

## نقش فناوری در کنترل اجتماعی جرم؛ فرصت‌ها و تهدیدها

فناوری‌های نوین نظارتی در عرصه کنترل اجتماعی جرم، همچون شمشیری دولبه عمل می‌کنند که هم‌زمان فرصت‌ها و تهدیدهای گسترده‌ای به همراه می‌آورند. از یک سو، این فناوری‌ها با ارتقای کارایی نظام عدالت کیفری، تسهیل کشف جرائم پیچیده و بهینه‌سازی مصرف منابع محدود، ابزاری ضروری برای مقابله با چالش‌های امنیتی عصر حاضر محسوب می‌شوند. از سوی دیگر، اتکای بی‌قید و شرط به آنها پیامدهای ناخواسته‌ای را رقم می‌زند که مهمترین آنها نقض حریم خصوصی افراد، کاهش برابری اجتماعی و تبدیل ابزارهای نظارتی به اهدافی خودمختار است. این پژوهش بر آن است که به شیوه توصیفی - تحلیلی و با استناد به منابع کتابخانه‌ای ضمن بررسی نقش فناوری در کنترل جرم و تبعات استفاده افراطی از فناوری‌های نظارتی، راهکارهایی برای کاهش این تبعات ارائه نماید. یافته‌های پژوهش حاکی از آن است که فناوری‌های نظارتی، اگرچه در کوتاه مدت امنیت را افزایش می‌دهد، در بلند مدت به فرسایش حریم خصوصی، تبعیض ساختاری و کم‌رنگ شدن اصول اخلاقی منجر می‌شوند. لذا با اتخاذ تدابیری نظیر برقراری تعادل میان امنیت و حریم خصوصی، تدوین قوانین شفاف برای محدودیت جمع‌آوری داده‌ها، افزایش آگاهی کنشگران نظام عدالت کیفری درباره محدودیت‌های فناوری، می‌توان تا حدودی این پیامدها را کاهش داده و کرامت انسانی را محترم شمرد.

### واژگان کلیدی: فناوری، کنترل اجتماعی، حریم خصوصی، نظام عدالت کیفری

#### مقدمه

اولین دوره ظهور فناوری در کنترل اجتماعی جرم، دوران کلاسیک است که از فناوری‌های ساده نظیر قفل‌های مکانیکی، سیستم‌های هشدار و روشنایی معابر به عنوان نخستین اشکال مهندسی محیطی برای کاهش فرصت‌های مجرمانه استفاده شد. (Clarke, 1997, P.143) در دوره بعدی که به دوران مدرن شناخته می‌شود با ظهور دوربین‌های مدار بسته (CCTV) در دهه ۱۹۷۰ و سیستم‌های شناسایی الکترونیکی (RFID) که نظارت غیرحضور را ممکن ساخت، همراه بود. (Grabosky, 1998, P.53) آخرین دوره یعنی دوره کنونی به عصر دیجیتال معروف است که از مشخصه‌های بارز آن می‌توان به: یکپارچه سازی هوش مصنوعی (AI)، پردازش کلان داده‌ها و الگوریتم‌های پیشینی‌کننده جرم (PredPol, COMPAS) برای تبدیل داده‌ها به راهکارهای کنترلی اشاره نمود. (Ferguson, 2017, P. 86)

از نیمه قرن بیستم، استفاده از فناوری برای کنترل رفتارهای اجتماعی و کاهش جرم، گسترش قابل توجهی نمود. کنترل از طریق فناوری در عملکرد جامعه مدرن نقش اساسی دارد. تشدید کنترل در ایالات متحده و تصویب قوانینی نظیر قانون میهن پرستی<sup>۱</sup> و ایجاد وزارت

<sup>1</sup> Patriot Act

امنیت داخلی<sup>۲</sup> منجر به ایجاد هزینه‌های گزاف به منظور تحقیق و توسعه، گسترش بین‌المللی ابزارهایی نظیر تجزیه و تحلیل DNA، تراشه‌های RFID، هواپیماهای بدون سرنشین، سیستم‌های تشخیص چهره، افزایش کنترل‌های از راه دور، افزایش اشتراک‌گذاری اطلاعات و هماهنگی میان آژانس‌های دولتی، خصوصی، محلی و بین‌المللی شده است. (Liu T, Yang B, Geng Y and Du S, 2021, P.318) بسیاری از فناوری‌های پیشرفته که در ابتدا برای کاربردهای نظامی طراحی شده بودند، نظیر اینترنت، ماهواره‌ها و حسگرها، اکنون به عرصه کنترل اجتماعی راه یافتند.

در قرن بیست و یکم تلاش برای مقابله با چالش جرم به طرز قابل توجهی با کمک ابزارهای مبتنی بر فناوری صورت می‌گیرد. ارتقای سیستم‌های قفل و هشدار به دستگاه‌های جدید برای مکان‌یابی، شناسایی و نظارت به منظور کنترل افراد خطرناک، وظایف کنترل جرم را هرچند برای پلیس و جامعه آسانتر کرده است ولی چالش‌هایی نظیر امکان سوءاستفاده یا آسیب به افراد بی‌گناه را هم به همراه آورده است. (Grabosky, 1998, P.19) از سویی سازگاری و خلاقیت منفی بزه‌کاران، مستلزم توسعه مداوم ابزارهایی جهت جلوگیری و یا به حداقل رساندن فعالیت مضر آنها است.

به دلیل گستردگی جوامع امروزی و عدم امکان نظارت و کنترل همه رفتارهای افراد جامعه، دولت‌ها، کنترل اجتماعی را تنظیم می‌کنند. مراد از کنترل اجتماعی، مطالعه چند وجهی هنجارها و قوانین اجرایی است. این امر شامل ایجاد قوانین و هنجارهایی است که رفتار افراد را تنظیم می‌کند. لذا کنترل اجتماعی جرم در این پژوهش به مثابه یک مفهوم چند بعدی تعریف می‌شود که شامل تمام سازوکارهای هنجاری، فناوریانه و نهادی به منظور تنظیم رفتارهای اجتماعی، پیشگیری از جرائم و حفظ نظم عمومی است. این مفهوم نه صرفاً محدود به کنترل قهری (کیفری) است و نه منحصرأ معطوف به پیشگیری اقلیتی؛ بلکه ترکیبی از هر دو رویکرد را در بر می‌گیرد. (نجنفی ابرندآبادی، ۱۴۰۳، چ، هفتم ص. ۶۸) کنترل اجتماعی همچنین به طور متمرکز شامل تلاش‌هایی برای اجرای هنجارها می‌شود. بخش مهمی از تلاش‌های اجرایی معاصر به استفاده از فناوری در کاهش نقض قوانین، افزایش شناسایی مجرمان - نظیر ثبت اطلاعات شخصی در سیستم‌های الکترونیک - و به حداقل رساندن آسیب، اختصاص یافته است. هدف اصلی کنترل اجتماعی، حفظ نظم، انسجام اجتماعی و کاهش تخلفات است. منظور از تنظیم، هر شکل از کنترل است که مطلوب سیستم بوده و اجرای مقررات را آسان می‌نماید. تغییر در مقیاس زندگی، موجب تفاوت در تنظیم کنترل اجتماعی می‌شود. در مجموع همه واحدهای اجتماعی از کوچکترین مقیاس تا کل جامعه

<sup>2</sup> Department Of Homeland Security

تحت نظارت قرار دارند. بدیهی است اشکال مختلف رفتار در مقیاس‌های کوچکتر به راحتی قابل کنترل است، ولی استفاده از آن روش کنترل برای دیگر مقیاس‌ها و تنظیمات اجتماعی، غیرممکن است. (Mohapatra, Seema, 2016, P.94) مشکل اصلی جوامع امروزی علاوه بر مشکلات نظارتی، کم‌رنگ شدن اصول اخلاقی و عدم وفاق ارزشی است. رایج‌ترین راه حل در جوامع با مقیاس بزرگ، استفاده از فناوری در ابزارهای مختلف کنترل اجتماعی است و نیز ثبت و ضبط تمام سوابق و اطلاعات افراد در سیستم‌های الکترونیکی است. در جامعه‌ای که از سیستم‌های کنترل فناوری محور استفاده می‌شود، صرفاً از اخلاق یک استفاده ابزاری شده و اخلاق در صورتی مورد پذیرش قرار می‌گیرد که با عقلانیت جامعه مدرن در تعارض نباشد.

از مهمترین حقوقی که قرابت نزدیکی با کرامت انسانی دارد، حق بر حریم خصوصی است. حریم خصوصی را برخی به معنای حق برخورداری از زندگی در انزوا، حق دوری جستن از شهرت ناخواسته و حق زندگی کردن عاری از مداخله ناموجه مردم در اموری که ارتباط با عموم ندارد، تعریف کرده‌اند. (Garner, 2004, P. 43) هر چند دامنه حریم خصوصی در منابع علمی متفاوت است، اما دو دیدگاه اصلی وجود دارد: ۱- حریم خصوصی به عنوان یک حق بنیادین ۲- حریم خصوصی به عنوان یک کالای قابل مبادله. در گذشته تمرکز اصلی بر تعریف هنجاری «حق بر خلوت» یا حق بر تنها ماندن بود. با افزایش سرعت فناوری در قرن ۲۱ نگرش به حریم خصوصی تغییر کرده و بیشتر به عنوان کالایی در نظر گرفته می‌شود که می‌توان آن را با امنیت یا منافع اقتصادی مبادله کرد. همچون بسیاری از مفاهیم علمی، هیچ تعریف واحد جهانی از حریم خصوصی وجود ندارد. با این وجود، رویکردهای مفیدی برای تبدیل حریم خصوصی به مفهومی مفید و کاربردی وجود دارد. (Thomas G, & Others, 2007, P.112) یکی از این رویکردها درک حریم خصوصی از نظر کنترل است. از جمله مثال‌های معروف، تعریف وستین است که حریم خصوصی را به عنوان حقی که افراد می‌بایست تصمیم بگیرند که کدام اطلاعات را در خصوص خودشان و تحت چه شرایطی در اختیار دیگران قرار دهند، تعریف نموده است. (Westin, 1967, P.33)

هدف اصلی این پژوهش، بررسی پیامدها و آثار اتکای بی قید و شرط به فناوری‌های مدرن در کنترل اجتماعی جرم است و بر این نکته تأکید دارد که افزایش آگاهی کنشگران نظام عدالت کیفری درباره این موضوع ضروری است؛ چراکه صرف استفاده از تجهیزات پیشرفته و روزآمد، بدون در نظر گرفتن تبعات و پیامدهای ناخواسته آن‌ها، به معنای دستیابی به موفقیت در مهار جرم نخواهد بود.

