DOI: 10.22034/mral.2024.2024435.1591

تاریخ ارسال: ۱۴۰۲/۱۲/۱۶ | تاریخ پذیرش: ۱۴۰۲/۱۲/۱۹

بانک‌های اطلاعاتی پلیس؛ توازن حق بر امنیت و حریم خصوصی اطلاعات

محسن صوفی[۱] و محسن رضایی[۲]

چکیده

پلیس به عنوان نهادی کلیدی در تضمین نظم و امنیت عمومی به طور گسترده با داده‌های شخصی شهروندان در تعامل است. این داده‌ها که در قالب بانک‌های اطلاعاتی تجمیع می‌شوند، افزون بر تسهیل خدمات و ارتقای کشف جرم، چالش‌هایی را در حوزه حفظ حریم خصوصی ایجاد می‌کنند. با توجه به نقش روزافزون اطلاعات به مثابه ابزار قدرت، هدف این پژوهش، بررسی سازوکارهای حقوقی و اجراییِ دست‌یابی به توازن میان منافع امنیت عمومی و صیانت از حریم خصوصی افراد در بهره‌برداری از داده‌ها در بانک‌های اطلاعاتی پلیس است.

این پژوهش به روش توصیفی و تحلیلی و با بهره‌گیری از منابع کتاب‌خانه‌ای انجام شده است و با رویکرد تطبیقی، نسبت میان منافع امنیتی و حقوق بنیادین شهروندان را در فرآیند تجمیع و بهره‌برداری از داده‌های پلیس بررسی می‌کند. داده‌های تجمیع‌شده در شناسایی الگوهای ارتکاب جرم، تحلیل رفتارهای مجرمانه و در پیش گرفتن تدبیرهای پیش‌گیرانه نقش محوری دارند. با این حال، خلأهای قانونی در زمینه گردآوری، نگه‌داری و بهره‌برداری از داده‌های شخصی به همراه نبود سازوکارهای نظارتی و پاسخ‌گویی می‌تواند زمینه‌ساز نقض حقوق شهروندی، کاهش اعتماد عمومی و مداخلات بی‌ضابطه در حریم خصوصی افراد گردد. هم‌چنین در غیاب نظام پاسخ‌گویی شفاف، امکان سوء استفاده از اطلاعات شخصی یا افشای غیر مجاز داده‌ها افزایش می‌یابد.

تأمین امنیت از سوی پلیس نباید به بهای نقض آزادی‌های بنیادین شهروندان تمام شود. از این رو، لازم است رویکردهای حقوقی و اجرایی در خصوص تجمیع اطلاعات و بهره‌برداری از آن‌ها بازنگری

۱. استادیار گروه حقوق، دانشکده علوم و فنون انتظامی، دانشگاه افسری و تربیت پلیس امام حسن مجتبی (ع)، تهران، ایران، (نویسنده مسئول)، M.sufi61@gmail.com.

۲. استادیار گروه حقوق، دانشکده علوم و فنون انتظامی، دانشگاه افسری و تربیت پلیس امام حسن مجتبی (ع)، تهران، ایران، mohsenrezaee3492@gmail.com،

شود. طراحی چارچوب‌های قانونی شفاف، پیش‌بینی حمایت‌های کیفری در برابر بهره‌برداری غیر مجاز، آگاه‌سازی ذی‌نفعان، تقویت نظارت نهادی و ایجاد سازوکارهای جبران خسارت از جمله الزامات اساسی برای ایجاد توازن میان امنیت و آزادی‌های فردی در نظام حقوقی مرتبط با بانک‌های اطلاعاتی پلیس است.

واژگان کلیدی: امنیت، داده‌های شخصی، بانک اطلاعاتی، پلیس، حریم خصوصی اطلاعات.

مقدمه

در دهه‌های اخیر، تحولات گسترده در عرصه فناوری اطلاعات، ابزارهای نظارت هوشمند و بسترهای ارتباطی دیجیتال، الگوهای سنتی کنش‌های انتظامی را دگرگون ساخته‌اند. پلیس به عنوان یکی از بازیگران اصلی در حفظ نظم عمومی ناگزیر است در برابر پیچیدگی‌های روزافزون جرایم نوظهور به ویژه جرایم سایبری و فرامکانی، از شیوه‌های نوین بهره‌گیری از داده‌ها استفاده کند. شکل‌گیری بانک‌های اطلاعاتی گسترده و تجمیع داده‌های شخصی شهروندان در قالب سامانه‌های هوشمند، از جمله ابزارهایی است که به پلیس امکان می‌دهد فرآیند شناسایی تهدیدها، پیش‌گیری از وقوع جرم و ارتقای اثربخشی عملیات خود را هدفمند و کارآمدتر دنبال کند.

