمیق نیز دارد؛ بنابراین نیازمند تحلیل دقیق و چندبعدی است.

واژگان کلیدی: فناوری های نوین، حقوق بشر، هوش مصنوعی، حقوق کیفری



بخش اول: کلان داده؛ وقتی اطلاعات روزمره به ابزار پیش بینی رفتار تبدیل می شود

کلان داده یعنی مجموعه ای عظیم از اطلاعات که از هزاران منبع مختلف جمع آوری می شود؛ منابعی که بسیاری از مردم حتی به آنها توجه نمی کنند. وقتی فردی با تلفن همراه خود مسیرش را بررسی می کند، وقتی خرید اینترنتی انجام می دهد، زمانی که پست شبکه اجتماعی می گذارد یا از کارت بانکی برای پرداخت استفاده می کند، هر بار داده هایی تولید می شود که می تواند در سیستم های تحلیل رفتار ثبت شود. دوربین های شهری، سنسورهای ترافیکی، سامانه های حمل و نقل هوشمند، تراکنش های دیجیتال، آهنگ موقعیت یابی GPS، فعالیت های آنلاین و حتی دستگاه های هوشمند خانه (که روشن و خاموش شدن وسایل را ثبت می کنند) همه به منابع بزرگ داده تبدیل شده اند.

در حوزه نظارت کیفی، این داده ها برای اهداف مختلف به کار می روند؛ از پیش بینی نقاط جرم خیز گرفته تا تحلیل ارتباطات افراد، تشخیص تجمع های غیرمعمول و حتی بررسی الگوهای رفتاری که ممکن است نشانه خطر تلقی شوند. پلیس می تواند با تحلیل داده هایی که از گذشته به دست آمده، الگوهایی از «رفتارهای پرخطر» استخراج کند و بر اساس آن تصمیم بگیرد که چه مناطقی نیازمند گشت بیشتر هستند یا چه گروه هایی رفتارهایی مشابه گروه های مجرم قبلی دارند.

مزیت این فناوری سرعت و دقت آن است. مثلاً با بررسی داده های ترافیکی، دوربین های شهری و تراکنش ها می توان مسیرهای احتمالی یک مجرم فراری را در زمان بسیار کوتاهی مشخص کرد. یا با تحلیل رفتار گذشته می توان تشخیص داد کدام منطقه ممکن است در آینده شاهد افزایش یک نوع جرم خاص باشد.



اما مشکل اصلی اینجاست که بسیاری از مردم نمی‌دانند چنین حجم عظیمی از داده‌های روزمره آنها ذخیره می‌شود. حتی نمی‌دانند که چگونه می‌توانند از داده‌هایشان محافظت کنند یا چه نهادی حق دسترسی به آنها را دارد. از منظر حقوق بشر، این وضعیت خطرناک است، زیرا جمع‌آوری داده بدون رضایت و بدون محدودیت زمانی، می‌تواند باعث ایجاد «احساس نظارت دائمی» شود. این احساس به مرور موجب تغییر رفتار اجتماعی و کاهش آزادی فردی می‌شود، زیرا فرد تصور می‌کند هر رفتاری even-رفتار غیرمجرمانه—ممکن است ثبت و تحلیل شود.

نکته مهم‌تر این است که کلان‌داده همیشه دقیق نیست. ممکن است داده‌ها ناقص، گمراه‌کننده یا خارج از زمینه باشند. برای مثال، فردی که به‌طور اتفاقی چندبار در یک منطقه با میزان جرم بالا حضور داشته، بدون اینکه خطایی از او سر زده باشد، ممکن است به عنوان «الگوی رفتاری مشکوک» ثبت شود. همین ممکن است در آینده برای او ایجاد محدودیت کند. همچنین داده‌هایی که برای اهداف امنیتی جمع‌آوری شده‌اند، ممکن است در آینده برای اهداف سیاسی، اقتصادی یا اجتماعی به کار گرفته شوند؛ موضوعی که حقوق بشر آن را بسیار خطرناک می‌داند.

بخش دوم: هوش مصنوعی؛ وقتی ماشین‌ها جای انسان تصمیم می‌گیرند

هوش مصنوعی یکی از پیچیده‌ترین ابزارهای نظارت کیفری است، زیرا برخلاف کلان‌داده که صرفاً اطلاعات را ذخیره می‌کند، AI می‌تواند تصمیم‌گیری کند، تحلیل انجام دهد و رفتار آینده را پیش‌بینی کند. امروزه سیستم‌های هوشمند به‌طور گسترده در پیش‌بینی جرم استفاده می‌شوند. پلیس از الگوریتم‌های پیچیده استفاده می‌کند که «نقشه‌های خطر» می‌سازند؛ نقشه‌هایی که نشان می‌دهند کدام محله‌ها در چه روزهایی احتمال وقوع جرم بیشتری دارند.