<sup>3</sup> Right to be left alone

این مقاله با اذعان به اینکه تعداد کمی از نوآوری‌های جدید کاملاً بدون مشکل هستند، مترصد پاسخگویی به دو پرسش اساسی است: ۱- استفاده بی‌رویه از فناوری‌های نظارتی در کنترل اجتماعی با چه چالش‌هایی مواجه است؟ ۲- چگونه می‌توان تبعات نامطلوب استفاده از فناوری در کنترل اجتماعی جرم را به حداقل رساند؟ برای پاسخ به این پرسش‌ها، محقق به مطالعات تطبیقی و بررسی رویکرد کشورهای که در استفاده از فناوری در ابعاد مختلف کنترل اجتماعی پیش‌تاز هستند، تمسک جسته است. این تحقیق در زمره پژوهش‌هایی<sup>۴</sup> است که محقق افزون بر تصویرسازی آنچه که هست، به تشریح و تبیین دلایل چگونه بودن و چرایی وضعیت مسئله می‌پردازد. از این رو تحقیق «توصیفی - تحلیلی» به شمار می‌رود.

پژوهش حاضر به لحاظ پرداختن به چالش‌های استفاده افراطی از فناوری در کنترل اجتماعی و توجه به تبعات و پیامدهای سوء آن از جمله نادیده انگاشتن حریم خصوصی افراد با پژوهش‌های انجام شده تمایز آشکار دارد و همین امر بیانگر ضرورت انجام این پژوهش است. این پژوهش در ۳ بخش اصلی سازمان‌دهی شده است: ۱- جایگاه فناوری در کنترل اجتماعی جرم: این بخش به بررسی نقش فناوری در پیشگیری، کشف و مدیریت جرم پرداخته است. ۲- پیامدهای ساختاری، انکای انحصاری به فناوری: این بخش به شناسایی مخاطراتی مانند نقض حریم خصوصی، تبعیض ساختاری و کاهش اصول اخلاقی اختصاص یافته است. ۳- راهکارهای کاهش تبعات استفاده از فناوری‌های نظارتی: در بخش سوم محقق به ارائه راهکارهای عملی برای کاهش تبعات منفی استفاده بی‌رویه از فناوری در کنترل جرم، نظیر تدوین قوانین شفاف و تقویت آگاهی کنشگران قضایی پرداخته است.

## ۱- جایگاه فناوری در کنترل اجتماعی جرم

فناوری به عنوان **بنیان تحول آفرین** در کنترل اجتماعی جرم، از جایگاهی راهبردی در نظام‌های عدالت کیفری معاصر برخوردار است. این بخش با بررسی سیر تکاملی فناوری و کاربست آن در سه حوزه کلیدی پیشگیری، کشف و مهار جرم، جایگاه محوری آن را تبیین می‌کند.

<sup>۴</sup> تاکنون پژوهش مستقلی در ایران به این دو پرسش پاسخ نداده است. اما در خصوص نظارت الکترونیک در فضای مجازی، مسعودی (۱۴۰۰) در مقاله‌ای با عنوان همگرایی تناقض نمای نظارت الکترونیک در برخورد تکنوکراسی و حریم خصوصی، ضمن پذیرش ضرورت نظارت الکترونیک، آن را مقتضای امنیت افراد در فضای مجازی دانسته و به بازتعریف حریم خصوصی در فضای مجازی پرداخته است. در پژوهش دیگری، کریمی نیا، سلمانی و انصاری مقدم (۱۴۰۰) در مقاله‌ای تحت عنوان نقش صنعت و فناوری رسانه در پیشگیری از وقوع جرم، وجود فناوری را به مثابه یک ابزار سودمند در راستای پیشبرد اهداف رسانه و کمک به دستگاه عدالت کیفری در راه مبارزه با بزهکاری تلقی نمودند.

## ۱-۱. مهندسی کنترل اجتماعی

مهندسی کنترل اجتماعی به عنوان یکی از رویکردهای نوین در پیشگیری و مهار جرم، با تمرکز بر طراحی محیطی و فناوری محور، تلاش می‌کند امکان ارتکاب جرم را از طریق تغییر شرایط محیطی یا محدودسازی دسترسی مجرمان به فرصت‌های مجرمانه کاهش دهد. این رویکرد که ریشه در نظریه‌های جرم‌شناسی، مانند نظریه انتخاب عقلانی (Rational Choice Theory) و نظریه فعالیت روزمره (Routine Activity Theory) دارد، بر این ایده استوار است که جرائم نه صرفاً برآمده از نیت مجرمانه، بلکه محصول تعامل سه عنصر مجرم، **مُصمم، هدف مناسب و نبود نگهبانان** مؤثر است. (نجفی ابرندآبادی، ۱۳۹۶، چ، هفتم، ص. ۱۵) برخی از کارکردهای اساسی مهندسی کنترل اجتماعی با محوریت فناوری به شرح زیر است:

الف) **تقویت پیشگیری موقعیت محور:** (Situational Crime Prevention) طراحی محیطی با به‌کارگیری فناوری در معماری شهری، نظیر چراغ‌های حسگر حرکت، این چراغ‌ها با افزایش نور در مسیرهای تاریک، فرصت‌های جنایی را کاهش می‌دهند. نمونه عینی این فناوری را می‌توان در سیستم هوشمند روشنایی معابر در سنگاپور مشاهده کرد که مطابق گزارش پلیس سنگاپور در مناطق نصب شده، آمار جرم سرقت تا ۳۰ درصد کاهش یافته است. دسترسی بیومتریک به ساختمان‌ها، فرصت‌های ارتکاب جرم را کاهش می‌دهد. (نیازپور، ۱۴۰۲، ص. ۴۸) همچنین دوربین‌های هوشمند با قابلیت تشخیص چهره، رفتارهای مشکوک یا سلاح، مانند سیستم ShotSpotter برای مداخله پیش از وقوع جرم استفاده می‌شوند. (Laufs & Borrión, 2022, P.412)

ب) **تحول در کشف و پیگرد جرائم و شناسایی مجرمان:** بهره‌گیری از بانک‌های DNA، نمونه عینی استفاده از تحلیل DNA در تیرئه متهمان بی‌گناه را می‌توان در پروژه Innocence Project در آمریکا مشاهده نمود که با استفاده از آزمایش DNA تاکنون بیش از ۳۷۵ نفر را از اعدام یا حبس‌های طولانی نجات داده است. ردیابی دیجیتال تراکنش‌های مالی و تحلیل ارتباطات شبکه‌ای برای کشف سازمان‌های جنایی، جملگی محصول حضور و نقش فعال فناوری در کنترل اجتماعی جرم است. (Levi & Wall, 2004, P.16) ادله الکترونیک نظیر استخراج داده از تلفن‌های همراه، رسانه‌های اجتماعی و شبکه‌های اطلاعاتی به عنوان مدرک در محاکم قضایی مورد استفاده قرار گرفته و سبب تسهیل کشف و اثبات جرائم ارتكابی می‌گردند. (پورصادقی، ۱۴۰۰، ص. ۱۱۶)

ج) بهینه‌سازی مدیریت منابع قضایی: سیستم‌های مدیریت پرونده با دیجیتال‌سازی فرآیندهای دادرسی - تشکیل پرونده‌های الکترونیک سبب کاهش زمان رسیدگی و جلوگیری از اطاله دادرسی می‌شوند. (Cheng, 2013, P.43) استفاده از نقشه‌های حرارتی جرم (Crime Mapping) برای توزیع هدفمند نیروهای پلیس، موجب پیش‌بینی کانون‌های جرم‌خیز و حضور پررنگ پلیس در این کانون‌ها می‌گردد. (Byrne & Marx, 2011, P.65)

با بررسی سیر تحول فناوری در کنترل اجتماعی جرم، به نظر می‌رسد جایگزینی روش‌های سنتی با فناوری‌های نظارتی نه تنها یک تحول اجتناب‌ناپذیر است، بلکه پیامدهای پارادوکس گونه‌ای را ایجاد کرده است که نیازمند بازاندیشی جدی است. این جایگزینی در عمل به کاهش نقش کنشگران انسانی و تبدیل ابزارهای نظارتی به اهداف خود مختار منجر شده است، بدون آنکه الزاماً به ارتقای کیفی عدالت کیفری بینجامد.

## ۱-۲. جایگزینی شیوه‌های کنترل اجتماعی سنتی با فناوری‌های نظارتی

فناوری‌های جدید در نظام عدالت کیفری به منظور پیشگیری از جرم و بهبود عملکرد پلیس مورد استفاده قرار می‌گیرند. اما در خصوص چگونگی و چرایی اتخاذ برخی از این فناوری‌ها و پیامدهای آن و همچنین راه‌حل‌های فناوری محور برای حل مشکل جرم، اطلاعات بسیار کمی در دسترس است.

استفاده از فناوری‌های جدید با کمک ابزارهای مبتنی بر هوش مصنوعی در نظام عدالت کیفری، صرف نظر از تسهیل فرآیند کشف و پیگیری جرائم به ویژه جرائم پیچیده‌ای نظیر پولشویی و کلاهبرداری‌های الکترونیک، ذاتاً برای جوامع صنعتی و حتی جوامع غیر صنعتی جذاب است. مخالفت با فناوری‌های جدید هرچند عملیات آن ناشناخته و تبعات آن غیر قابل پیش‌بینی باشد، از سوی جوامع قابل پذیرش نیست؛ زیرا همواره فناوری مترادف با پیشرفت تلقی شده است. از اینرو مخالفت با فناوری به مثابه عقب مانده بودن، مقاوم بودن در برابر تغییر و واپس‌گرا بودن تعبیر می‌شود. (Byrne & Marx 2011, P.32)

هر قسم از فناوری در بردارنده پیامدهای ناخواسته‌ای برای فرآیندهای کنترل اجتماعی است که درک آن‌ها از اهمیت بسیاری برخوردار است. اولین و شاید برجسته‌ترین موضوع مرتبط با فناوری‌های مدرن این باشد که آیا در طول زمان متولیان سیاست جنایی، نظیر افسران پلیس، قضات دادگاه، مددکاران اصلاحات اجتماعی و... با اشکال مختلف فناوری جایگزین خواهند شد یا خیر؟ به عنوان مثال با وجود