در همین راستا، در سطح بین‌المللی، مطالعات ارزنده‌ای صورت گرفته است که به ابعاد حقوقی، اخلاقی و اجتماعی این تحولات پرداخته‌اند. از جمله، دانیل جی. سولوف[1] در کتاب درک حریم خصوصی (۲۰۰۸)[2] تلاش کرده است ماهیت پیچیده حریم خصوصی را در فضای دیجیتال تبیین کند و نسبت به تهدیدهای پنهان نظارت‌های دولتی هشدار دهد. هم‌چنین شوشانا زوباف[3] در اثر مهم خود، عصر سرمایه‌داری نظارتی (۲۰۱۹)[4] نشان می‌دهد چگونه بهره‌برداری بی‌ضابطه از داده‌ها توسط نهادهای دولتی و تجاری، مرزهای آزادی فردی را به چالش می‌کشد. در همین زمینه، اندرو گاتام فرگوسن[5] در کتاب ظهور پلیس داده‌محور: نظارت، نژاد و آینده اجرای قانون (۲۰۱۷)،[6] رویکردهای تحلیلی و انتقادی به کارگیری کلان‌داده‌ها در سیستم‌های پلیسی را بررسی کرده و به چالش‌های تبعیض‌آمیز و نفی پاسخ‌گویی پرداخته است.

در فضای علمی داخلی نیز مطالعات محدود، اما مهمی انجام شده‌اند. برای نمونه، محمدی (۱۳۹۸) در مقاله «چالش‌های حقوقی بهره‌برداری پلیس از اطلاعات شخصی در ایران»، ضعف چارچوب‌های

1. Daniel J. Solove
2. Understanding Privacy
3.. Shoshana Zuboff
4. The Age of Surveillance Capitalism
5.. Andrew Guthrie Ferguson
6. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement

قانونی و نظارتی را از منظر حقوق شهروندی بررسی می‌کند. هم‌چنین حسن‌زاده و کریمی (۱۴۰۰) در پژوهش «بانک‌های اطلاعاتی پلیس و حق بر حریم خصوصی در نظام کیفری ایران» با تمرکز بر نقش این سامانه‌ها در پیش‌گیری از جرم، به الزامات قانونی و پی‌آمدهای استفاده نادرست از اطلاعات پرداخته‌اند. افزون بر این، شریفی (۱۳۹۷) در مقاله «سیاست کیفری و تعارض میان امنیت و آزادی‌های فردی»، نبود تعادل موجود میان اهداف امنیتی و صیانت از حریم خصوصی را از منظر سیاست‌گذاری کیفری تحلیل کرده است. رحیمی (۱۴۰۱) در «حقوق کیفری داده‌ها و پاسخ‌گویی نهادی در عصر دیجیتال»، بر ضرورت تدوین سیاست‌هایی شفاف در بهره‌برداری از داده‌های شخصی تأکید کرده است. این پیشینه‌ها در ادبیات جهانی و مطالعات بومی نشان‌دهنده این واقعیتند که بهره‌برداری پلیسی از داده‌ها بدون پشتوانه شفاف قانونی و نظارت مؤثر می‌تواند مخاطرات جدّی برای حقوق بنیادین شهروندان به دنبال داشته باشد.

سؤال اصلی پژوهش حاضر این است که چگونه می‌توان بهره‌برداری پلیس از بانک‌های اطلاعاتی و داده‌های شخصی شهروندان را در چارچوبی حقوقی و اخلاقی با رعایت توازن میان حق بر امنیت و حریم خصوصی تنظیم کرد؟ فرضیه پژوهش بر این استوار است که در صورت وجود چارچوب‌های شفاف قانونی، سازوکارهای نظارتی مؤثر و الزام به پاسخ‌گویی نهادی می‌توان بهره‌برداری پلیس از داده‌ها را به‌گونه‌ای سامان داد که هم امنیت عمومی تأمین شود و هم از تعرض به حریم خصوصی شهروندان پیش‌گیری گردد.

