



The Role of Technology in Social Control of Crime; Opportunities and Threats

Sara Meshkin Sanjabi¹ ✉

1. Corresponding Author, PhD Graduate in Criminal Law and Criminology, Faculty of Law, Tarbiat Modares University, Tehran, Iran. Email: s_meshkin@modares.ac.ir

Article Info

Article type:
Research Article

Received: 17 March 2025
Revised: 8 August 2025
Accepted: 19 August 2025
Available Online: 25 August 2025

Keywords

Technology, Social Control, Privacy, Criminal Justice System.



Abstract

New monitoring technologies in the field of social crime control act like a double-edged sword, simultaneously bringing vast opportunities and threats. These technologies are considered essential tools for addressing contemporary 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, and the transformation of monitoring tools into autonomous objectives. 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 monitoring technologies. Research findings indicate that monitoring 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 transparent laws to limit data collection, and increasing the awareness of criminal justice system activists about the limitations of technology, these consequences can be reduced to some extent and human dignity can be respected.

Cite this article: Meshkin Sanjabi, S. (2024). The Role of Technology in Social Control of Crime; Opportunities and Threats. *Criminal Law Doctrines*, 21(28), 299-328. <https://doi.org/10.30513/cld.2025.6818.2086>



© The Author(s). Publisher: Razavi University of Islamic Sciences.



نقش فناوری در کنترل اجتماعی جرم؛ فرصت‌ها و تهدیدها

✉ سارا مشکین سنجابی^۱

۱. نویسنده مسئول، دانش‌آموخته دکتری، گروه حقوق، دانشکده حقوق، دانشگاه تربیت مدرس تهران، ایران. رایانامه:

s.meshkin@modares.ac.ir

چکیده

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 جرایم 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 مهم‌ترینشان 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 کوتاه‌مدت امنیت را افزایش می‌دهد، در بلندمدت 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 داد و کرامت انسانی را محترم شمرد.

استناد: مشکین سنجابی، سارا. (۱۴۰۳). نقش فناوری در کنترل اجتماعی جرم؛ فرصت‌ها و تهدیدها. آموزه‌های حقوق کیفری، ۲۱(۲۸)، ۳۲۸-۳۹۹.

<https://doi.org/10.30513/cld.2025.6818.2086>



اطلاعات مقاله

نوع مقاله: پژوهشی

تاریخ ارسال: ۱۴۰۳/۱۲/۲۷

تاریخ بازنگری: ۱۴۰۴/۰۵/۱۷

تاریخ پذیرش: ۱۴۰۴/۰۵/۲۸

تاریخ انتشار برخط: ۱۴۰۴/۰۶/۰۳

کلیدواژه‌ها

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). دوره بعدی یعنی دوران مدرن، با ظهور دوربین‌های مداربسته (CCTV) در دهه ۱۹۷۰ و سیستم‌های شناسایی الکترونیکی (RFID) که نظارت غیرحضور را ممکن ساخت، همراه بود (Grabosky, 1998, P.53). آخرین دوره دوره کنونی است که به عصر دیجیتال معروف است و از مشخصه‌های بارز آن می‌توان به یکپارچه‌سازی هوش مصنوعی (AI)، پردازش کلان داده‌ها و الگوریتم‌های پیش‌بینی‌کننده جرم (PredPol, COMPAS) برای تبدیل داده‌ها به راهکارهای کنترلی اشاره کرد (Ferguson, 2017, P. 86).

از نیمه قرن ۲۰ 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^۱ و ایجاد وزارت امنیت داخلی^۲ 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 & 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 ۲۱ 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

1. Patriot Act

2. Department Of Homeland Security

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 چندوجهی 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 مفهومی چندبعدی 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 اقماعی، بلکه ترکیبی از هر دو رویکرد را در بر می‌گیرد (نجفی ابرندآبادی، ۱۴۰۳، 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 است 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 تحت نظارت قرار دارند. بدیهی است اشکال مختلف رفتار در مقیاس‌های کوچک‌تر را به راحتی می‌توان کنترل کرد، 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. در جامعه‌ای که از سیستم‌های کنترل فناوری محور استفاده می‌شود، صرفاً از اخلاق استفاده ابزاری شده است و اخلاق در صورتی پذیرش می‌یابد 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).

هرچند دامنه حریم خصوصی در منابع علمی متفاوت است، اما دو دیدگاه اصلی وجود دارد: ۱. حریم خصوصی به عنوان حقی بنیادین؛ ۲. حریم خصوصی به عنوان کالایی قابل مبادله. در گذشته، تمرکز اصلی بر تعریف هنجاری «حق بر خلوت»^۲ یا حق بر تنها ماندن بود. با افزایش سرعت فناوری در قرن ۲۱ نگرش به حریم خصوصی تغییر کرده است 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 وجود این، 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 بی‌قید 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.

این مقاله با اذعان به این که تعداد کمی از نوآوری‌های جدید کاملاً بدون مشکل‌اند، 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 کشورهایی که در استفاده از فناوری در ابعاد مختلف کنترل

3. Right to be left alone

اجتماعی پیشتازند، تمسک بسته است. این تحقیق در زمره پژوهش‌هایی^۴ است که محقق افزون بر تصویرسازی آنچه هست، به تشریح و تبیین دلایل چگونه بودن و چرایی وضعیت مسئله می‌پردازد. لذا تحقیق پیش‌رو «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 انجام‌شده 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 می‌پردازد.
۲. پیامدهای ساختاری اتکای 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 تحول‌آفرین در کنترل اجتماعی جرم، جایگاهی راهبردی در نظام‌های عدالت کیفری معاصر دارد. این بخش با بررسی سیر تکاملی فناوری و کاربردش در سه حوزه کلیدی پیشگیری، کشف و مهار جرم، جایگاه محوری آن را تبیین می‌کند.