دوربین‌های مدار بسته در مکان‌های عمومی و دوربین‌های کنترل سرعت، همچنان حضور افسران پلیس برای گشت‌زنی در خیابان‌ها ضروری است؟ آیا این پرسش مطرح نمی‌شود که چرا با وجود دوربین‌های کنترل سرعت و دوربین‌های تشخیص چهره برای شناسایی متخلفان قوانین راهنمایی و رانندگی، همچنان از نیروهای پلیس در راه‌ها و جاده‌ها استفاده می‌شود؟ سناریوهای مشابهی را می‌توان در خصوص تأثیر احتمال فناوری‌های مختلف در دادگاه‌ها و ایجاد پرونده‌های الکترونیک، صدور احکام با کمک هوش مصنوعی به جای قضات، استفاده از دستگاه‌های ردیاب زندانیان به جای ناظران زندان و نصب دوربین‌هایی با قابلیت ردیابی و مکان‌یابی در مکان‌های عمومی برای کشف و شناسایی مظنونان و پیشگیری از نقض قوانین ارائه نمود. (Cheng, Lijiao, 2013, P.54) فناوری که در ابتدا با هدف کمک و ارتقای نظام عدالت کیفری مورد استفاده قرار گرفت و می‌بایست به عنوان یک ابزار در خدمت متولیان سیاست جنایی استفاده می‌شد، با توسعه استفاده از آن رفته رفته جایگزین این متولیان از جمله قضات خواهند شد. در چنین شرایطی این نرم افزار یا ربات است که تصمیم می‌گیرد نه قضات و کارشناسان حرفه‌ای، تصمیماتی که تبعات حقوقی متعدد دارد. (هالوی، ۱۴۰۰، ص. ۱۱۸) برای مثال، در پرونده‌های تکرارشونده با موضوعات همسان، نظیر جرائم راهنمایی و رانندگی که پاسخ‌ها تقریباً سیستمی ارائه می‌گردد، همواره این خطر به طور جدی وجود دارد. لذا چنین مسائلی جملگی از دغدغه‌های اصلی استفاده بی‌رویه از فناوری در کنترل اجتماعی جرم است. به اعتقاد نگارنده، جایگزینی فناوری‌های نظارتی با روش‌های سنتی، تنها زمانی به تحقق عدالت کیفری کمک می‌کند که در چارچوب یک مدل تکمیلی قرار گیرد. به عنوان مثال الگوریتم‌های پیش‌بینی کننده جرم، می‌بایست صرفاً به عنوان داده‌های مقدماتی در اختیار قضات قرار گیرند، نه اینکه مبنای صدور حکم باشند. لذا بازتعریف مفهوم امنیت به مثابه مفهوم چند بعدی که افزون بر کنترل فیزیکی، بر پیشگیری اجتماعی و حفظ کرامت انسانی تأکید دارد، ضروری می‌نماید. این رویکرد مستلزم تدوین چارچوب‌های حکمرانی مسئولانه (شامل قوانین شفاف، نهادهای ناظر مستقل و آموزش اخلاق فناوری برای کنشگران) است تا از تبدیل فناوری به ابزار سرکوب جلوگیری کند.

## ۲. پیامدهای ساختاری اتکای انحصاری به فناوری

استفاده انحصاری از فناوری در کنترل جرم، در حال تبدیل شدن به پارادایم مسلط در نظام‌های عدالت کیفری معاصر است. این رویکرد اگرچه وعده‌دهنده افزایش کارایی و کاهش هزینه‌هاست، اما با ایجاد یک بحران سه گانه (اخلاقی-اجتماعی-انسانی) مواجه است. فناوری محوری بی‌ضابطه، نه تنها ارزش‌های بنیادین حقوق کیفری را تخریب می‌کند، بلکه خود به عاملی برای تولید نابرابری و بی‌اعتمادی

ساختاری تبدیل می‌شود. با این حال، اتکای بی‌رویه به شیوه‌های مهندسی کنترل، بدون در نظر گرفتن پیامدهای اجتماعی و اخلاقی، می‌تواند به جای حل مسئله، بحران‌های جدیدی در نظام عدالت کیفری ایجاد کند که در اینجا چند مورد از آن‌ها مورد اشاره قرار می‌گیرد:

استفاده انحصاری از فناوری به عنوان ابزار اصلی کنترل اجتماعی جرم، اگرچه ظرفیت افزایش کارایی نظام عدالت کیفری را دارد، اما تحولات ساختاری عمیقی در بنیان‌های نظام عدالت کیفری ایجاد می‌کند. این بخش به تحلیل دقیق سه چالش بنیادین ناشی از این رویکرد می‌پردازد: ۱- فروپاشی اصول اخلاقی در عدالت کیفری ۲- تهدید حریم خصوصی و شکل‌گیری جامعه نظارتی ۳- جایگزینی تدریجی کنشگران انسانی با سیستم‌های خودکار

## ۲-۱. فروپاشی اصول اخلاقی در عدالت کیفری

اتکای بی‌قید به فناوری، نظام عدالت کیفری را به سمت ابزاری شدن اخلاق<sup>۵</sup> سوق می‌دهد. مهندسی کنترل اجتماعی مبتنی بر الگوریتم‌ها، با حذف نقش محوری انسان در تصمیم‌گیری‌های قضایی، دو آسیب اساسی ایجاد می‌کند:

### الف: جایگزینی عدالت رویه‌ای با عدالت الگوریتمی

ابزارهای مهندسی کنترل در علوم جنایی نظیر حذف عامل انسانی و تهدید اصل فردی‌سازی مجازات‌ها، سیستم‌های خودکار نظیر الگوریتم‌های پیش‌بینی جرم (PredPol) یا نرم‌افزارهای ارزیابی خطر تکرار جرم (COMPAS)، اگرچه در شناسایی الگوهای مجرمانه کارآمد هستند، اما با تقلیل رفتار انسان به داده‌های آماری، اصولی چون تناسب مجازات با شخصیت مرتکب و توجه به زمینه‌های اجتماعی جرم را نادیده می‌گیرند (Angwin, J & Others, 2016, P,45). برای مثال، در ایالات متحده، استفاده از نرم‌افزار COMPAS منجر به افزایش نرخ برجسب «پرخطر» برای افراد رنگین‌پوست شد، که نشان‌دهنده تبعیض ساختاری در الگوریتم‌هاست. (Rudin, 2020, P. 615) سیستم‌های پیش‌بینی جرم (مثل نرم‌افزارهای سنجش خطر تکرار جرم) بر پایه داده‌های تاریخی و کلی‌شده عمل می‌کنند و قادر به درک «اوضاع و احوال خاص» مؤثر در ارتکاب جرم، نظیر سوابق فردی، شرایط اجتماعی و زمینه‌های فرهنگی نیستند. این مسئله با تناسب جرم و کیفر و فردی‌سازی مجازات‌ها در تعارض است (ابراهیمی، ۱۴۰۱، ص. ۳۸).

### ب: فرسایش مسئولیت‌پذیری اخلاقی

<sup>5</sup> Ethical Instrumentalization

هنگامی که قضات یا پلیس صرفاً به خروجی نرم‌افزارها متکی می‌شوند، استدلال اخلاقی و تفسیر انسانی از عدالت به حاشیه رانده می‌شود. به تعبیر گری مارکس: «هیچ روحی در سیستم‌های جدید وجود ندارد» (Marx, 2015). نمونه عینی این مسئله در پرونده‌های ایالات متحده مشاهده شد که استفاده از COMPAS – نرم‌افزار پیش‌بینی کننده جرم – منجر به نرخ خطای بالاتری برای افراد رنگین پوست گردید. (Angwin et al, 2016, P. 45) اگر به استفاده از فناوری در کنترل جرم بیش از حد بها داده شود، این فناوری ممکن است سیستم اصلاحات ما را به مسیر اشتباهی هدایت کند. شاید لازم باشد به یک الگوی اصلاحی فکر کنیم که در آن فناوری به جای تأکید بر کنترل مجرم، به دنبال اصلاح و تغییر او است. انجام این شیوه با یک درس ساده از تاریخ حقوق کیفری؛ «نیروهای بی‌رحم اغلب شکست می‌خورند» (James M, 2008, P.23) سازگار است.

با فرض اینکه ضعف نظام عدالت کیفری، تمایل فعلی آن را نسبت به طیف گسترده‌ای از نوآوری‌های مبتنی بر فناوری سوق می‌دهد، ولی علت اصلی طرفداری این نظام از فناوری، به لحاظ افزایش توانایی او در کنترل رفتار اشخاص است، به جای آنکه به دنبال تغییر و اصلاح رفتار آن‌ها باشد. (Purshouse, Joe, 2019, P 324) در مطالعه کنترل اجتماعی، عنصر اصلی درک جامعه شناختی است. فناوری، عدالت را به محاسبات تقلیل می‌دهد؛ حال آنکه عدالت ماهوی، درک درد انسان‌هاست نه تحلیل داده‌ها" (Miriam, 2012, P.194) درکی که مستلزم توجه به تمام تبعات کنترل، از جمله محدود نمودن حریم خصوصی افرادی است که همواره به رعایت هنجارهای قانونی و اجتماعی وفادار بوده‌اند. لذا اتخاذ چنین رویکردی فارغ از توجه به پیامدهای آن، عدالت رویه‌ای را به عدالت الگوریتمی تقلیل داده و منجر به تضعیف مسئولیت‌پذیری اخلاقی قضات و پلیس می‌گردد. زمانی که تصمیم‌ها بر پایه خروجی نرم‌افزارها باشد، استدلال اخلاقی جای خود را به محاسبات مکانیکی می‌دهد.