پژوهش حاضر با تمرکز بر بانک‌های اطلاعاتی پلیس در پی تبیین الزامات قانونی، اخلاقی و حقوق بشری بهره‌برداری از داده‌های شخصی شهروندان است و می‌کوشد با نگاهی تحلیلی و تطبیقی، ابعاد مختلف این مداخلات را واکاوی کند و راهکارهایی برای تأمین توازن میان حق بر امنیت و صیانت از حریم خصوصی اطلاعات ارائه دهد. این توازن نه فقط یک ضرورت حقوقی، بلکه یکی از پیش‌شرط‌های اساسی برای تحقق امنیت پایدار، مشروعیت نهادی و تضمین حقوق بنیادین در عصر داده‌محور امروز است.

گفتار اول. الزامات حقوق اداری و حقوق بشری در بهره‌برداری پلیس از بانک‌های اطلاعاتی

با گسترش فناوری‌های اطلاعاتی و توسعه نظام‌های داده‌محور، بهره‌برداری از بانک‌های اطلاعاتی به یکی از ابزارهای کلیدی نهادهای امنیتی و انتظامی از جمله پلیس در مدیریت نظم اجتماعی و پیش‌گیری از جرم تبدیل شده است. با این حال، دسترسی به اطلاعات شخصی شهروندان، چالشی عمیق در تقابل با حقوق بنیادین فردی و اصول حاکم بر اداره عمومی پدید می‌آورد. در این میان، بهره‌گیری مشروع از داده‌ها باید در چارچوبی روشن مبتنی بر قوانین داخلی، اصول حقوق اداری و الزامات حقوق بشری صورت گیرد.

نظام حقوقی جمهوری اسلامی ایران هم در قالب اصول قانون اساسی و هم از طریق قوانین عادی، ضوابطی برای تحدید اختیارات اجرایی در بهره‌برداری از داده‌های خصوصی پیش‌بینی کرده است. هم‌چنین تعهدات بین‌المللی دولت ایران در زمینه حقوق بشر از جمله مفاد میثاق بین‌المللی حقوق مدنی و سیاسی، مداخلات در حریم خصوصی را صرفاً در صورت وجود ضرورت، تناسب و قانون‌مندی مجاز می‌داند. در این راستا، گفتار حاضر در دو بند مجزا، ابتدا به تحلیل چارچوب‌های حقوق اداری در نظام جمهوری اسلامی ایران و سپس به بررسی ملاحظات حقوق بشری با تأکید بر تعهدات بین‌المللی و اصول قانون اساسی پرداخته است.

بند اول. الزامات حقوق اداری در مدیریت داده‌های توسط پلیس

در نظام حقوقی ایران، نهادهای اجرایی از جمله پلیس در بهره‌برداری از بانک‌های اطلاعاتی، ملزم به رعایت اصول حقوق اداری هستند. این اصول در قانون اساسی، قوانین عادی و دکترین حقوق عمومی ریشه دارند. مهم‌ترین اصل حاکم، اصل قانونی بودن است که در مواد متعدد قانون اساسی از جمله اصل ۲۵، ۲۲ و ۱۷۳ منعکس شده است.

اصل ۲۲ قانون اساسی، حمایت از حریم خصوصی و حیثیت افراد را تضمین می‌کند و تعرض به آن را صرفاً در صورت وجود نص قانونی موجه مجاز می‌داند. در اصل ۲۵ نیز با صراحت به ممنوعیت شنود، بازرسی و نظارت بر مکاتبات و مکالمات بدون حکم قانونی اشاره دارد. هم‌چنین اصل ۱۷۳ با

پیش‌بینی صلاحیت دیوان عدالت اداری برای نظارت بر نهادهای اجرایی از جمله نیروی انتظامی، امکان کنترل مشروعیت اقدامات اداری را فراهم می‌سازد.

در حوزه قوانین عادی نیز می‌توان به ماده ۱۰ قانون آیین دادرسی کیفری (۱۳۹۲) اشاره کرد که جمع‌آوری داده‌ها را مشروط به رعایت حقوق متهمان، ضرورت قضایی و دریافت مجوزهای قانونی می‌داند. هم‌چنین قانون جرایم رایانه‌ای مصوب ۱۳۸۸ در مواد ۱، و ۱۳، پردازش داده‌های شخصی را به مجوز قانونی و رعایت اصول حقوق فردی وابسته کرده است.