در دستگاه قضایی نیز برخی کشورها از سیستم های الگوریتمی برای تعیین وثیقه، پیش بینی احتمال تکرار جرم و حتی کمک به قاضی در صدور حکم استفاده می کنند. این سیستم ها به ظاهر بی طرف و منطقی اند، چون بر اساس تحلیل داده های گذشته عمل می کنند. اما واقعیت این است که الگوریتم ها تنها الگوها را تقلید می کنند؛ اگر داده های گذشته آغشته به تبعیض بوده باشد، AI همان تبعیض را «هوشمندانه تر» تکرار خواهد کرد.

مثلاً اگر آمار نشان دهد که پلیس در گذشته بیشتر در محله های فقیرنشین افراد را متوقف کرده، داده های مربوط به «جرم» در آن محله ها بیشتر ثبت شده است. هوش مصنوعی این داده ها را می بیند و نتیجه می گیرد که «این محله جرم خیز است». بنابراین به پلیس پیشنهاد می کند در همان مناطق تمرکز بیشتری داشته باشد. این باعث می شود آمار بیشتر شود و چرخه تبعیض ادامه پیدا کند، بدون اینکه کسی توجه کند که این جرم خیزی واقعی نیست، بلکه نتیجه تمرکز تاریخی پلیس بر آن منطقه است.

یکی دیگر از مشکلات، نبود شفافیت است. بسیاری از الگوریتم ها مانند یک جعبه سیاه عمل می کنند. یعنی فقط نتیجه را می دهند اما نحوه رسیدن به آن نتیجه روشن نیست. اگر سیستم یک فرد را «پرخطر» تشخیص دهد، فرد نمی تواند بفهمد که چرا این برچسب به او زده شده. این مسئله با اصول دادرسی عادلانه، حق اعتراض و حق توضیح خواهی در تضاد است.

از طرف دیگر، مشخص نیست اگر AI اشتباه کند، چه کسی باید پاسخگو باشد:

- آیا شرکت سازنده؟
- پلیس؟
- قاضی؟



- برنامه‌نویس؟

- یا خود سیستم که هویت حقوقی ندارد؟

این ابهام می‌تواند باعث شود حقوق مردم نادیده گرفته شود و هیچ کس مسئولیت نپذیرد.

بخش سوم: تشخیص چهره؛ دقیق، سریع، و در عین حال خطرناک

تشخیص چهره یکی از بحث‌برانگیزترین فناوری‌های نظارتی است، زیرا مستقیماً با هویت افراد سروکار دارد. این سیستم قادر است چهره افراد را در میان جمعیت شناسایی کند، حتی اگر در حال حرکت باشند، صورت سایه داشته باشد یا حتی قسمتی از چهره پوشیده باشد. این قدرت در صورت استفاده صحیح می‌تواند برای امنیت مفید باشد؛ مثلاً در پیدا کردن افراد گمشده یا شناسایی مظنونان فراری.

اما مشکل اینجاست که تشخیص چهره دقیق نیست. تحقیقات نشان می‌دهد که برای برخی گروه‌ها، مثل زنان، سالمندان و افراد با رنگ پوست تیره، نرخ خطای سیستم بیشتر است. این اشتباهات می‌تواند باعث «بازداشت اشتباه»، «اتهام نادرست» یا «قرار گرفتن نام فرد در فهرست مظنونان» شود که آسیب‌های روحی و اجتماعی فراوان دارد.

اما مهم‌تر از همه، استفاده گسترده از تشخیص چهره در فضاهای عمومی می‌تواند جامعه را به «جامعه تحت نظارت دائمی» تبدیل کند؛ جامعه‌ای که در آن مردم همیشه فکر می‌کنند دیده می‌شوند. این احساس باعث خودسانسوری، کاهش آزادی بیان و ترس از شرکت در تجمعات قانونی می‌شود. به عبارت ساده: اگر مردم بدانند هر حرکتشان ثبت می‌شود، دیگر آزادانه رفتار نخواهند کرد.



ترکیب تشخیص چهره با کلان داده و هوش مصنوعی قدرتی به دولت ها می دهد که در تاریخ بی سابقه است؛ قدرت ردیابی لحظه به لحظه افراد، تحلیل روابط اجتماعی، پیش بینی رفتار آینده و حتی شناسایی گرایش های فکری از طریق تحلیل حضور در تجمعات. چنین قدرتی اگر بدون کنترل باشد، می تواند آزادی های فردی را به شدت تهدید کند.