## ۲-۲. نادیده گرفتن حریم خصوصی و ایجاد جامعه نظارتی

استفاده گسترده از فناوری به عنوان ابزار اصلی کنترل اجتماعی در عصر حاضر، تبعات اجتناب ناپذیری در بر دارد؛ از جمله تحت کنترل و نظارت درآوردن همه افراد اجتماع، اعم از مجرم و غیر مجرم، که این به معنی پایان مفهوم حریم خصوصی و افزایش بی‌اعتمادی و ترویج ترس از جرم در میان اعضای اجتماع است. (Jorge, Martinez-lucena, 2023, P. 212) فناوری‌هایی مانند دوربین‌های تشخیص چهره یا ردیابی موقعیت مکانی، با گسترش دامنه نظارت به کل جامعه (نه فقط مجرمان)، حریم خصوصی شهروندان را نقض می‌کنند. نمونه عینی این مسئله، پروژه اسکورینگ اجتماعی<sup>۱</sup> در چین است که با رصد رفتارهای روزمره شهروندان (مانند خریدها یا

تعاملات اجتماعی)، امتیازاتی را به آن‌ها اختصاص می‌دهد و دسترسی به خدمات عمومی مثل سفر با قطار را مشروط به این امتیازات می‌کند. (Botsman, R, 2017, P. 36) این رویکرد نه تنها با حق بر حریم خصوصی در تضاد است، بلکه ممکن است به سرکوب گروه‌های معترض بینجامد. (Creemers, R, 2018, P. 86) همچنین استفاده از فناوری پایش الکترونیک محکومان (دستبند یا پابند الکترونیک) اگرچه منجر به کاهش جمعیت زندان‌ها با جایگزینی حبس خانگی و دوری از فضای جرم‌زای زندان شده است ولی با چالش نقض حریم خصوصی خانواده‌ها با شنود غیر قانونی همراه است.<sup>۶</sup>

عادی‌سازی نظارت ۲۴ ساعته در اماکن عمومی، شهروندان را ناخواسته به اشتراک‌گذاران دائمی داده‌های شخصی تبدیل می‌کند. سیستم‌های تشخیص چهره در چین با ۶۲۰ میلیون دوربین، شهروندان را به "اشیای اسکن‌پذیر" تبدیل کرده‌اند. اسکورینگ اجتماعی چین با رصد رفتارهای روزمره - خرید، تعاملات اجتماعی - دسترسی به خدمات عمومی را مشروط به امتیازات می‌کند که این امر نه تنها حق ناشناس ماندن در عرصه عمومی را نقض می‌کند، بلکه به ایجاد جامعه‌ای مبتنی بر بی‌اعتمادی دامن می‌زند. (Botsman, 2017, P. 98) پژوهش لافس نشان می‌دهد ۸۷٪ شهروندان اروپایی، حضور در فضاهای عمومی را همراه با "اضطراب نظارتی" تجربه می‌کنند. (Laufs, 2022, P.45)

در حالیکه قوانینی مانند GDPR در اروپا یا BIPA در ایلینویز<sup>۷</sup> جمع‌آوری داده‌های بیومتریک را مشروط به رضایت آگاهانه می‌کنند، (Wang and Others, 2024, P. 187) در بسیاری از کشورها از جمله ایران، چارچوب جامعی برای نظارت بر فناوری‌های نوین وجود ندارد. این امر در حالیست که جمع‌آوری داده‌های بیومتریک به صورت گسترده در ایران مورد استفاده قرار می‌گیرد. نهادهایی نظیر **بانک‌ها** با احراز هویت مشتریان با اثر انگشت و اسکن عنبیه - مطابق دستورالعمل بانک مرکزی - **سازمان ثبت احوال** از طریق ثبت الگوی چهره و اثر انگشت در صدور کارت‌های هوشمند ملی و همچنین **پلیس** با استفاده از سیستم‌های تشخیص چهره در فضاهای عمومی نظیر متروی تهران یا مرزها به جمع‌آوری این داده‌ها در سطح کلان می‌پردازند. ایران فاقد قانون خاصی شبیه GDPR در اروپا یا BIPA در آمریکا برای نظارت بر جمع‌آوری، ذخیره و استفاده از داده‌های بیومتریک است. این خلأ حقوقی به سوءاستفاده نهادی و

<sup>۶</sup> پرونده‌های قضایی در ایالت کالیفرنیا، ۲۰۲۲

<sup>۷</sup> Illinois Biometric Information Privacy Act

احتمال نشت داده‌ها – مانند نشت اطلاعات بیومتریک در پایگاه‌های احراز هویت موبایل در سال ۱۴۰۰- و تبعیض سیستماتیک دام می‌زند.

فناوری‌های نظارتی با ایجاد شفافیت اطلاعاتی<sup>۸</sup> به باز تعریف مفهوم امنیت پرداخته و با تغییر ماهیت نظارت از «هدفمند» به «جمعی»، ساختارهای حقوقی و اجتماعی را بازتعریف می‌کنند. استفاده گسترده از فناوری‌های نظارتی، نگرانی‌های اخلاقی و اجتماعی قابل توجهی را ایجاد می‌کند. وابستگی به بخش خصوصی و برون سپاری مدیریت داده‌های حساس به شرکت‌هایی مانند Clearview AI، کنترل نهادهای دولتی بر اطلاعات را تضعیف و خطر سوءاستفاده تجاری یا امنیتی را افزایش می‌دهد. (Fussell, 2021, P.54). به عنوان مثال شرکت Clearview AI داده‌های چهره را از شبکه‌های اجتماعی استخراج نموده و در اختیار پلیس قرار می‌دهد که منجر به نقض حریم خصوصی در ابعاد جهانی می‌گردد. (Hill, 2020, P.23) افزون بر آن اخلاف در عملکرد الگوریتم‌ها به دلیل خطاهای فنی، تحریم‌ها یا حملات سایبری، می‌تواند کل فرآیند قضایی را متوقف کند. این مسئله در بحران‌هایی همچون؛ همه‌گیری کووید-۱۹ که افزایش استفاده از دادرسی الکترونیک را ضروری ساخت آشکار شد. (Laufa & Borrin 2022, P.11)

خصوصی‌سازی فناوری‌های نظارتی (مانند استفاده از شرکت‌های فناوری برای مدیریت داده‌های پلیس)، کنترل اطلاعات حساس را از دست نهادهای دولتی خارج می‌کند. بنابراین مهندسی کنترل اجتماعی با وجود آنکه ابزاری قدرتمند برای مقابله با جرم است، اما بدون توجه به ابعاد اخلاقی و حقوقی، می‌تواند به ابزاری برای نقض کرامت انسانی بدل شود. پیوند این رویکرد با علوم جنایی مستلزم باز تعریف مفاهیمی همچون؛ «امنیت» و «عدالت» در چارچوبی است که هم به کارایی فناوری احترام بگذارد و هم حقوق بنیادین شهروندان را پاس دارد.

حریم خصوصی به طور صریح در قوانین ایران مورد حمایت قرار نگرفته است، ولی می‌توان ذیل قوانین مختلف حریم خصوصی را مورد بررسی قرار داد. اصل ۲۵ قانون اساسی، از آزادی ارتباطات در خصوص رایج‌ترین وسایل ارتباطی حمایت کرده است. این اصل یکی از اصول مهم قانون اساسی است که به نحو روشن و مشخص به حمایت از حریم خصوصی ارتباطات پرداخته است. با تفسیر کلمات حیثیت و جان مندرج در اصل ۲۲ قانون اساسی، حریم خصوصی جسمانی را نیز می‌توان مشمول حمایت‌های قانون اساسی دانست.

<sup>8</sup>Information Transparency

(انصاری، ۱۳۸۳) به موجب قانون آیین دادرسی کیفری در خصوص منازل، حق حریم خصوصی و حق مالکیت با یکدیگر ادغام شده است، لذا حمایت از حریم خصوصی منازل در مقایسه با حریم خصوصی سایر اماکن مضاعف می‌شود. در مواد ۵۸ و ۵۹ قانون تجارت الکترونیک برخی از اصول ناظر بر حمایت از حریم داده‌های شخصی در محیط الکترونیکی مورد توجه قرار گرفته است که از آن جمله می‌توان به اصل تحصیل قانونی و مبتنی بر رضایت سوژه یا شخص موضوع گراوری و پردازش (ماده ۵۸) اصل تحصیل داده‌های مضیق و مرتبط (بندهای الف و ب ماده ۵۹) اصل درستی و صحت داده‌های گراوری شده (ماده ۵۹) اصل دسترسی ذینفع به داده پیام‌های مرتبط با خود (بند دوم ماده ۵۹) و اصل اصلاح و امحاء (بند ۲ ماده ۵۹) اشاره کرد.

در ماده ۵۷۰ قانون مجازات اسلامی در خصوص آزادی شخصی افراد و مواد ۵۷۲ تا ۵۷۵ در حمایت از حریم خصوصی جسمانی افرادی که به حبس یا توقیف غیر قانونی افراد ملت اقدام می‌کنند، مجازات‌هایی را مقرر نموده است. مواد ۵۸۰ و ۶۹۴ برای نقض حریم خصوصی منازل و مواد ۶۹۱ و ۶۹۲ برای حریم خصوصی اماکن، ضمانت اجرای کیفری لحاظ کرده‌اند.

با توجه به آنکه فناوری‌های عرصه کنترل اجتماعی، تقویت کننده امنیت و نقض حریم خصوصی به شمار می‌آیند، انتظار می‌رود که شهروندان در ازای امنیت بیشتر، بخشی از حریم خصوصی خود را معامله کنند. درحالی‌که این امر شهروندان را مجبور می‌کند که امنیت و حریم خصوصی را به عنوان بخشی از کالاهای قابل مبادله در نظر بگیرند، این مبادله پیامدهای اقتدار گرایانه احتمالی فناوری‌های امنیتی را پنهان می‌کند. بنابراین بحث مهم پیرامون تأثیر این فناوری‌ها بر میزان امنیت و حق حریم خصوصی افراد جامعه مطرح می‌شود. رویکردهای حاصل از تئوری‌های اقتصادی، رابطه میان حریم خصوصی و امنیت را به عنوان یک مبادله تعریف می‌کنند که به موجب آن هر افزایش در سطوح امنیتی، میزان حریم خصوصی شهروندان را محدود می‌کند. از نظر اجتماعی و سیاسی رویکرد مبادله مورد انتقاد قرار گرفته است؛ زیرا بحث سیاست امنیتی را به صرف موضوع ایجاد تعادل میان امنیت و حریم خصوصی محدود می‌کند. (Coleman & Mccahill, 2010, P. 43)

در واقع تصمیم افراد به مبادله حریم خصوصی و امنیت ناشی از فناوری‌های نظارتی تحت تأثیر عوامل جمعیتی، نهادی و فرهنگی است. شاخص‌هایی نظیر هویت قومی، نژادی، تحصیلات و سن شهروندان بر تمایل آن‌ها برای تجارت حریم خصوصی در ازای امنیت تأثیر می‌گذارد. در واقع نظر مردم در خصوص فناوری‌های امنیتی ممکن است تحت تأثیر عوامل دیگری قرار بگیرد که بیشتر به نحوه پرداختن این فناوری‌ها به اولویت‌های اجتماعی آن‌ها و زمینه‌های اجتماعی و نهادی که این فناوری‌ها در آن اجرا می‌شود، مربوط است. هرچه

شهروندان به نهادهای دولتی و عمومی اعتماد بیشتری داشته باشند، امنیت را به عنوان یک اولویت و فناوری را به عنوان روشی مؤثر برای رسیدگی به این اولویت می‌بینند. در مقابل هر چه میزان بی‌اعتمادی به دولت‌ها بیشتر باشد، حریم خصوصی بیشتر در اولویت قرار گرفته و وجود مشکلات امنیتی از سوی شهروندان انکار می‌شود.