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 تا امکان ارتکاب جرم را از طریق تغییر شرایط

۴. 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 تناقض‌نمای 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 پژوهشی دیگر، کریمی‌نیا و همکاران (۱۴۰۰) در مقاله «نقش صنعت و فناوری رسانه در پیشگیری از وقوع جرم»، وجود فناوری را به مثابه ابزاری سودمند در راستای پیشبرد اهداف رسانه و کمک به دستگاه عدالت کیفری در مبارزه با بزهکاری تلقی نمودند.

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 نگهداران مؤثر است (نجفی ابرنآبادی، ۱۳۹۶، ص ۱۵). برخی کارکردهای اساسی مهندسی کنترل اجتماعی با محوریت فناوری چنین است:

الف. تقویت پیشگیری موقعیت محور (Situational Crime Prevention): طراحی محیطی با به‌کارگیری فناوری در معماری شهری، نظیر چراغ‌های حسگر حرکت که با افزایش نور در مسیرهای تاریک، فرصت‌های جنایی را کاهش می‌دهند. نمونه عینی این فناوری را می‌توان در سیستم هوشمند روشنایی معابر در سنگاپور دید. بنابر گزارش پلیس سنگاپور، در مناطق نصب‌شده، آمار جرم سرقت تا ۳۰ درصد کاهش یافته است. دسترسی بیومتریک به ساختمان‌ها از فرصت‌های ارتکاب جرم می‌کاهد (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 یافت که با استفاده از آزمایش DNA تاکنون بیش از ۳۷۵ نفر را از اعدام یا حبس‌های طولانی نجات داده است. ردیابی دیجیتال تراکشن‌های 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، به‌عنوان مدرک در محاکم قضایی استفاده می‌شوند و سبب تسهیل کشف و اثبات جرائم ارتكابی می‌گردند (پورصادقی، ۱۴۰۰، ص ۱۱۶).

ج. بهینه‌سازی مدیریت منابع قضایی: سیستم‌های مدیریت پرونده با دیجیتال‌سازی فرایندهای 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 قانون‌های جرم‌خیز و حضور پررنگ پلیس در این قانون‌ها 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 تحولی اجتناب‌ناپذیر است، بلکه پیامدهای پارادوکس‌گونه‌ای را ایجاد کرده است که نیازمند بازاندیشی جدی است. این جایگزینی در عمل به کاهش نقش کنشگران انسانی و تبدیل ابزارهای نظارتی به اهداف خودمختار منجر شده است، بدون آن‌که الزاماً به ارتقای کیفی عدالت کیفری بینجامد.

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

فناوری‌های جدید در نظام عدالت کیفری به منظور پیشگیری از جرم و بهبود عملکرد پلیس استفاده می‌شوند. اما در خصوص چگونگی و چرایی اتخاذ برخی از این فناوری‌ها و پیامدهای آن و همچنین راه‌حل‌های فناوری‌محور 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، صرف‌نظر از تسهیل فرایند کشف و پیگیری جرائم، به‌ویژه جرائم پیچیده‌ای نظیر پول‌شویی و کلاهبرداری‌های الکترونیکی، ذاتاً برای جوامع صنعتی و حتی جوامع غیرصنعتی جذاب است. مخالفت با فناوری‌های جدید، هرچند عملیات آن ناشناخته و تبعاتش غیرقابل پیش‌بینی باشد، از سوی جوامع قابل پذیرش نیست، زیرا همواره فناوری مترادف با پیشرفت تلقی شده است. از این‌رو مخالفت با فناوری به مثابه عقب‌مانده بودن، مقاوم بودن در برابر تغییر و واپس‌گرا بودن تعبیر می‌شود (Byrne & Marx, 2011, p. 32).

هر قسم از فناوری دربردارنده پیامدهای ناخواسته‌ای برای فرایندهای کنترل اجتماعی است که درک آن‌ها اهمیت بسیاری دارد. اولین و شاید برجسته‌ترین موضوع مرتبط با فناوری‌های مدرن این باشد که آیا در طول زمان، متولیان سیاست جنایی نظیر افسران پلیس، قضات دادگاه و مددکاران اصلاحات اجتماعی، با اشکال مختلف فناوری جایگزین خواهند شد؟ برای مثال، با وجود دوربین‌های مداربسته در مکان‌های عمومی و دوربین‌های کنترل سرعت، آیا 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 کرد (Cheng, Lijiao, 2013, P. 54).

فناوری که در ابتدا با هدف کمک و ارتقای نظام عدالت کیفری استفاده گردید و می‌بایست به عنوان یک ابزار در خدمت متولیان سیاست جنایی استفاده می‌شد، با توسعه، استفاده از آن رفته‌رفته جایگزین این متولیان از جمله قضات خواهد شد. در چنین شرایطی، این نرم‌افزار یا ربات است که تصمیم می‌گیرد نه قضات و کارشناسان حرفه‌ای؛ تصمیماتی با تبعات حقوقی متعدد (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 مدلی تکمیلی قرار گیرد. برای مثال، الگوریتم‌های پیش‌بینی‌کننده جرم می‌بایست صرفاً به عنوان داده‌های مقدماتی در اختیار قضات قرار گیرند نه این‌که مبنای صدور حکم باشند. لذا بازتعریف مفهوم امنیت به مثابه مفهومی چندبعدی 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.