نتیجه گیری

پیشرفت شتابان فناوری های نوین نظارت کیفری، به ویژه کلان داده، هوش مصنوعی و سامانه های تشخیص چهره، موجب تحول اساسی در سیاست جنایی معاصر شده است. این فناوری ها با افزایش سرعت کشف جرم، ارتقای دقت تحلیل اطلاعات، پیش بینی الگوهای مجرمانه، تخصیص بهینه منابع انتظامی و تسهیل فرآیندهای تحقیق و تعقیب، ظرفیت قابل توجهی برای افزایش کارآمدی نظام عدالت کیفری فراهم کرده اند. با این حال، بهره گیری از این ابزارها صرفاً یک مسئله فنی نیست، بلکه آثار عمیق حقوقی، اخلاقی و اجتماعی به دنبال دارد که نمی توان از آن ها چشم پوشی کرد. مهم ترین چالش این فناوری ها، ایجاد تعارض میان ضرورت تأمین امنیت عمومی و حفظ حقوق بنیادین اشخاص است. گردآوری و تحلیل گسترده داده های شخصی، نظارت مستمر بر رفتار شهروندان، امکان شناسایی افراد در اماکن عمومی از طریق فناوری تشخیص چهره و استفاده از الگوریتم های هوشمند در تصمیم گیری های کیفری، در صورت فقدان ضوابط قانونی کافی، می تواند منجر به نقض حق حریم خصوصی، آزادی های فردی، اصل برائت، حق بر دادرسی عادلانه و حتی کرامت انسانی شود. افزون بر این، احتمال وجود سوگیری های الگوریتمی، خطاهای ناشی از کیفیت داده ها، عدم شفافیت تصمیمات مبتنی بر هوش مصنوعی و دشواری نظارت مؤثر بر عملکرد این سامانه ها، خطر تبعیض و تصمیم گیری های ناعادلانه را افزایش می دهد. از منظر حقوق بشر،



اصل تناسب، ضرورت و قانونی بودن مداخلات دولت باید مبنای استفاده از فناوری‌های نظارتی قرار گیرد. به عبارت دیگر، هیچ فناوری، صرف‌نظر از میزان کارآمدی آن، نباید جایگزین تضمین‌های بنیادین حقوق بشر شود. استفاده از ابزارهای هوشمند تنها زمانی مشروع خواهد بود که بر پایه قوانین شفاف و دقیق، با اهداف مشخص، در محدوده زمانی و مکانی معین، تحت نظارت مراجع مستقل و همراه با امکان اعتراض و جبران خسارت برای افراد متضرر صورت گیرد. همچنین تصمیمات نهایی در فرآیند کیفری باید همچنان با نظارت و مسئولیت انسان اتخاذ شوند و نباید به‌طور کامل به الگوریتم‌های هوشمند واگذار شوند. بررسی اسناد و استانداردهای بین‌المللی نیز نشان می‌دهد که گرایش غالب نظام‌های حقوقی، نه ممنوعیت مطلق فناوری‌های نوین نظارتی و نه پذیرش بی‌قید و شرط آن‌ها، بلکه تنظیم‌گری هوشمند و مبتنی بر حقوق بشر است. تجربه بسیاری از کشورها بیانگر آن است که وضع قوانین جامع حمایت از داده‌های شخصی، الزام به ارزیابی اثرات حقوق بشری پیش از استقرار سامانه‌های هوش مصنوعی، شفافیت الگوریتم‌ها، مسئولیت‌پذیری نهادهای بهره‌بردار و ایجاد نهادهای مستقل نظارتی، از مهم‌ترین راهکارهای کاهش مخاطرات این فناوری‌ها محسوب می‌شود.

در نظام حقوقی ایران نیز هرچند برخی اصول قانون اساسی، قواعد آیین دادرسی کیفری و مقررات مرتبط با حقوق شهروندی تا حدودی از حریم خصوصی حمایت می‌کنند، اما توسعه سریع فناوری‌های مبتنی بر کلان‌داده و هوش مصنوعی، خلأهای تقنینی موجود را بیش از پیش آشکار ساخته است. نبود قانون جامع حفاظت از داده‌های شخصی، فقدان ضوابط اختصاصی برای استفاده از سامانه‌های تشخیص چهره و هوش مصنوعی در فرآیندهای کیفری، ابهام در مسئولیت ناشی از تصمیمات الگوریتمی و کمبود سازوکارهای نظارت مستقل، از جمله