از منظر ساختار نظارتی، نهادهای داخلی هم‌چون واحد حفاظت اطلاعات، حراست، سازمان بازرسی کل کشور و دیوان عدالت اداری در شمار ابزارهای کنترل قانونی بر عملکرد پلیس در استفاده از اطلاعات شخصی قرار دارند. نبود نظارت مؤثر، زمینه را برای تخطی از حدود صلاحیت، سلب اعتماد عمومی و تضییع حقوق شهروندی فراهم می‌سازد.[1]

بند دوم. الزامات حقوق بشری در مدیریت داده‌های توسط پلیس

حفظ حریم خصوصی، یکی از بنیادی‌ترین حقوق بشری است که در اسناد داخلی و بین‌المللی شناسایی شده است. ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (ICCPR)که ایران نیز به آن ملحق شده، به صراحت، هرگونه مداخله خودسرانه یا غیر قانونی در حریم خصوصی، مکاتبات و حیثیت افراد را ممنوع دانسته است. بر اساس تفسیر عمومی شماره ۱۶ کمیته حقوق بشر سازمان ملل متحد (۱۹۸۸)، مشروعیت، ضرورت و تناسب، سه رکن اساسی برای مداخله در حریم خصوصی‌اند.

در حقوق داخلی نیز اصل ۲۲ و ۲۵ قانون اساسی ایران ناظر بر همین اصولند. به علاوه، منشور حقوق شهروندی جمهوری اسلامی ایران (۱۳۹۵) در مواد ۳۷ تا ۴۰، بر لزوم حفاظت از داده‌های شخصی و الزام دولت به شفاف‌سازی در این زمینه تأکید کرده است.

در حقوق تطبیقی نیز تجربه‌های کشورهای عضو اتحادیه اروپا قابل توجه است. دادگاه حقوق بشر اروپا در رأی(S. and Marper v. the United Kingdom 2008) تصریح می‌کند که نگه‌داری اطلاعات

---

۱. محمدی، زهرا، **نظام نظارت اداری در ایران**، تهران: پژوهشکده قوه قضاییه، ۱۳۹۸.

زیستی شهروندان بدون ضرورت، نقض ماده ۸ کنوانسیون اروپایی حقوق بشر است. هم‌چنین (General Data Protection Regulation (GDPR) اتحادیه اروپا، الگویی شفاف و دقیق از نحوه دسترسی نهادهای عمومی به داده‌های شهروندان ارائه می‌دهد که اصولی چون رضایت آگاهانه، دسترسی شهروند و حق فراموش شدن در آن لحاظ شده است.[1]

گفتار دوم. حریم خصوصی و چالش‌های امنیت‌گرایی

چالش‌های پیش‌رو در زمینه پایش و تحلیل اطلاعات فردی و تجمیع داده‌ها در نهادهای دولتی، سازمان‌های اجرایی و بخش خصوصی، در سال‌های اخیر به یکی از محورهای اساسی برخی پژوهش‌ها بدل شده است. در این پژوهش‌ها، بارها به این پرسش پاسخ داده شده است که چرا باید به حریم خصوصی افراد احترام گذاشت؛ پاسخی که در صدر آن، حفظ کرامت ذاتی انسان‌ها قرار دارد. همان کرامتی که با موجودیت فردی گره خورده است و در صورت نقض حریم خصوصی به شدت آسیب‌پذیر می‌شود.

در تبیین این موضوع که چرا کرامت انسان امری ذاتی تلقی می‌شود، دیدگاه‌های متعددی ارائه شده است؛ از جمله نظریه حقوق طبیعی، نظریه اصالت فرد و نظریه خودمختاری اخلاقی. در رویکردهای حقوقی و جامعه‌شناختی، مفهوم حریم خصوصی بر بنیاد ارزش‌گذاری بر آزادی‌های فردی و آرامش روانی اشخاص بنا شده است و رعایت خلوت و حریم شخصی افراد، یکی از ارکان این مفهوم به شمار می‌آید.