با این حال، اگرچه این امر پذیرفته شده است که نظارت بیشتر لزوماً به معنای امنیت بیشتر است، این قضیه که نظارت بیشتر باید به قیمت نقض حریم خصوصی باشد، مورد پذیرش قرار نگرفته است. (Degli, Esposti, 2010, P. 15) از سوی دیگر این فناوری‌ها فرآیندهای تبعیض آمیز طبقه‌بندی شهروندان را به گروه‌های پر خطر و کم خطر تسهیل می‌کنند، رویه‌ای که از طریق آن همه شهروندان تحت نظارت، با شاخص‌های خطر کدگذاری می‌شوند و افراد به «مسافران مورد اعتماد»<sup>9</sup> یا کم خطر و «مهاجران مشکوک»<sup>10</sup> یا پر خطر دسته‌بندی می‌شوند. این رویه در کشورهای توسعه یافته معمولاً از سوی شرکت‌های خصوصی انجام می‌شود که به پذیرش گروه‌های خاصی از مسافران، نظیر تاجران و مدیران و محدود نمودن گروه‌هایی مانند مهاجران و پناهجویان منتهی می‌گردد. (Ibid, P.18) افزایش نظارت بر گروه‌های خاصی به منظور پیشگیری از خطر ارتکاب و یا تکرار جرم، می‌تواند به اختلافات قومی، نژادی، اجتماعی و اقتصادی دامن زده و آن‌ها را بازتولید کند. به عنوان مثال؛ نرم افزار آمریکایی سنجش خطر تکرار جرم، آمار جمعیت آفریقایی - آمریکایی رادر دوره زمانی دو سال بعد از تحمل کیفر، دو برابر بیشتر از دیگران تخمین می‌زند.

افزون بر این، فناوری ناتوان از استدلال حقوقی و یا علت شناسی است. رویکرد جرم شناختی علت شناسی که همچون یک سینماگر به دنبال گردآوری اطلاعات از مراحل مختلف زندگی مرتکب و چیدمان سکانس‌های زندگی شخصی و اجتماعی او است (نجفی ابرندآبادی، ۱۳۹۸، ص. ۲۴)، به گونه‌ای در مواد مختلف قانون مجازات و آیین دادرسی کیفری تجلی یافته است. ماده ۱۸ قانون مجازات اسلامی در همین راستا دادگاه را مکلف ساخته که در صدور حکم تعزیری با رعایت مقررات قانونی (بند ب) سوابق و وضعیت فردی، خانوادگی و اجتماعی مرتکب را مورد توجه قرار دهد. اصولاً اجرایی نمودن این بند با تشکیل پرونده شخصیت امکان پذیر است که در برخی جرائم به موجب ماده ۲۰۳ قانون آیین دادرسی کیفری، بازپرس مکلف است در حین انجام تحقیقات، دستور تشکیل آن را به واحد مددکاری اجتماعی صادر کند. از اینرو تصمیم قاضی اساساً بر پایه ارزش‌های انسانی و ملاحظات اجتماعی مبتنی است، درحالی‌که رایانه

<sup>9</sup> Trusted travellers

<sup>10</sup> Suspicious immigrants

از درک این ارزش‌ها عاجز است. عادی سازی نظارت مستمر افزون بر بی‌اعتمادی ساختاری موجب می‌شود که شهروندان در ازای امنیت کاذب، آزادی‌های خود را معامله کنند، بدون آنکه بدانند داده‌هایشان چگونه علیه آن‌ها مورد استفاده قرار می‌گیرد. لذا به جای تمسک صرف به استفاده از فناوری در کنترل اجتماعی، می‌بایست با اتخاذ تدابیر شایسته، فناوری را با لحاظ تبعات و آثار سوء آن مورد استفاده قرار داد.

### ۲-۳. جایگزینی کنشگران انسانی و تهدید مشروعیت نظام قضایی

تبدیل فناوری از ابزار کمکی به حاکم مطلق، موجب دگرذیسی ساختاری در نهادهای عدالت کیفری گشته و دو خطر جدی ایجاد می‌کند :

#### الف: حذف تدریجی نقش انسان

نمونه‌های عینی مانند جایگزینی قضات با هوش مصنوعی در صدور حکم جرائم تکرار شونده (مثل تخلفات راهنمایی و رانندگی)، یا استفاده از نرم‌افزارهای پیش‌بینی جرم به جای مددکاران اجتماعی، حذف عنصر انسانی از فرآیندهای قضایی را تسریع می‌کند .

#### ب: تغییر هدف از اصلاح به کنترل

تمرکز انحصاری بر «پیشگیری موقعیت‌مدار» (مثل دوربین‌های مدار بسته) بدون سرمایه‌گذاری در حوزه پیشگیری اجتماعی (آموزش، اشتغال، بازپروری)، نظام عدالت را از مأموریت اصلی خود—یعنی اصلاح مجرمان و بازگرداندن آن‌ها به جامعه—دور می‌کند و نتیجه این امر تولید چرخه معیوب جرم به جای بازپروری مجرمان است. (نیازپور، ۱۴۰۲، چ دوم، ص. ۲۱)

پیامدهای فوق حاکی از این است که؛ اتکای انحصاری به فناوری، کنترل اجتماعی جرم را به پروژه‌ای خود ویرانگر تبدیل می‌کند که از بعد اخلاقی منجر به تقلیل انسان به داده‌های زیستی<sup>۱۱</sup> و از بعد اجتماعی موجب ایجاد دیوار نامرئی میان شهروندان و حکومت می‌گردد و از نظر حقوقی با نقض سیستماتیک اصول حاکمیت قانون همراه است. این امر نه تنها کارکرد اصیل نظام عدالت کیفری – مانند اصلاح مجرمان و تضمین دادرسی منصفانه – را تضعیف می‌کند بلکه با ایجاد وابستگی ساختاری، شکنندگی سیستم را افزایش می‌دهد. برای خروج از این بن‌بست، باید از الگوی تکمیلی بهره برد که در آن فناوری در خدمت عدالت کیفری باشد نه جایگزین آن. این تحولات

<sup>11</sup> Biological Data Points

باز تعریف مفاهیمی مانند «عدالت»، «مسئولیت پذیری» و «حریم خصوصی» در چارچوب فناوریانه را اجتناب ناپذیر ساخته است. بنابراین فناوری ذاتاً شر نیست، اما اتکای انحصاری و بی ضابطه به آن، تهدیدی جدی برای عدالت، اخلاق و کرامت انسانی است. لذا به نظر می‌رسد که راه نجات در تلفیق فناوری با رویکردهای اصلاحی است.

### ۳. راهکارهای کاهش تبعات استفاده از فناوری های نظارتی

به منظور کاهش عواقب نامطلوب استفاده از فناوری در کنترل اجتماعی در درجه نخست این مسئله می‌بایست مورد توجه قرار گیرد که آیا صرف هزینه در بکارگیری فناوری در شیوه‌های غیر قهری پیشگیری، نظیر ارتقای سطح آموزش، ارتقای کیفیت و استحکام خانه‌ها و ساخت خانه‌های هوشمند، جابه‌جایی افراد از مناطق جرم‌خیز به منطقه‌هایی با امکانات رفاهی و ورزشی بیشتر، ایجاد شغل برای جوانان بیکار، استفاده بیشتر از پلیس پیاده به جای گشت‌های سواره و نظارت‌های الکترونیک و ... نتیجه بهتری در پیشگیری و کنترل جرائم دارد یا صرف هزینه در ایجاد و نصب ابزارهای مبتنی بر فناوری و حذف هرچه بیشتر نیروی انسانی می‌تواند مفیدتر باشد؟

ما به یافتن راه‌هایی برای استفاده از فناوری برای اهداف مهم‌تر و تقویت عملکرد اخلاقی در هر دو سطح فردی و نهادی نیاز داریم. بنابر نظر محققانی همچون رایلی<sup>۱۲</sup>؛ هر جا که اراده‌ای وجود داشته باشد، راهی وجود دارد<sup>۱۳</sup>. با امکانات کنترل گری که به واسطه علم و فناوری در دسترس همگان قرار گرفته است، این جمله ممکن است به این صورت معکوس شود: هر جا که راهی هست، اراده‌ای وجود داشته است. لذا همواره باید مراقب بود که مطمئن شویم که این انسان است که فناوری را کنترل می‌کند نه فناوری انسان را.

همانگونه که Jacques در سال ۱۹۶۴ استدلال کرد، این خطر همواره وجود دارد که ابزارهای مبتنی بر فناوری خود به خود تقویت و روزآمد شده و بدون آنکه متوجه شویم، دور از چشم جامعه و بدون خواست و اراده انسان، تبدیل به هدف نهایی شده و یا حتی اهداف خود را به جامعه تحمیل کنند. از اینرو می‌بایست همواره به ارزیابی اثربخشی فناوری‌های فناوری محور در اصلاحات سازمانی و اجتماعی ادامه دهیم و راهکارهایی جهت کاهش پیامدهای ناخواسته این نوع از فناوری را مورد توجه و بررسی قرار دهیم که مبدا فناوری جدید

مترادف با کنترل افراد باشد. (Wang, Xukang and Others, 202, P. 44)

<sup>12</sup> Wryly

<sup>13</sup> Where there is a will, there is a way

### ۳-۱. برقراری تعادل میان استفاده از فناوری‌های نظارتی و حمایت از حریم خصوصی

یکی از چالش‌های اصلی در استفاده از فناوری‌های نظارتی، ایجاد تعادل مناسب میان مزایای بالقوه این فناوری‌ها و نیاز به حمایت از حریم خصوصی است. سیستم‌های فناوری نظارتی از قابلیت‌های عدیده‌ای در حوزه‌های متفاوت برخوردارند، از افزایش امنیت و ساده‌سازی فرآیندهای شناسایی گرفته تا استفاده‌های شخصی و تسهیل دریافت خدمات. با این وجود، همانگونه که مطالعات موردی نشان می‌دهد، استقرار فناوری‌های نظارتی می‌تواند منجر به نقض جدی حریم خصوصی و تحت نظارت قرار گرفتن عموم جامعه در صورت عدم وجود حفاظت و نظارت متناسب شود. در سطح فردی سیستم‌های نظارتی مفاهیم مرسوم از حریم خصوصی به ویژه مفهوم حریم خصوصی در عموم - حق یک فرد برای ناشناس ماندن در ملاء عام<sup>۱۴</sup> - را به چالش می‌کشد. مباحث علمی کنونی بر عدم رضایت ضمنی در فضاهای عمومی، حمایت از رضایت صریح و آگاهانه که حساسیت‌های فناوری‌های نظارتی را تشخیص دهد، تأکید می‌کند. (Ibid, P.46)

معمای اخلاقی زمانی پدیدار می‌گردد که افرادی که تمایلی به تسلیم شدن در برابر فناوری‌های نظارتی و افشای اطلاعات هویتی خود ندارند، اغلب چاره‌ای جز کناره‌گیری از خدمات عمومی یا اجتماعی ندارند، امری که خود مستلزم نوعی رضایت اجباری است که با هنجارهای اخلاقی در تضاد آشکار است.