چالش هایی است که نیازمند بازنگری جدی در سیاست تقنینی کشور است. در نهایت، می توان نتیجه گرفت که آینده عدالت کیفری به طور اجتناب ناپذیر با فناوری های هوشمند گره خورده است؛ اما مشروعیت و مقبولیت این تحول، تنها در صورتی تضمین خواهد شد که توسعه فناوری همگام با توسعه قواعد حقوقی، تضمین های حقوق بشری و اصول حکمرانی مطلوب صورت گیرد. دستیابی به تعادل میان کارآمدی نظام عدالت کیفری و صیانت از حقوق و آزادی های اساسی شهروندان، مهم ترین رسالت سیاست جنایی در عصر هوش مصنوعی است. از این رو، تدوین قوانین جامع در حوزه حفاظت از داده های شخصی، ایجاد چارچوب های شفاف برای استفاده از فناوری های نظارتی، تقویت نظارت قضایی و عمومی، الزام به شفافیت و پاسخگویی الگوریتم ها و توسعه همکاری میان متخصصان حقوق، علوم داده و فناوری اطلاعات، از مهم ترین الزامات تحقق عدالت کیفری مبتنی بر فناوری و در عین حال منطبق با موازین حقوق بشر به شمار می رود.



منابع و مآخذ

• کتاب‌ها و منابع دانشگاهی فارسی

۱. انصاری، باقر. «حق بر حریم خصوصی در نظام حقوقی ایران». نشر میزان، ۱۳۹۶.
۲. مهرپور، حسین. «حقوق بشر و آزادی‌های فردی». نشر میزان، ۱۳۹۵.
۳. ضیایی بیگدلی، محمدرضا. «حقوق بین‌الملل عمومی». نشر گنج دانش.
۴. کاظمی، محمدهادی. «جرم‌شناسی پیش‌بینی محور». انتشارات دانشگاه تهران، ۱۴۰۳.
۵. فضلی‌نژاد، میثم. «هوش مصنوعی و حقوق کیفری». انتشارات جنگل، ۱۴۰۳.
۶. عبدالحی، رضا. «مسئولیت مدنی ناشی از تصمیمات الگوریتمی». انتشارات میزان، ۱۴۰۴.
۷. خسروی، علی. «مدیریت داده و امنیت اطلاعات». انتشارات حتمی، ۱۳۹۸.
۸. موسوی خلخالی، ناصر. «فناوری‌های نوین و چالش‌های حقوق بشر». پژوهشگاه فرهنگ و اندیشه، ۱۴۰۰.
۹. کتاب سال حقوق فناوری اطلاعات، مجموعه مقالات، سازمان فناوری اطلاعات ایران، ۱۳۹۹.

• مقالات و گزارش‌های فارسی تخصصی

۱۰. مرکز پژوهش‌های مجلس: «ارزیابی حقوقی و فنی سامانه‌های هوش مصنوعی در نظام عدالت کیفری»، ۱۴۰۰.



۱۱. قوه قضاییه، معاونت حقوقی: «نقش فناوری‌های هوشمند در تصمیم‌گیری قضایی»، ۱۳۹۹.

۱۲. پژوهشگاه قوه قضاییه: «چشم‌انداز استفاده از کلان‌داده در مبارزه با جرم»، ۱۴۰۱.

۱۳. پژوهشگاه ارتباطات و فناوری اطلاعات: «چالش‌های اخلاقی در تشخیص چهره»، ۱۴۰۰.

۱۴. دانشگاه شهید بهشتی، گروه حقوق بشر: «تأثیر نظارت هوشمند بر آزادی تجمعات»، ۱۳۹۸.

۱۵. مقالات فصلنامه «مطالعات حقوق فناوری» (شماره‌های ۱ تا ۱۰)، شامل پژوهش‌های متعدد در زمینه حریم خصوصی، هوش مصنوعی و داده‌محوری.

• کتاب‌های لاتین

- ۴۰. O'Neil, Cathy. "Weapons of Math Destruction. " ۲۰۱۸.
- ۴۱. Crawford, Kate. "Atlas of AI. " ۲۰۲۳.
- ۴۲. Bostrom, Nick. "Superintelligence. " ۲۰۲۴.
- ۴۳. Pasquale, Frank. "The Black Box Society. " ۲۰۲۲.
- ۴۴. Russell, Stuart & Norvig, Peter. "Artificial Intelligence: A Modern Approach. "

• مقالات و پژوهش‌های لاتین

- ۴۵. Barocas, Solon & Selbst. "Big Data's Disparate Impact. " California Law Review, ۲۰۲۰.
- ۴۶. Selbst, Andrew et al. , "Fairness and Abstraction in Socio-Technical Systems", ۲۰۱۹.



-
۴۷. Whittaker, Meredith et al. , “*AI Now Report*”, ۲۰۱۷-۲۰۲۱.
۴۸. Mittelstadt, Brent. “*Principles for Ethical AI*”, ۲۰۲۴.
۴۹. Floridi, Luciano & Cowls, Josh. “*Unified Framework for Ethical AI*. ” ۲۰۲۲.