۳-۱. 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 بحرانی 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 این جا به چند مورد از آن‌ها اشاره می‌شود:

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. فروپاشی اصول اخلاقی در عدالت کیفری

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

۱-۲. 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 کارآمدند، 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 (نرم‌افزار پیش‌بینی‌کننده جرم) منجر به افزایش نرخ برچسب «پرخطر» برای افراد رنگین‌پوست شد، که نشان‌دهنده تبعیض ساختاری در الگوریتم هاست (Rudin, 2019, P. 615). سیستم‌های پیش‌بینی جرم (مثل نرم‌افزارهای سنجش خطر تکرار جرم) بر پایه داده‌های تاریخی و کلی شده 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).

۲-۲. فرسایش مسئولیت‌پذیری اخلاقی

هنگامی که قضات یا پلیس صرفاً به خروجی نرم افزارها متکی می‌شوند، استدلال اخلاقی و تفسیر انسانی از عدالت به حاشیه رانده می‌شود. به تعبیر گری مارکس: «هیچ روحی در سیستم‌های جدید وجود ندارد (Gary, 2015). نمونه عینی این مسئله در پرونده‌های ایالات متحده مشاهده شد که استفاده از COMPAS منجر به میزان 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، ممکن است سیستم اصلاحات ما را به مسیر اشتباهی هدایت کند. شاید لازم باشد به الگویی اصلاحی فکر کنیم که در آن، فناوری به جای تأکید بر کنترل مجرم، به دنبال اصلاح و تغییر اوست. انجام این شیوه با درسی 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 آن در کنترل رفتار اشخاص است، به جای آن‌که به دنبال تغییر و اصلاح رفتار آن‌ها باشد (Purshouse, Joe, 2019, P 324). عنصر اصلی در مطالعه کنترل اجتماعی درک جامعه‌شناختی است. فناوری عدالت را به محاسبات تقلیل می‌دهد، حال آن‌که عدالت ماهوی درک درد انسان‌هاست نه تحلیل داده‌ها (Gur-Arye, 2012, P. 194)؛ درکی مستلزم توجه به تمام تبعات کنترل، از جمله محدود نمودن حریم خصوصی افرادی 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 می‌دهد و منجر به تضعیف مسئولیت‌پذیری اخلاقی قضات و پلیس می‌گردد. زمانی که تصمیم‌ها بر پایه خروجی نرم افزارها باشد، استدلال اخلاقی جای خود را به محاسبات مکانیکی می‌دهد.

۳-۲. نادیده گرفتن حریم خصوصی و ایجاد جامعه نظارتی

استفاده گسترده از فناوری به عنوان ابزار اصلی کنترل اجتماعی در عصر حاضر، تبعات

اجتناب‌ناپذیری دارد، از جمله تحت کنترل و نظارت در آوردن همه افراد اجتماع، اعم از مجرم و غیرمجرم، که این به معنای 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» 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 غیرقانونی همراه است (نک: پرونده‌های قضایی در ایالت کالیفرنیا، ۲۰۲۲).

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). این در حالی است که قوانینی مانند GDPR در اروپا یا BIPA در ایلینویز 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 حالی است که جمع‌آوری داده‌های بیومتریک به صورت گسترده در

ایران استفاده می‌شود. نهادهایی به جمع‌آوری این داده‌ها در سطح کلان می‌پردازند، 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. 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 احتمال نشت داده‌ها (مانند نشت اطلاعات بیومتریک در پایگاه‌های احراز هویت موبایل در سال ۱۴۰۰) و تبعیض سیستماتیک دامن می‌زند.

فناوری‌های نظارتی با ایجاد شفافیت اطلاعاتی^۷ به بازتعریف مفهوم امنیت پرداخته‌اند 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 برون‌سپاری مدیریت داده‌های حساس به شرکت‌هایی مانند AI Clearview، کنترل نهادهای دولتی بر اطلاعات را تضعیف می‌کند و خطر سوءاستفاده تجاری یا امنیتی را افزایش می‌دهد (Fussell, 2021, P.54). برای مثال، شرکت AI Clearview داده‌های چهره را از شبکه‌های اجتماعی استخراج می‌کند و در اختیار پلیس قرار می‌دهد، که منجر به نقض حریم خصوصی در ابعاد جهانی می‌گردد (Hill, 2020, P.23). افزون بر آن، اخلال در عملکرد الگوریتم‌ها به دلیل خطاهای فنی، تحریم‌ها یا حملات سایبری، می‌تواند کل فرایند قضایی را متوقف کند. این مسئله در بحران‌هایی چون 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 بازتعریف مفاهیمی چون «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 حمایت نشده است، ولی می‌توان ذیل قوانین مختلف حریم خصوصی را بررسی کرد. 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 (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، به برخی از اصول ناظر بر حمایت از حریم داده‌های شخصی در محیط الکترونیکی توجه شده است، از جمله اصل تحصیل قانونی و مبتنی بر رضایت سوژه یا شخص موضوع گردآوری و پردازش (ماده ۵۸)؛ اصل تحصیل داده‌های مضیق و مرتبط (بند الف و ب ماده ۵۹)؛ اصل درستی و صحت داده‌های گردآوری شده (ماده ۵۹)؛ اصل دسترسی ذی‌نفع به داده پیام‌های مرتبط با خود (بند د ماده ۵۹) و اصل اصلاح و امحا (بند ۲ ماده ۵۹).