نظارت مستمر بر رفتار فرد یا دسترسی غیر مجاز به اطلاعات شخصی او بدون رضایت و آگاهی‌اش، نه تنها آزادی فردی را مخدوش می‌سازد، بلکه منجر به اضطراب روانی و سلب آسایش وی می‌شود. در یک جامعه آزاد، تصمیم‌گیری در مورد افشای اطلاعات خصوصی اشخاص ـ با در نظر گرفتن استثنائات محدود و منافع عمومی ـ باید در اختیار خود فرد باشد. از همین رو، حق تعیین زمان، شیوه و میزان افشای داده‌های شخصی، از مصادیق اصلی حریم خصوصی به شمار می‌رود.[2]

1..Zuboff, Shoshana, The Age of Surveillance Capitalism, PublicAffairs, 2019.

۲. یعقوبی، محدثه و همکاران، «**تبیین چالش‌های قانون دسترسی آزاد به اطلاعات از منظر اساتید ارتباطات و اصحاب رسانه**»، فصل‌نامه مطالعات رسانه‌های نوین، سال ششم، شماره ۲۱، ۱۳۹۹.

با این حال، برخی رویکردها. به ویژه نگرش‌های امنیت‌گرا. چالشی جدّی برای حریم خصوصی ایجاد کرده‌اند. در این دیدگاه‌ها، امنیت به عنوان یکی از نیازهای بنیادین بشر، گاه بر دیگر حقوق مقدّم دانسته می‌شود و این امر به دولت اجازه می‌دهد تا در صورت تهدید نظم اجتماعی، به واسطه نیروهای امنیتی و پلیس به مداخله بپردازد. این دیدگاه اگرچه بر «نفع عمومی» تأکید دارد، اما می‌تواند به اضطراب اجتماعی و ناامنی روانی دامن بزند.[1]

نمونه بارز این رویکرد را می‌توان در ایالات متحده امریکا پس از حملات ۱۱ سپتامبر مشاهده کرد؛ جایی که تنها ۴۵ روز بعد، کنگره آمریکا با تصویب قانون «میهن‌پرستی»، محدودیت‌هایی گسترده را بر آزادی‌های مدنی وارد ساخت.[2] در قالب این قانون، اختیارات وسیعی به نهادهای امنیتی داده شد تا از جمله وارد حریم خصوصی افراد شوند، مکالمات را شنود و ایمیل‌ها را رصد کنند، بدون حکم قضایی به تفتیش دست بزنند، مانع تجمعات مسالمت‌آمیز شوند، افراد مظنون را بدون محدودیت بازداشت کنند، حق دسترسی به وکیل را از برخی متهمان سلب کنند و رسیدگی به پرونده‌ها را به دادگاه‌های نظامی بسپارند.[3]

نقد دیگر وارد بر رویکرد امنیت‌محور در مبارزه با تروریسم، تقدم دادن مداوم امنیت بر دیگر حقوق بنیادین است؛ در حالی که امنیت نه در تئوری و نه در عمل، مطلق نیست و هیچ جامعه‌ای نمی‌تواند به طور کامل از تهدید خشونت‌طلبان در امان بماند. از این رو، ایجاد تعادل میان آزادی و امنیت ضرورتی انکارناپذیر دارد.[4]

در رژیم‌های اقتدارگرا نیز تمایل به کسب قدرت نامحدود، با نفی کامل حریم خصوصی شهروندان همراه است. در چنین نظام‌هایی، نظارت همه‌جانبه بر زندگی افراد، شرط تحقق قدرت مطلق تلقی می‌شود. حتی در جوامع دموکراتیک نیز در شرایط بحرانی، احتمال تقدم امنیت بر حریم خصوصی

---

۱. . یورگنسون، رایکه فرانک، **حقوق بشر در جامعه جهانی اطلاعات**، ترجمه: بهرام مستقیمی، قم: آیین احمد، ۱۳۸۶.

2..**USA PATRIOT ACT**: Uniting and Strengthing America by Providing Appropriate Tools to Intercept and Obstruct terrorism.

۳. . موذن‌زادگان، حسن‌علی، «**تضمینات حقوق دفاعی متهمان و امر بازجویی در مرحله تحقیقات مقدماتی**»، پژوهش حقوق و سیاست، شماره ۲۸، ۱۳۸۹.

۴. بیابانی، غلام‌حسین، **اطلاعات جنایی**، تهران: کارآگاه، پلیس آگاهی ناجا، ۱۴۰۱.