افراد اغلب از اینکه چه زمانی، چگونه و برای چه هدفی اطلاعات هویتی آن‌ها تجزیه و تحلیل شده، بی‌اطلاع هستند. این شیوه پنهانی جمع‌آوری داده‌ها، نه تنها موجب نقض حریم خصوصی افراد می‌شود، بلکه موجب عدم تعادل قدرت میان افراد جامعه و نهادهایی که حق دسترسی به این داده‌ها را دارند، می‌گردد، اعم از اینکه دولتی یا خصوصی باشند.

فرآیند کالاسازی هویت شخصی بر نگرانی‌های مربوط به سوء استفاده‌های احتمالی و غیر انسانی از قدرت می‌افزاید. (Ibid, P.47)

لذا می‌بایست مزایای بهره‌وری از فناوری‌های نظارتی با مصالح اخلاقی عمیق سنجیده شود. چنین امری مستلزم ایجاد چارچوب‌های دولتی است که استقلال، رضایت معنادار افراد و حفاظت از حریم خصوصی در ملاء عام را در اولویت قرار دهد. ایجاد تعادل مناسب میان ابزارهای نظارت الکترونیک و حمایت از حقوق بشر، مستلزم اتخاذ رویکرد چند جانبه و تطبیقی از سوی حکومت است. سیاستگذاران و توسعه دهندگان فناوری‌های نظارتی می‌بایست در تعامل مداوم با اخلاق‌گرایان، حقوق‌دانان و جامعه مدنی باشند تا اطمینان حاصل کنند

<sup>14</sup> An individual's right to anonymity in public spaces

که این فناوری به گونه‌ای توسعه یافته و مورد استفاده قرار می‌گیرد که به حقوق فردی و ارزش‌های اجتماعی احترام می‌گذارد. این متضمن شفاف سازی و پاسخگویی قوی نهادها در برابر افراد و همچنین ارائه گزینه‌هایی در اختیار افراد به منظور انصراف از ضبط اطلاعات هویتی خویش است. در نهایت هدف اصلی این رویکرد، استفاده از مزایای فناوری نظارتی در عین کاهش خطرات و اثرات منفی آن است. با محوریت حقوق بشر و اخلاق در اداره فناوری‌های نظارتی، می‌توان به سمت آینده‌ای حرکت نمود که فناوری بدون به مخاطره انداختن حقوق و آزادی‌های اساسی انسان در خدمت منافع عمومی باشد. این امر نه تنها مستلزم اتخاذ تدابیر فنی و حقوقی است، بلکه نیازمند یک تغییر فرهنگی به سوی ارزش گذاری بیشتر حریم خصوصی و استقلال فردی در یک دنیای دیجیتال است.

## ۳-۲. استفاده از فناوری با رعایت چارچوب‌های اخلاقی

این حق می‌بایست برای همه افراد جامعه به رسمیت شناخته شود که بدانند چه زمانی و چگونه اطلاعات حاصل از فناوری‌های نظارتی جمع‌آوری شده و مورد استفاده قرار می‌گیرد. مقررات مربوط به استفاده از سیستم‌های نظارتی باید آشکارا در خصوص اهداف جمع‌آوری اطلاعات، نهادهایی که حق استفاده از آن‌ها را دارند و حقوق شهروندان شفاف سازی کند. در صورت امکان می‌بایست به افراد، فرصتی برای انتخاب یا انصراف از جمع‌آوری و استفاده از داده‌های نظارتی داده شود. در شرایطی که ممکن است اخذ رضایت فردی امکان پذیر نباشد، می‌بایست اقدامات شفاف برای اطمینان از پاسخگویی عمومی اتخاذ شود. نظر به سرعت تغییرات سیستم‌های مبتنی بر فناوری و ماهیت در حال تحول خطرات و مضرات این فناوری‌ها، بسیار مهم است که چارچوب‌های نظارتی، شامل تدوین مقررات منسجمی به منظور نظارت و بررسی مستمر فناوری‌ها و شیوه‌های کسب اطلاعات وجود داشته باشد. این امر می‌تواند شامل ارزیابی اثرات و تبعات منفی فناوری‌های نظارتی، آثار رضایت اجباری، انجام تحقیقات منظم از سوی اشخاص ثالث مستقل و نظارت مستمر بر میزان دقت این سیستم‌ها و بررسی سوگیری و احتمال سوءاستفاده از این داده‌ها باشد.

در بسیاری از ایالات آمریکا هر داده‌ای که از فناوری‌های نظارتی به صورت غیر مجاز و بدون اجازه شهروندان در اختیار پلیس قرار بگیرد، باید سریعاً پاک شود و حق طرح دعوا در دادگاه به بزه‌دیدگان استفاده غیر مجاز از فناوری‌های نظارتی اعطا شده است. این بزه‌دیدگان

می‌توانند خسارات وارده را از دادگاه مطالبه نموده و به ازای هر جرم، خسارت تعیین شده با توجه به میزان تبعات جرم از ۱۰۰۰ دلار تا ۱۰۰۰۰۰ دلار قابل پرداخت است.<sup>۱۵</sup>

اعلامیه جهانی حقوق بشر، میثاق بین‌المللی حقوق مدنی و سیاسی و سایر اسناد حقوق بشر، بنیادی را برای حفاظت از حریم خصوصی، کرامت و عدم تبعیض در زمینه فناوری‌های نوظهور فراهم می‌کند. همسویی فناوری‌هایی با چارچوب‌های بین‌المللی می‌تواند به اطمینان از سازگاری و قابلیت همکاری در سراسر حوزه‌های قضایی، تسهیل جریان داده‌های فرامرزی و همکاری در رسیدگی به چالش‌های فراملی کمک کند. توسعه حکمرانی مؤثر و مقررات گذاری در خصوص فناوری‌های نظارتی، مستلزم همکاری مستمر میان طیف متنوعی از ذینفعان، از جمله سیاستگذاران، مدیران صنعتی، سازمان‌های مردم‌نهاد، محققان دانشگاهی و جوامع آسیب‌دیده است. همکاری فراگیر و میان‌رشته‌ای می‌تواند کمک کند تا اطمینان حاصل شود که دیدگاه‌ها و تخصص‌های متعددی در خصوص حل چالش‌های پیچیده فناوری‌های نظارتی ایجاد شده است و چارچوب‌هایی، مناظر یا تجربه‌زندگی افرادی که بیشترین تأثیر را از این فناوری‌ها متحمل شده‌اند، تدوین گشته است. این رویکرد مشترک باید صداها و منافع جوامع به حاشیه رانده شده و آسیب‌پذیر را که ممکن است با خطرات و آسیب‌های نامتناسب ناشی از استقرار فناوری‌های نظارتی مواجه شوند، در اولویت قرار دهد.

از اینرو محققان خواستار توسعه چارچوب‌های اخلاقی برای گرایش به استفاده مسئولانه از فناوری‌های نظارتی شده‌اند. این چارچوب‌ها بر اصولی نظیر شفافیت، پاسخگویی، انصاف و احترام به حقوق افراد تأکید می‌کنند. برخی از محققان راه‌حل‌های فنی نظیر طراحی الگوریتم‌های حفظ حریم خصوصی و انجام محاسبات چند جانبه ایمن را برای کاهش خطرات فناوری‌های نظارتی پیشنهاد کرده‌اند. (van Brake, Rosamunde, & De Hert, 2011, P.113) منشور اروپایی اخلاق حرفه‌ای در زمینه استفاده از هوش مصنوعی در نظام قضایی، مصوب چهارم دسامبر ۲۰۱۸ کمیسیون اروپا که برای کشگران دولتی و خصوصی متصدی طراحی، توسعه و بکارگیری هوش مصنوعی جنبه ارشادی دارد، بر ۵ اصل کلی متکی است: ۱- رعایت حقوق بنیادین؛ ۲- شفافیت؛ ۳- مدیریت هوش مصنوعی

<sup>۱۵</sup> - این مقرر مبنی بر قانون حریم خصوصی اطلاعات بیومتریک ایلینوی (BIPA) مصوب ۲۰۰۸ در ایالت ایلینوی آمریکا است. به استناد ماده ۲۰ این قانون؛ هر فرد زیان‌دیده برای هر نقض (violation) غیر عمدی ۱۰۰۰ دلار و برای هر نقض عمدی ۵۰۰۰ دلار غرامت دریافت کند یا خسارت واقعی (actual damages) را مطالبه نماید. (هر کدام بیشتر باشد). در پرونده‌های گروهی (class action) با نقض‌های مکرر، مجموع غرامت‌ها ممکن است به صدها هزار دلار برسد.

توسط استفاده کننده؛ ۴- عدم تبعیض؛ ۵- امنیت. لذا الگوریتم پیش‌بینی رفتار توسط فناوری هوش مصنوعی می‌بایست به گونه‌ای طراحی و اجرا شود که با این ۵ اصل سازگار باشد.

از اینرو گونه‌های مختلف تبعیض میان افراد یا گروه‌ها باید کنار گذاشته شود تا از هر نوع نتیجه‌ای که متضمن ورود صدمه به حقوق و آزادی‌های بنیادین می‌گردد، اجتناب شود. روش‌های ارزیابی و پردازش داده‌ها نیز می‌بایست قابل درک و فهم بوده و به منظور حفظ اعتماد افراد به نظام عدالت کیفری، در دسترس همگان قرار گیرد. همچنین استفاده کنندگان از فناوری، از جمله پلیس و قضات ضروریست که به اندازه کافی از عملکرد آن اطلاع داشته باشند، به گونه‌ای که در هیچ شرایطی فناوری جایگزین انسان نشود. (ابراهیمی، ۱۴۰۱، ص. ۵۰)

بدیهی است که چالش‌های مذکور در استفاده از فناوری در کنترل اجتماعی و پیشگیری از جرم، نباید موجب شود که این فناوری کاملاً پرنقص جلوه کند. ناگفته پیداست که توان پردازش اطلاعات در این قبیل ابزارها از جمله هوش مصنوعی، قابل مقایسه با انسان نیست. در شرایطی که امروزه نظام عدالت کیفری با کمبود نیروی انسانی کارآمد و بودجه محدود مواجه است، ابزارهای مبتنی بر فناوری می‌توانند اطلاعات تکمیلی مفیدی در اختیار کشگران عدالت کیفری قرار دهند. از اینرو تمسک به فناوری در کنترل اجتماعی مفید است، مشروط به اینکه جایگاه و حدود مداخلات آن، از پیش در قانون تعریف و تعیین شده باشد و همچون یک ابزار هدایت‌گر در اختیار پلیس و سایر متولیان سیاست جنایی قرار بگیرد. از طرفی می‌بایست قدرت برتر متولیان در تشخیص و برآورد احتمال ارتکاب جرم حفظ شود. متولیان نظام قضایی از جمله قضات می‌بایست اختیار داشته باشند، زمانیکه اوضاع و احوال خاص مؤثر در ارتکاب جرم و نیز شخصیت مرتکب (نیازپور، ۱۳۹۳، ص. ۸۶) اقتضاء می‌کند، پیش‌بینی‌های حاصل شده از فناوری را کنار نهاده و ملزم به تبعیت از نتایج نرم افزارها نباشند.