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 غیرقانونی افراد ملت اقدام می‌کنند، مجازات‌هایی 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 تقویت‌کننده 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 اقتدارگرایانه احتمالی فناوری‌های امنیتی را پنهان می‌کند. بنابراین بحث مهم درباره 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 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. هر چه 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 می‌گیرد 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 فرایندهای تبعیض‌آمیز طبقه‌بندی شهروندان را به گروه‌های پرخطر و کم‌خطر تسهیل می‌کنند؛ رویه‌ای که از طریق آن همه شهروندان تحت نظارت، با شاخص‌های خطر کدگذاری می‌شوند و افراد به «مسافران مورد اعتماد»^۸ یا کم‌خطر و «مهاجران مشکوک»^۹ یا پرخطر دسته‌بندی می‌شوند. این رویه در کشورهای توسعه‌یافته 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 (Degli, Esposti, 2010, P. 18). افزایش نظارت بر گروه‌های

8. Trusted travellers

9. Suspicious immigrants

خاصی به منظور پیشگیری از خطر ارتکاب یا تکرار جرم می‌تواند به اختلافات قومی، نژادی، اجتماعی و اقتصادی دامن زند و آن‌ها را بازتولید کند. برای مثال، نرم‌افزار آمریکایی سنجش خطر تکرار جرم، آمار جمعیت آفریقایی-آمریکایی را در دوره زمانی دو سال بعد از تحمل کیفر، دو برابر بیشتر از دیگران تخمین می‌زند.

افزون بر این، فناوری ناتوان از استدلال حقوقی یا علت‌شناسی است. رویکرد جرم‌شناختی علت‌شناسی که همچون سینماگر به دنبال گردآوری اطلاعات از مراحل مختلف زندگی مرتکب و چیدمان سکنس‌های زندگی شخصی و اجتماعی اوست (نجفی ابرنآبادی، ۱۳۹۸، ص ۲۴)، به‌گونه‌ای در مواد مختلف قانون مجازات و آیین دادرسی کیفری تجلی یافته است. ماده ۱۸ قانون مجازات اسلامی در همین راستا دادگاه را مکلف ساخته است 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 امکان‌پذیر 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 این رو تصمیم قضایی اساساً بر پایه ارزش‌های انسانی و ملاحظات اجتماعی مبتنی است، درحالی‌که رایانه از درک این ارزش‌ها عاجز است. عادی‌سازی 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 استفاده می‌شود. 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.

۳. جایگزینی کنشگران انسانی و تهدید مشروعیت نظام قضایی

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

۱-۳. حذف تدریجی نقش انسان

نمونه‌های عینی مانند جایگزینی قضات با هوش مصنوعی در صدور حکم جرائم تکرارشونده

(مثل تخلفات راهنمایی و رانندگی) یا استفاده از نرم افزارهای پیش‌بینی جرم به جای مددکاران اجتماعی، حذف عنصر انسانی از فرایندهای قضایی را تسریع می‌کند.

۲-۳. تغییر هدف از اصلاح به کنترل

تمرکز انحصاری بر «پیشگیری موقعیت مدار» (مثل دوربین‌های مداربسته) 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، ص ۲۱).

پیامدهای فوق حاکی از این است که اتکای انحصاری به فناوری کنترل اجتماعی جرم را به پروژه‌ای خودویرانگر تبدیل می‌کند که از بعد اخلاقی منجر به تقلیل انسان به داده‌های زیستی^{۱۰} 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 بازتعریف مفاهیمی مانند «عدالت»، «مسئولیت‌پذیری» و «حریم خصوصی» در چارچوب فناوریانه را اجتناب‌ناپذیر ساخته است. بنابراین فناوری ذاتاً شر نیست، اما اتکای انحصاری و بی‌ضابطه 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.

۳-۳. راهکارهای کاهش تبعات استفاده از فناوری‌های نظارتی

به منظور کاهش عواقب نامطلوب استفاده از فناوری در کنترل اجتماعی، در درجه نخست باید به این مسئله توجه کرد که آیا صرف هزینه در به‌کارگیری فناوری در شیوه‌های غیرقهری 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

10. Biological Data Points

الکترونیک و... نتیجه بهتری در پیشگیری و کنترل جرائم دارد یا صرف هزینه در ایجاد و نصب ابزارهای مبتنی بر فناوری و حذف هر چه 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، "هر جا که اراده‌ای وجود داشته باشد، راهی وجود دارد."^{۱۱} با امکانات کنترل‌گری 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 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 شوند و بی‌آن‌که متوجه شویم، دور از چشم جامعه و بدون خواست و اراده انسان، تبدیل به هدف نهایی گردند و یا حتی اهداف خود را به جامعه تحمیل کنند. از این رو باید همواره به ارزیابی اثربخشی فناوری‌های فناوری محور در اصلاحات سازمانی و اجتماعی ادامه دهیم و راهکارهایی برای کاهش پیامدهای ناخواسته این نوع از فناوری را بررسی کنیم تا مبادا فناوری جدید مترادف با کنترل افراد باشد (Wang, Xukang and Others, 2024, P. 44).