وجود دارد، به گونه‌ای که در بسیاری از موارد، امنیت به عنوان اصل مقدم بر حقوق شهروندی لحاظ می‌شود.[۱] در این چارچوب، موضوع کشف جرم و پیش‌گیری از آن به محل تلاقی امنیت و دیگر منافع عمومی بدل می‌شود. هرگاه اولویت مطلق به امنیت داده شود، امکان دارد حقوق بنیادین اشخاص به حاشیه رانده شود.

در سیاست جنایی نیز شاهد رشد فزاینده گرایش به مدیریت خطر با تکیه بر داده‌پردازی آماری و فناوری‌های نوین هستیم؛ رویکردی که به جای پرداختن به عوامل واقعی و اجتماعی جرم‌زا. مانند نابرابری یا فقر. تمرکز خود را بر دسته‌بندی گروه‌های پرخطر آماری می‌گذارد. نتیجه این نگاه، تلاش برای خنثی‌سازی، حذف یا طرد این گروه‌ها از جامعه است.

در چنین فضایی، فرهنگ کنترل چیره می‌شود و سرمایه‌گذاری در سیاست‌های سرکوبگر و واکنشی افزایش می‌یابد؛ در حالی که صلاحیت و کارکرد متخصصان علوم اجتماعی در شناسایی علل جرم‌زا کم‌رنگ می‌شود. سیاست‌های پیش‌گیری به جای تقویت اقدامات اجتماعی، به سمت امنیتی‌سازی فضاهای عمومی با حضور پررنگ پلیس و رویکردهای پیش‌گیری وضعی هدایت شده‌اند. گارلند بر این باور است که این جهت‌گیری به جای اصلاحات اجتماعی، تمرکز خود را بر مسئولیت‌پذیری فردی، افزایش کنترل اجتماعی و پاسخ‌های کیفری سرکوبگر گذاشته است. در نتیجه، نقش پیش‌گیری اجتماعی کاهش و پاسخ‌ها بیش‌تر به سمت واکنش‌های کیفری بازدارنده و قهری سوق یافته‌اند.

گفتار سوم. رویکردهای پیش‌گیرانه پلیس در بهره‌گیری از اطلاعات و تجمیع آن

در دهه‌های اخیر، یکی از محورهای اصلی سیاست‌های پیش‌گیرانه پلیس در بسیاری از کشورها، تمرکز بر کاهش گم‌نامی و شناسایی به‌موقع تهدیدات بالقوه از طریق گردآوری، تجزیه و تحلیل داده‌های اطلاعاتی گسترده بوده است. این رویکرد نه تنها به شناسایی افراد مظنون در فرآیندهای پلیسی کمک می‌کند، بلکه امکان پیش‌گیری هدفمند از جرایم در مراحل اولیه را نیز فراهم می‌آورد.[۲]

۱. محسنی، فرید، «**تحولات کیفری در قانون میهن‌پرستی آمریکا**»، دیدگاه‌های حقوق قضایی، شماره ۱۸، ۱۳۹۱، ص۱۸۰.

۲. وفادار، حسین، «**فناوری اطلاعات و تأثیرات آن در رفتار سازمانی پلیس**»، دانش انتظامی، شماره ۳۵، ۱۳۸۶، صص ۷۶-۹۵.

در این راستا، دو مؤلفه کلیدی یعنی کنترل هویت افراد و تجمیع داده‌های اطلاعاتی در فرآیندهای نوین پیش‌گیری نقشی بنیادین دارند.

بند اول. کنترل هویت و کاهش گم‌نامی

در بسیاری از بسترهای اجتماعی و فضای دیجیتال، گم‌نامی افراد می‌تواند بستر مساعدی برای ارتکاب انواع جرایم فراهم آورد. به ویژه در محیط‌هایی مانند شبکه‌های اجتماعی، بازارهای دارک‌وب یا تجمعات گسترده، بزهکاران از خلأهای هویتی برای پنهان‌سازی اقدامات مجرمانه خود بهره می‌گیرند. از این رو، پلیس‌ها در کشورهای مختلف با هدف کاهش فرصت ارتکاب جرم به شناسایی دقیق هویت افراد از طریق فناوری‌های نوین اقدام کرده‌اند.