به نظر می‌رسد وضع قوانین شفاف به منظور تنظیم چارچوب حقوقی استفاده از فناوری‌های نظارتی، اگرچه گامی ضروری است، اما به تنهایی برای پیشگیری از سوءاستفاده ساختاری کافی نیست. چالش اصلی در فقدان سازوکارهای نظارتی مستقل و ضعف در اجرای قانون نهفته است. به عنوان مثال حتی در کشورهای پیشرو نظیر اتحادیه اروپا با وجود GDPR نقض حریم خصوصی از سوی نهادهای دولتی گزارش شده است. در ایران نیز با توجه به پراکندگی قوانین موجود - نظیر مواد پراکنده در قانون تجارت الکترونیک یا قانون مجازات اسلامی - نیاز به یکپارچه سازی نظام حقوقی با محوریت حریم خصوصی در عصر دیجیتال احساس می‌شود. نکته حیاتی دیگر، خطر

نظارت نمایشی است؛ جاییکه نهادهای ناظر فاقد اختیارات کافی یا تخصص فنی هستند و صرفاً مبادرت به مشروعیت سازی صوری می کنند. از سویی اگرچه افزایش آگاهی متولیان سیاست جنایی ضروری است، اما این آموزش ها نباید به شعارهای اخلاقی تقلیل یابد. مسئله بنیادین، تقابل گفتمان امنیت محور با گفتمان حقوق شهروندی است. برای نمونه پلیس در عمل تحت فشار افکار عمومی برای کاهش جرم، ممکن است به رغم آگاهی از محدودیت های فناوری به ابزارهای نظارتی متوسل شود. همچنین مشارکت شهروندان در نظارت بر سیستم ها (مانند پلتفرم های گزارش دهی، چنانچه بدم تضمین شفافیت و پاسخگویی باشد، به نظارت جمعی خودخواسته تبدیل می شود که خود تهدیدی برای دموکراسی است. پیشنهاد کلیدی، تبدیل حریم خصوصی از یک موضوع به گفتمان اجتماعی با استفاده از ظرفیت های هنر و رسانه است.

### ۳-۳. ادغام مهندسی کنترل با رویکردهای اصلاحی

با سرمایه گذاری در طیف گسترده ای از فناوری های تغییر رفتار مجرم (اعم از سخت و نرم) مانند زندان های درمان محور، برنامه های اصلاح جامعه مبتنی بر آموزش و افزایش آگاهی افراد به کمک فناوری، استفاده از داروهای جدید برای کمک به معتادان و بیماران روانی، ممکن است بتوانیم راه هایی برای اعمال فناوری برای اهداف اصلاحی و تغییر رفتار مجرمان به جای روش های قهرآمیز و کنترل - گری، به شیوه هایی که منجر به اجتناب ارادی آن ها از رفتار مجرمانه باشد، یافت.

به جای تمرکز صرف بر پیشگیری موقعیت محور (Situational Crime Prevention)، که صرفاً با حمایت از آماج های جرم به دنبال پیشگیری از بزه دیدگی است، (نجفی ابرندآبادی، ۱۳۹۴، ص. ۳۷) می توان از فناوری برای توانمندسازی جامعه استفاده کرد. استفاده از راهبردهایی نظیر برنامه های آموزشی هوشمند برای جوانان مناطق جرم خیز یا استفاده از اپلیکیشن های گزارش دهی جرم با حفظ ناشناس بودن کاربران، شفاف سازی الگوریتم ها و مقابله با تبعیض، الزام به انتشار کدهای منبع (Open Source) و نرم افزارهای پیش بینی جرم، تشکیل کمیته های اخلاقی متشکل از حقوق دانان، جرم شناسان و جامعه مدنی برای بررسی سوگیری های الگوریتم، تقویت چارچوب های حقوقی می تواند در کاهش تبعات منفی استفاده از فناوری های نظارتی، بسیار کارآمد باشد. همانگونه که اتحادیه اروپا با تدوین قوانینی مانند مقررات عمومی حفاظت از داده ها (GDPR)، جمع آوری و استفاده از داده های بیومتریک را بدون رضایت صریح افراد ممنوع نمود.

البته باید اذعان داشت که تمرکز صرف بر توسعه الگوریتم‌های اخلاق محور - نظیر حریم خصوصی تفاضلی - ممکن است به توهم حل مسئله بینجامد. این فناوری‌های اگرچه مفیدند، اما مسئله تبعیض ساختاری را ریشه کن نمی‌کنند، چراکه داده‌های آموزشی خود اغلب انعکاس دهنده نابرابری‌های موجود در جامعه هستند. به علاوه هوش مصنوعی تبیین پذیر (XAI) هرچند شفافیت را افزایش می‌دهد، اما برای قضات و پلیس فاقد دانش کافی، به جعبه سیاه پیچیده‌تری تبدیل می‌شود. راه حل واقعی، سرمایه‌گذاری موازی در توانمندسازی نیروی انسانی - نظیر برگزاری دوره‌های سواد داده‌ای برای قضات - و باز طراحی فرآیندها است تا فناوری در خدمت انسان باقی بماند نه جایگزین آن.

راهکارهای ارائه شده در این بخش، علیرغم جامعیت نظری، با دو مانع اساسی در عمل روبه‌رو هستند: ۱- فقدان اراده سیاسی برای محدود کردن قدرت نهادهای امنیتی - قضایی ۲- سلطه گفتمان فناوری محور بر گفتمان حقوق بشری بشری در سیاست‌گذاری عمومی. ازاینرو تحقق این راهکارها مستلزم خیزشی سه جانبه از سوی حقوقدانان اصلاح طلب به منظور تدوین قوانین پیشرو، جامعه مدنی آگاه برای مطالبه‌گری و فناوری‌ان مسئولیت پذیر برای طراحی اخلاق محور است. بدون این ائتلاف، فناوری نظارتی نه تنها تهدیدات موجود را کاهش نخواهد داد، که خود به ابزار جدیدی برای بازتولید نابرابری بدل خواهد گشت.

### نتیجه‌گیری و پیشنهادها

پذیرش گسترده فناوری‌های نظارتی در کنترل اجتماعی جرم، شبکه پیچیده‌ای از فرصت‌ها و تهدیدها را آشکار ساخته است. با توجه به یافته‌های این پژوهش، فناوری‌های نظارتی در کنترل اجتماعی جرم، همچون شمشیری دولبه عمل می‌کنند: از یک سو با افزایش کارایی نظام عدالت کیفری، کشف جرائم پیچیده و بهینه‌سازی منابع، ابزاری ضروری برای مقابله با چالش‌های امنیتی عصر حاضر هستند؛ از سوی دیگر، پیامدهای ناخواسته‌ای چون؛ نقض حریم خصوصی، کاهش برابری اجتماعی، جابه‌جایی ارزش‌های اخلاقی و تبدیل ابزارهای نظارتی به اهدافی خودمختار را به همراه دارند. برای بهره‌گیری مسئولانه از این فناوری‌ها، پیشنهادها زیر در سه سطح راهبردی ارائه می‌شود:

الف: تدابیر حقوقی و نهادی (پیشگیری از سوءاستفاده ساختاری)

- تدوین چارچوب‌های شفاف قانون: وضع قوانین اختصاصی برای محدودیت جمع‌آوری داده‌ها) مانند GDPR اروپا یا BIPA آمریکا (با تأکید بر اصل حداقلی بودن داده (جمع‌آوری داده‌های ضروری)، لزوم اخذ رضایت آگاهانه پیش از جمع‌آوری اطلاعات بیومتریک، حق دسترسی، اصلاح و حذف داده‌ها توسط شهروندان

- ایجاد نهاد ناظر مستقل، متشکل از حقوق‌دانان، فناوران و جامعه مدنی برای بازرسی دوره‌ای الگوریتم‌ها (پیشگیری از تبعیض سیستماتیک)، اصلاح سازوکارهای نظارتی، الزام به انتشار کد منبع (Open Source) در سیستم‌های پیش‌بینی جرم مانند (COMPAS) برای شفافیت و شناسایی سوگیری‌های نژادی-اجتماعی، ممنوعیت استفاده از فناوری‌های نظارتی بدون ارزیابی تأثیرات اخلاقی و حقوقی پیشین

ب: راهکارهای فنی و عملیاتی (کاهش پیامدهای منفی)

- طراحی فناوری‌های اخلاق محور: توسعه الگوریتم‌های مبتنی بر حریم خصوصی تفاضلی (Differential Privacy) برای تحلیل داده‌ها بدون شناسایی افراد

- ادغام هوش مصنوعی تفسیرپذیر (Explainable AI) در سیستم‌های قضایی تا قضات و پلیس بتوانند منطق تصمیم‌گیری را درک کنند (پیشگیری از جعبه سیاه)

- تلفیق فناوری با رویکردهای اصلاحی: جایگزینی نظارت صرف با فناوری‌های توانمندساز جامعه مانند برنامه‌های آموزشی هوشمند برای جوانان مناطق جرم‌خیز، طراحی پلتفرم‌های گزارش‌دهی جرائم با حفظ ناشناس ماندن کاربران، سرمایه‌گذاری در زندان‌های درمان محور و برنامه‌های بازپروری مبتنی بر داده‌های رفتاری به جای تمرکز انحصاری بر کنترل موقعیت مدار.

ج: راهبردهای فرهنگی و آموزشی تقویت تاب‌آوری اجتماعی

- افزایش آگاهی متولیان سیاست جنایی: برگزاری دوره‌های آموزش اخلاق فناوری برای پلیس، قضات و مددکاران اجتماعی با محوریت اصولی همچون؛ محدودیت‌های ذاتی فناوری‌های نظارتی، ضرورت تلفیق فناوری با اصل فردی سازی مجازات‌ها (ماده ۱۸ قانون مجازات اسلامی)، تدوین منشور اخلاقی استفاده از هوش مصنوعی در عدالت کیفری (الگوبرداری از دستورالعمل‌های کمیسیون اروپا، ۲۰۱۸).