۳-۴. 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 فرایندهای شناسایی گرفته تا استفاده‌های شخصی و تسهیل دریافت خدمات. با وجود این، 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 به‌ویژه مفهوم

11. Wryly

12. Where there is a will, there is a way.

حریم خصوصی در عموم (حق یک فرد برای ناشناس ماندن در ملأ عام^{۱۳}) 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 (Wang, Xukang, 2024, 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 ناگزیر به کناره‌گیری از خدمات عمومی یا اجتماعی می‌شوند، 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 هویتی‌شان تجزیه و تحلیل شده است، بی‌اطلاع‌اند. 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.

فرایند کالاسازی هویت شخصی بر نگرانی‌های مربوط به سوءاستفاده‌های احتمالی و غیرانسانی از قدرت می‌افزاید (Wang, Xukang and Others, 2024, 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 ملأ عام را در اولویت قرار دهد. ایجاد تعادل مناسب میان ابزارهای نظارت الکترونیک و حمایت از حقوق بشر مستلزم اتخاذ رویکرد چندجانبه و تطبیقی حکومت است. سیاست‌گذاران و توسعه‌دهندگان فناوری‌های نظارتی باید در تعامل مداوم با اخلاق‌گرایان، حقوق‌دانان و جامعه مدنی باشند تا اطمینان یابند که این فناوری به‌گونه‌ای توسعه یافته و استفاده می‌شود که به حقوق فردی و ارزش‌های اجتماعی احترام می‌گذارد. این امر متضمن شفاف‌سازی 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 (Zuboff, S., 2019, P. 132).

13. An individual's right to anonymity in public spaces

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 تغییری فرهنگی به سوی ارزش‌گذاری بیشتر حریم خصوصی و استقلال فردی در دنیای دیجیتال است.

۳-۵. استفاده از فناوری با رعایت چارچوب‌های اخلاقی

این حق باید برای همه افراد جامعه به رسمیت شناخته شود که بدانند چه زمانی و چگونه اطلاعات حاصل از فناوری‌های نظارتی جمع‌آوری شده و استفاده می‌گردد. 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 شفاف‌سازی 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 امکان‌پذیر نباشد، باید اقدامات شفافی برای اطمینان از پاسخ‌گویی عمومی اتخاذ گردد. 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 غیرمجاز و بدون اجازه شهروندان در اختیار پلیس قرار بگیرد، باید سریعاً پاک شود و حق طرح دعوا در دادگاه به بزه‌دیدگان استفاده غیرمجاز از فناوری‌های نظارتی اعطا شده است. این بزه‌دیدگان می‌توانند خسارات وارده را از دادگاه مطالبه کنند و به ازای هر جرم، خسارت تعیین شده با توجه به میزان تبعات جرم از ۱۰۰۰ دلار تا ۱۰۰۰۰۰ دلار قابل پرداخت است (Adkins, 2007, P.451).^{۱۴}

اعلامیه جهانی حقوق بشر، میثاق بین‌المللی حقوق مدنی و سیاسی و سایر اسناد حقوق

۱۴. 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 باید برای هر نقض (violation) غیرعمدی 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.

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 مقررات‌گذاری 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 متناظر با تجربه زندگی افرادی که بیشترین تأثیر را از این فناوری‌ها متحمل شده‌اند، تدوین گشته است. این رویکرد مشترک باید صداها و منافع جوامع به حاشیه‌رانده شده و آسیب‌پذیر را که ممکن است با خطرات و آسیب‌های نامتناسب ناشی از استقرار فناوری‌های نظارتی مواجه شوند، در اولویت قرار دهد.

از این رو 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 راه‌حل‌هایی فنی نظیر طراحی الگوریتم‌های حفظ حریم خصوصی و انجام محاسبات چندجانبه 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 کنشگران دولتی و خصوصی متصدی طراحی، توسعه و به‌کارگیری هوش مصنوعی جنبه ارشادی دارد، بر ۵ اصل کلی متکی است: ۱. رعایت حقوق بنیادین؛ ۲. شفافیت؛ ۳. مدیریت هوش مصنوعی توسط استفاده‌کننده؛ ۴. عدم تبعیض؛ ۵. امنیت. لذا الگوریتم پیش‌بینی رفتار توسط فناوری هوش مصنوعی می‌بایست به‌گونه‌ای طراحی و اجرا شود که با این ۵ اصل سازگار باشد.

از این رو گونه‌های مختلف تبعیض میان افراد یا گروه‌ها باید کنار گذاشته شوند 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 باشند و به‌منظور حفظ

اعتماد افراد به نظام عدالت کیفری، در دسترس همگان قرار گیرند. همچنین استفاده‌کنندگان از فناوری، از جمله پلیس و قضات ضروری است 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 کنشگران عدالت کیفری قرار دهند. از این رو تمسک به فناوری در کنترل اجتماعی مفید است، مشروط به این‌که جایگاه و حدود مداخلات آن، در قانون تعریف و تعیین شده باشد و همچون 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 باید اختیار داشته باشند، زمانی که اوضاع و احوال خاص مؤثر در ارتکاب جرم و نیز شخصیت مرتکب (نیازپور، ۱۳۹۳، ص ۸۶) اقتضا می‌کند، پیش‌بینی‌های حاصل شده از فناوری را کنار بکنند و ملزم به تبعیت از نتایج نرم‌افزارها نباشند.

به نظر، 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 را باید در فقدان سازوکارهای نظارتی مستقل و ضعف در اجرای قانون جست. برای 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؛ جایی که نهادهای ناظر فاقد اختیارات کافی یا تخصص فنی اند و صرفاً مبادرت به مشروعیت سازی صوری می‌کنند. از سویی، اگرچه افزایش آگاهی متولیان سیاست جنایی ضروری است، اما این آموزش‌ها نباید به شعارهای اخلاقی تقلیل یابند. 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 به‌رغم آگاهی از محدودیت‌های فناوری به ابزارهای نظارتی متوسل شود. همچنین مشارکت شهروندان در نظارت بر سیستم‌ها (مانند پلتفرم‌های گزارش‌دهی، چنانچه بدم تضمین شفافیت و پاسخگویی باشد، به نظارت جمعی خودخواسته تبدیل می‌شود که خود تهدیدی برای دموکراسی است. پیشنهاد کلیدی، تبدیل حریم خصوصی از یک موضوع به گفت‌وگو اجتماعی با استفاده از ظرفیت‌های هنر و رسانه است.

۳-۶. ادغام مهندسی کنترل با رویکردهای اصلاحی

با سرمایه‌گذاری در طیف گسترده‌ای از فناوری‌های تغییر رفتار مجرم (اعم از سخت و نرم) مانند زندان‌های درمان‌محور، برنامه‌های 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 راه‌هایی برای اعمال فناوری برای اهداف اصلاحی و تغییر رفتار مجرمان به جای روش‌های قهرآمیز و کنترل‌گری، به شیوه‌هایی که منجر به اجتناب ارادی آن‌ها از رفتار مجرمانه باشد، یافت. به جای تمرکز صرف بر پیشگیری موقعیت‌محور (Situational Crime Prevention) که صرفاً با حمایت از آماج‌های جرم به دنبال پیشگیری از بزه‌دیدگی است (نجفی ابرندآبادی، ۱۳۹۴، ص ۳۷) می‌توان از فناوری برای توانمندسازی جامعه بهره برد. استفاده از راهبردهایی نظیر برنامه‌های آموزشی هوشمند برای جوانان مناطق جرم‌خیز یا استفاده از اپلیکیشن‌های گزارش‌دهی جرم با حفظ ناشناس بودن کاربران، شفاف‌سازی الگوریتم‌ها و مقابله با تبعیض، الزام به انتشار کدهای منبع (Open Source) و نرم‌افزارهای پیش‌بینی جرم، تشکیل کمیته‌های اخلاقی متشکل از حقوق‌دانان، جرم‌شناسان و جامعه مدنی برای بررسی سوگیری‌های الگوریتم، تقویت چارچوب‌های حقوقی می‌تواند در کاهش تبعات منفی استفاده از فناوری‌های نظارتی، بسیار کارآمد باشد، همان‌گونه که اتحادیه اروپا با تدوین قوانینی مانند مقررات عمومی حفاظت از داده‌ها (GDPR)، جمع‌آوری و استفاده از داده‌های بیومتریک را بدون رضایت صریح افراد ممنوع نمود (Lyon, D. 2018, P. 56). البته باید اذعان داشت که تمرکز صرف بر توسعه الگوریتم‌های اخلاق‌محور نظیر حریم خصوصی تفاضلی، ممکن است به توهم حل مسئله بینجامد. این فناوری‌ها اگرچه مفیدند، اما مسئله تبعیض ساختاری را ریشه‌کن نمی‌کنند، چراکه داده‌های آموزشی خود اغلب انعکاس‌دهنده نابرابری‌های موجود در جامعه‌اند. به علاوه، هوش

مصنوعی تبیین‌پذیر (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 بازطراحی فرایندهاست 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 روبه‌رویند: ۱. فقدان اراده سیاسی برای محدود کردن قدرت نهادهای امنیتی-قضایی؛ ۲. سلطه گفتمان فناوری محور بر گفتمان حقوق بشری در سیاست‌گذاری عمومی. ازاین‌رو تحقق این راهکارها مستلزم خیزش سه‌جانبه حقوق دانان اصلاح طلب به منظور تدوین قوانین پیشرو، جامعه مدنی آگاه برای مطالبه‌گری، و فناوریان مسئولیت‌پذیر برای طراحی اخلاق محور است. بدون این ائتلاف، فناوری نظارتی نه تنها تهدیدات موجود را کاهش نخواهد داد، بلکه خود به ابزار جدیدی برای بازتولید نابرابری بدل خواهد شد.

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 حاضرند. 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 پیشنهادهای 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 حقوق دانان، 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 قضاوت 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 موقعیت‌مدار.

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 فردی‌سازی 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 گفت‌وگو عمومی درباره «مبادله امنیت - حریم خصوصی» از طریق کمپین‌های رسانه‌ای (کاهش انفعال شهروندان).

یافته‌های این پژوهش حاکی از آن است که فناوری نظارتی نه دشمن جامعه است و نه معجزه‌گر 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 فرایندهای قضایی. لذا تنها با اتخاذ رویکردی چندرشته‌ای حقوقی، فنی، اخلاقی و اجتماعی می‌توان از تبدیل فناوری به ابزار سرکوب جلوگیری کرد و آن را به خدمت اهداف اصیل عدالت کیفری یعنی تضمین دادرسی عادلانه و حفظ حریم خصوصی درآورد. بنابراین، آینده مطلوب نه در انفعال در مقابل فناوری، بلکه در طراحی فعالانه چارچوب‌های حکمرانی مسئولانه آن است.