- تقویت مشارکت شهروندان از رهگذر تدابیری نظیر ایجاد پلتفرم‌های عمومی برای نظارت بر عملکرد سیستم‌های نظارتی؛ مانند دیده‌بانی جمع‌آوری داده‌های دوربین‌ها، ترویج گفتمان عمومی درباره «مبادله امنیت-حریم خصوصی» از طریق کمپین‌های رسانه‌ای (کاهش انفعال شهروندان).

یافته‌ها این پژوهش حاکی از این است که؛ فناوری نظارتی نه دشمن جامعه است و نه معجزه گر امنیتی؛ بلکه ابزاری است که کارایی آن در گرو برقراری تعادل میان چهار رکن است: ۱. شفافیت در اهداف و عملکرد سیستم‌ها ۲. پاسخگویی نهادهای مسئول در قبال سوءاستفاده ۳. رعایت انصاف و پیشگیری از تبعیض ساختاری ۴. احترام به کرامت انسانی و حفظ جایگاه محوری انسان در فرآیندهای قضایی. لذا تنها با اتخاذ رویکردی چندرشته‌ای حقوقی، فنی، اخلاقی و اجتماعی، می‌توان از تبدیل فناوری به ابزار سرکوب جلوگیری کرده و آن را به خدمت اهداف اصیل عدالت‌کفتری - یعنی تضمین دادرسی عادلانه و حفظ حریم خصوصی - درآورد. بنابراین، آینده مطلوب، نه در انفعال در مقابل فناوری، که در طراحی فعالانه چارچوب‌های حکمرانی مسئولانه آن است.

### پیشنهاد کلیدی برای پژوهش‌های آتی

بررسی امکان پیاده‌سازی مدل امتیازدهی اخلاقی (Ethical Scoring) برای فناوری‌های نظارتی در ایران، مبتنی بر معیارهای بومی (اسلامی‌سازی فناوری) و استانداردهای بین‌المللی.

## Abstract

New surveillance technologies in the field of social crime control act like a double-edged sword, simultaneously bringing vast opportunities and threats. On the one hand, these technologies are considered essential tools for addressing the security challenges by improving the efficiency of the criminal justice system, facilitating the detection of complex crimes and optimizing the use of limited resources. On the other hand, unconditional reliance on them leads to unintended consequences, the most important of which are the violation of individual privacy, the reduction of social equality. This research aims to present solutions to reduce these negative consequences, using a descriptive-analytical method and citing library resources, while examining the role of technology in crime control and the consequences of excessive use of surveillance technologies. Research findings indicate that surveillance technologies, although they increase security in the short term, in the long term lead to the erosion of privacy, structural discrimination, and the weakening of moral principles. Therefore, by adopting measures such as balancing security and privacy, developing clear laws to limit data collection, and increasing the awareness criminal justice system activists about the limitations of technology, can be reduced to some extent and human dignity can be respected

Keywords: Technology, Social Control, Privacy, Criminal Justice System

## فهرست منابع

- ابراهیمی، شهرام، ۱۴۰۱، «پیشگیری از تکرار جرم از طریق هوش مصنوعی؛ مقتضیات و محدودیت‌ها»، فصلنامه آموزه های حقوق کیفری، دوره نوزدهم، ش. ۲۳، صص ۳۳-۵۴
- انصاری، باقر، ۱۳۸۳، «حریم خصوصی و حمایت از آن در حقوق اسلام تطبیقی و ایران» مجله دانشکده حقوق و علوم سیاسی، ش. ۶۶
- بامپاسیکا، افیچیا، صادقی، سالار؛ ۱۴۰۲، «هوش مصنوعی به عنوان دلیل در محاکم کیفری»، فصلنامه تمدن حقوقی، دوره ۶، شماره ۱۸، صص ۲۴-۳۸ DOI:10.22034/L.2024.415210.1392
- سلیمی، میر رضا، گلدوست جویباری، رجب؛ ۱۴۰۱، «دروغ سنجی و حقوق متهم، مجله حقوقی دادگستری»، دوره ۸۶، شماره ۱۲۰، صص ۲۲۴-۲۰۱ DOI: 10.22106/JLJ.2022.542062.4506
- شکری، رضا؛ ۱۳۹۸، «حریم خصوصی ارتباطات در فضای الکترونیکی از منظر حقوق کیفری ایران و انگلستان»، فصلنامه حقوق و فناوری اطلاعات، سال اول، ش. ۱، صص ۶۵-۳۲
- فلاحتی، احمد، بزرگمهر، علی عباس؛ ۱۳۹۹، «بایسته های نوین علمی با رجوعی و تحقیق در قلمرو ادله اثبات حقیقت»، فصلنامه علمی مطالعات حقوق بشر اسلامی، دوره نهم، ش. ۱۹، صص ۱۸۸-۱۵۳
- DOR: 20.1001.1.23225637.1399.9.2.8.3
- مسعودی، امیر علی؛ ۱۴۰۰، «همگرایی تناقض نمای نظارت الکترونیک در برخورد تکنوکراسی و حریم خصوصی»، فصلنامه رهپویه ارتباطات و فرهنگ، دوره اول، شماره ۲، صص ۲۰-۷
- نجفی ابرند آبادی، علی حسین، ۱۳۹۴، به سوی تعریف یک سیاست ملی پیشگیری از بزهکاری، دیپاچه در براندون سی و دیوید پی فارینگتون، دانشنامه پیشگیری از جرم آکسفورد، تهران، میزان
- نجفی ابرند آبادی، ۱۳۹۶، پیشگیری عادلانه از جرم در علوم جنایی، مجموعه مقالات در تجلیل از دکتر محمد آشوری، ج. هفتم، تهران، انتشارات سمت

- نجفی ابرندآبادی، علی حسین، ۱۳۹۸، «پیوند حقوق کیفری و جرم شناسی»، مقاله در: افق‌های نوین حقوق کیفری، تهران، میزان
- نجفی ابرندآبادی، علی حسین، ۱۳۹۵ «کیفرشناسی نو - جرم شناسی نو، درآمدی بر سیاست جنایی مدیریتی خطر مدار»، مقاله در تازه های علوم جنایی (مجموعه مقالات)، زیر نظر علی حسین نجفی ابرندآبادی، کتاب اول، چاپ دوم، تهران، میزان
- نجفی ابرندآبادی، علی حسین، ۱۴۰۰ «نقش ریاضیات در آغاز و گسترش مطالعات علمی جرم»، دیپاچه در دایرةالمعارف ریاضیات و علوم جنایی، به کوشش مریم عباچی، چاپ دوم، تهران، میزان
- نجفی ابرندآبادی، علی حسین و هاشم بیگی، حمید ۱۴۰۳، **دانشنامه جرم شناسی**، چاپ هفتم، تهران، گنج دانش
- نیاز پور، امیرحسین، ۱۴۰۲، **پیشگیری از جرم**، چاپ دوم، تهران، داد گستر
- نیاز پور، امیرحسین، ۱۳۹۳، **اساسی سازی حقوق پیشگیری از جرم در ایران**، فصلنامه پژوهش حقوق کیفری، دوره دوم، شماره

۶

- Adkins, Lauren D, (2007), Biometrics: Weighing Convenience and National Security against Your Privacy, 13 Mich. Telecomm. & Tech. L. Rev, Volume 13, Issue, 2, 447 – 459
- An
- Angwin, J., Larson, J., Mattu, S., & Kirchner, L (2016). Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks.
- Botsman, R. (2017, October 21). Big Data Meets Big Brother as China Moves to Rate Its Citizens. Wired.
- Byrne, James & Marx, Gary, (2011), Technological Innovations in Crime Prevention and Policing, A Review of the Research on Implementation and Impact, Cahiers studies
- Cheng, Lijiao, (2013), Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory, journal homepage
- Clarke, R. V. (1997). Situational Crime Prevention: Successful Case Studies (2nd ed.). Routledge
- Creemers, R. (2018). China's Social Credit System: An Evolving Practice of Control. SSRN Electronic Journal.
- Degli Esposti, Sara, (2010), Public assessment of new security technologies: Beyond the trade-off between privacy and security, Calle Albasanz
- Ferguson, A. G. (2017). The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. NYU Press.
- Fussell, S. (2021, March 18). How Clearview AI Became a Tool of Law Enforcement—and Activists. The Atlantic.

- Garner, Bryan A, (2004), Black Law Dictionary; Eighth Edition, Thomson West, USA
- Gary T Marx, (2015), Technology and Social Control, Massachusetts Institute of Technology (MIT), Cambridge, MA, USA
- Grabosky, Peter, (1998), Technology & Crime Control, Australian Institute of Criminology
- Gur-Arye, Miriam, (2012), Human Dignity of “Offenders”: A Limitation on Substantive Criminal Law, *Crim Law and Philos*, 187-205
- Hill, K. (2020, January 18). The Secretive Company That Might End Privacy as We Know It. *The New York Times*.
- James M. Byrne, (2008), The best laid Plans: an assessment of the varied consequences of new technology of Crime and social control, Volume 72 Number 3
- Jorge, Martinez-lucena, (2023), The Issue of Social Control in Late Modernity: Alienation and Narrativity, *scientia fides*
- Laufs, Julian & Borrión, Hervé, (2022), Technological innovation in policing and crime prevention : Practitioner perspectives from London, *International Journal of Police Science & Management*, Vol. 24(2)
- Laufs, Julina, (2022), Crime Prevention and Detection Technologies in Smart Cities: Opportunities and Challenges, University College London
- Levi, Michael & Wall, David S, (2004), Technologies, Security, and Privacy in the Post-9/11 European Information Society, *Journal of Law and Society*, 194- 220
- Liu T, Yang B, Geng Y and Du S, (2021) , Research on Face Recognition and Privacy in China—Based on Social Cognition and Cultural Psychology, Department of Sociology,
- Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press.
- Mohapatra, Seema, (2016), Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation, Vol. 43: 1017
- Purshouse, Joe, (2019) Privacy & Campbell, Liz, Crime Control and Police use of Automated Facial Recognition Technology, *Criminal Law Review*, 188-204
- Rudin, C., Wang, C., & Coker, B. (2020). The Age of Secrecy and Unfairness in Recidivism Prediction. *Harvard Data Science Review*, 2(1).
- Thomas G. Blomberg and Carter Hay, (2007), *Visions of Social Control revisited ,Crime, Social Control and Human Rights*, Willan Publishing
- van Brake, Rosamunde, & De Hert, (2011), Paul, Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, nr. 20, 163-192
- Wang, Xukang and Others, (2024) “Beyond surveillance: privacy, ethics and regulations in face recognition technology, *Policy and Practice Reviews*
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.