د. پیشنهاد کلیدی برای پژوهش‌های آتی

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



فهرست منابع

۱. ابراهیمی، شهرام. (۱۴۰۱ش). پیشگیری از تکرار جرم از طریق هوش مصنوعی؛ مقتضیات و محدودیت‌ها. <https://doi.org/10.30513/cld.2023.4345.1701>. ۳۳-۵۴، (۲۳)۱۲.
۲. انصاری، باقر. (۱۳۸۳ش). حریم خصوصی و حمایت از آن در حقوق اسلام تطبیقی و ایران. **مجله دانشکده حقوق و علوم سیاسی**، ۶۶ (پیاپی ۵۲۰)، ۵۳-۱.
۳. بامپاسیکا، افیچیا؛ صادقی، سالار. (۱۴۰۲ش). هوش مصنوعی به‌عنوان دلیل در محاکم کیفری. **تمدن حقوقی**، ۶ (۱۸)، ۲۵-۳۸. <https://doi.org/10.22034/L.2024.415210.1392>
۴. پورصادقی، محمدصادق. (۱۴۰۰ش). روش‌های کشف و اثبات جرائم سایبری، کنفرانس بین‌المللی پژوهش در علوم و مهندسی.
۵. سلیمی، میررضا؛ گلدوست جویباری، رجب. (۱۴۰۱ش). دروغ‌سنجی و حقوق متهم. **مجله حقوقی دادگستری**، ۸۶ (۱۲۰)، ۲۰۱-۲۲۴. <https://doi.org/10.22106/ijl.2022.542062.4506>
۶. شکری، رضا. (۱۳۹۸ش). حریم خصوصی ارتباطات در فضای الکترونیکی از منظر حقوق کیفری ایران و انگلستان. **فصلنامه حقوق و فناوری اطلاعات**، ۱ (۱)، ۳۲-۶۵.
۷. فلاحتی، احمد؛ بزرگمهر، علی‌عباس. (۱۳۹۹ش). بایسته‌های نوین علمی بازجویی و تحقیق در قلمرو ادله اثبات حقیقت. **فصلنامه علمی مطالعات حقوق بشر اسلامی**، ۹ (۱۹)، ۱۵۳-۱۸۸. <https://doi.org/20.1001.1.23225637.1399.9.2.8.3>
۸. کریمی‌نیا، محمد مهدی؛ سلمانی، ناهید؛ انصاری‌مقدم، مجتبی. (۱۴۰۰ش). نقش صنعت و فناوری رسانه در پیشگیری از وقوع جرم، **دستاورد های نوین در مطالعات علوم انسانی**، ۴ (۳۸)، ۱۹۲-۲۰۵.
۹. مسعودی، امیرعلی. (۱۴۰۰ش). همگرایی تناقض‌نمای نظارت الکترونیک در برخورد تکنوکراسی و حریم خصوصی. **فصلنامه رهپویه ارتباطات و فرهنگ**، ۱ (۲)، ۷-۲۰. <https://doi.org/10.22034/rcc.2022.251311>
۱۰. نجفی ابرندآبادی، علی‌حسین. (۱۳۹۴ش). به‌سوی تعریف یک سیاست ملی پیشگیری از بزهکاری، دیپاچه در: براندون سی و دیوید پی فارینگتون. **دانشنامه پیشگیری از جرم آکسفورد**. تهران: میزان.
۱۱. نجفی ابرندآبادی، علی‌حسین. (۱۳۹۶ش). پیشگیری عادلانه از جرم در: **علوم جنایی**. مجموعه مقالات در تجلیل از دکتر محمد آشوری. تهران: سمت.
۱۲. نجفی ابرندآبادی، علی‌حسین. (۱۳۹۸ش). پیوند حقوق کیفری و جرم‌شناسی. در: **افق‌های نوین حقوق کیفری**. تهران: میزان.
۱۳. نجفی ابرندآبادی، علی‌حسین. (۱۳۹۵ش). کیفرشناسی نو - جرم‌شناسی نو، درآمدی بر سیاست جنایی مدیریتی خطرمدار. در: **تازه‌های علوم جنایی** (مجموعه مقالات)، (زیر نظر علی‌حسین نجفی ابرندآبادی). تهران: میزان.

۱۴. نجفی ابرندآبادی، علی حسین. (۱۴۰۰ش). نقش ریاضیات در آغاز و گسترش مطالعات علمی جرم. دیپاچه در دایرةالمعارف ریاضیات و علوم جنایی، (به کوشش مریم عباچی). تهران: میزان.
۱۵. نجفی ابرندآبادی، علی حسین؛ هاشمیگی، حمید. (۱۴۰۳ش). *دانشنامه جرم‌شناسی*. تهران: گنج دانش.
۱۶. نیازپور، امیرحسین. (۱۴۰۲ش). *پیشگیری از جرم*. تهران: دادگستر.
۱۷. نیازپور، امیرحسین. (۱۳۹۳ش). اساسی‌سازی حقوق پیشگیری از جرم در ایران، *فصلنامه پژوهش حقوق کیفری*، ۲(۶)، ۹۱-۱۱۳.
۱۸. هالوی، سید مهدی؛ حاجی‌زاده، فاطمه. (۱۴۰۰ش). چالش‌های ادله الکترونیکی در فرایند دادرسی. *مطالعات حقوق کیفری و جرم‌شناسی*، ۶(۱)، ۱۴۲-۱۱۱. DOI: 10.22054/JCI.2021.59800.1281
19. 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.
20. 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*. Available at <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>
21. Botsman, R. (2017, October 21). *Big Data Meets Big Brother as China Moves to Rate Its Citizens*. Available at <https://www.wired.com/story/chinese-government-social-credit-score-privacy-invasion/>
22. Byrne, James & Marx, Gary, (2011). Technological Innovations in Crime Prevention and Policing, A Review of the Research on Implementation and Impact. *Journal of Police Studies*, 3(20), 17-40. <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=268048>
23. Cheng, Lijiao, (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory, 19th Americas Conference on Information Systems (AMCIS 2013 , 160-186) DOI: 10.13140/RG.2.2.22466.58561
24. Clarke, R. V. (1997). *Situational Crime Prevention: Successful Case Studies* (2nd ed.). Routledge.
25. Coleman, Roy and McCahill, (2010) *"Surveillance and Crime, Key Approaches to Criminology"*, 212- 234. ISBN-10: 1847870310 , ISBN-13: 978-1847870318
26. Creemers, R. (2018). *China's Social Credit System: An Evolving Practice of Control*. SSRN Electronic Journal. <http://dx.doi.org/10.2139/ssrn.3175792>

27. Degli Esposti, Sara, (2010). Public assessment of new security technologies: Beyond the trade-off between privacy and security, *Public Understanding of Science*, Volume 23, Issue, 1 DOI: [10.1177/0963662513509760](https://doi.org/10.1177/0963662513509760)
28. Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press. ISBN:14798355880
29. Fussell, S. (2021, March 18). How Clearview AI Became a Tool of Law Enforcement—and Activists. *The Atlantic*. <https://www.theatlantic.com>
30. Garner, Bryan A, (2004). *Black Law Dictionary*. Eighth Edition, Thomson West. USA.
31. Gary T Marx, (2015). Technology and Social Control, *International Encyclopedia of the Social & Behavioral Sciences*, 1-7 <https://doi.org/10.1016/B978-0-08-097086-8.64113-9>
32. Grabosky, Peter, (1998). *Technology & Crime Control, Australian Institute of Criminology*. (ISBN): 0 642 24110 9 <https://www.aic.gov.au/sites/default/files/2020-05/ti78.pdf>
33. Gur-Arye, Miriam, (2012). Human Dignity of “Offenders”: A Limitation on Substantive Criminal Law, *Crim Law and Philosophy*, Volum (6), issue (2), 191-207. <https://doi.org/10.1007/s11572-011-9126-9>
34. Hill, K. (2020). The Secretive Company That Might End Privacy as We Know It. *The New York Times*. <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>
35. James M. Byrne, (2008). *Surveillance and Governance: Crime Control and Beyond Sociology of Crime*, Law, Emerald Group Publishing Limited Volume 10. [https://doi.org/10.1016/S1521-6136\(07\)00212-6](https://doi.org/10.1016/S1521-6136(07)00212-6)
36. Martinez-lucena, Jorge, (2023). *The Issue of Social Control in Late Modernity: Alienation and Narrativity, scientia et fides*. <https://doi.org/10.12775/SetF.2023.018>
37. 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). 382-407. <https://doi.org/10.1057/s41284-021-00270-w>
38. Laufs, Julina, (2022), *Crime Prevention and Detection Technologies in Smart Cities: Opportunities and Challenges*, University College London. <https://library.ucl.ac.uk/>
39. Levi, Michael & Wall, David S, (2004). Technologies, Security, and Privacy in the Post-9/11 European Information Society, *Journal of Law and Society*, Volum 31 (2), 194-220. DOI: [10.1111/j.1467-6478.2004.00287.x](https://doi.org/10.1111/j.1467-6478.2004.00287.x)

40. 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*.
41. Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press. ISBN: 5-216-5095-1
42. Mohapatra, Seema, (2016). Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation, *American Journal of Law & Medicine*, Vol. 43: 1017 <https://doi.org/10.1177/0098858817702793>
43. Purshouse, Joe, (2019). Privacy & Campbell, Liz, Crime Control and Police use of Automated Facial Recognition Technology, *Criminal Law Review*, 188-204. DOI: [10.1350/1740-5580-163.3.18](https://doi.org/10.1350/1740-5580-163.3.18)
44. Rudin, C., Wang, C., & Coker, B. (2020). The Age of Secrecy and Unfairness in Recidivism Prediction. *Harvard Data Science Review*, 2(1). <https://doi.org/10.1162/99608f92.6ed64b30>
45. Thomas G. Blomberg and Carter Hay, (2007). *Beyond the Myth of an 'Evil System': A Re-examination of the Control Model*, Willan Publishing. <https://doi.org/10.4324>
46. van Brake, Rosamunde, & De Hert, (2011). Paul, Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies, *Utrecht Law Review*, nr. 20, 163-192. <https://doi.org/10.18352/ulr.162>
47. Wang, Xukang and Others, (2024). "Beyond surveillance: privacy, ethics and regulations in face recognition technology, *Policy and Practice Reviews*.
48. Westin, Alan, (1967). *Privacy and Freedom*, Atheneum Publishers. ISBN-13: 978-1566431193. <https://www.worldcat.org/title/225958>
49. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. *Public Affairs*. ISBN-13: 978-1610395694 doi: [10.4324/9781912454057](https://doi.org/10.4324/9781912454057)