یکی از مهم‌ترین ابزارها در این راستا، سیستم‌های تشخیص هویت بیومتریک است که از طریق اسکن چهره، اثر انگشت، عنبیه چشم و دیگر ویژگی‌های زیستی، امکان شناسایی دقیق افراد را فراهم می‌کند. در حال حاضر، ایالات متحده آمریکا از سامانه US-VISIT بهره می‌برد که اطلاعات بیومتریک همه مهاجران، گردشگران و حتی شهروندان برخی کشورها (به ویژه کشورهای مسلمان) را ذخیره‌سازی می‌کند. این اطلاعات تا ۷۵ تا ۱۰۰ سال در پایگاه‌های اطلاعاتی پلیس و آژانس‌های اطلاعاتی باقی می‌مانند.[1]

نمونه‌های مشابهی از این اقدامات در روسیه، چین و ژاپن نیز دیده می‌شود. در بریتانیا، استفاده از فناوری تشخیص چهره در فضاهای عمومی با هدف پیش‌بینی رفتارهای مشکوک و دستگیری پیش‌دستانه در حال توسعه است. هرچند این رویکردها با انتقادهایی در حوزه حقوق بشر به ویژه درباره حفظ حریم خصوصی مواجه شده‌اند، اما دولت‌ها، آن‌ها را ابزارهایی مؤثر در پیش‌گیری وضعی از جرم می‌دانند.

از جمله دیگر ابزارهای کنترلی می‌توان به کارت‌های هویت هوشمند، گذرنامه‌های بیومتریک، گواهی‌نامه‌های دیجیتال، مالکیت ثبت‌شده سیم‌کارت‌ها، اطلاعات تراکنش‌های مالی و حتی دسترسی به داده‌های ذخیره‌شده در فضای ابری اشاره کرد. تمامی این ابزارها با هدف افزایش شفافیت، کاهش گم‌نامی و شناسایی رفتارهای مجرمانه در سطوح مختلف طراحی شده‌اند.

1.GAO. (2023). **Facial Recognition Services: Federal Law Enforcement Agencies Should Better Assess Privacy and Accuracy** Risks:www.gao.gov/products/gao-23-105607.

بند دوم. تجمیع اطلاعات فردی و دسترسی به بانک‌های اطلاعاتی

گام دوم در فرآیند پیش‌گیری پلیسی، بهره‌گیری از تجمیع داده‌های گسترده از منابع مختلف برای تحلیل دقیق رفتارهای مجرمانه و پیش‌بینی جرایم آتی است. تحلیل جرم[1] به عنوان فرآیندی ساختاریافته شامل بررسی اطلاعات گردآوری‌شده درباره جرایم رخ‌داده، شناسایی الگوها و روندها و ارائه گزارش‌های تحلیلی برای حمایت از عملیات پلیسی است.[2]

در این راستا، بانک‌های اطلاعاتی بزرگی در سطح ملی و بین‌المللی شکل گرفته‌اند که داده‌های مختلف از جمله سوابق کیفری، فعالیت‌های مالی، ارتباطات اجتماعی، مکالمات آنلاین، سوابق پزشکی و حتی علایق و رفتارهای رسانه‌ای افراد را گردآوری می‌کنند. یکی از نمونه‌های قابل توجه، پروژه‌های دولت الکترونیک نظیر **GSB** است که با اتصال نهادهای دولتی، اطلاعات شهروندان را به صورت یک‌پارچه در اختیار نهادهای امنیتی قرار می‌دهد.

بر اساس مطالعات جدید، تجزیه و تحلیل این داده‌ها با بهره‌گیری از فناوری‌هایی مانند هوش مصنوعی و یادگیری ماشینی می‌تواند به پیش‌بینی رفتارهای پرخطر و شناسایی مناطق جرم‌خیز کمک کند. برای مثال، در ایالت نیویورک، استفاده از مدل CompStat به پلیس اجازه داده است تا با تحلیل داده‌های مکان‌محور و زمانی، توزیع جغرافیایی جرم را شناسایی کند و اقدامات هدفمند انجام دهد.[3] البته چالش‌هایی نیز وجود دارد؛ داده‌های ناقص یا مخدوش، سوگیری الگوریتم‌ها، نقض حریم خصوصی و احتمال استفاده سوء از اطلاعات ذخیره‌شده از جمله مواردی هستند که می‌توانند منجر به بی‌اعتمادی عمومی یا حتی بازداشت اشتباه افراد شوند. برای مثال، در یکی از گزارش‌های ۲۰۲۳ خبرگزاری آسوشیتدپرس آمده است که فناوری تشخیص چهره موجب بازداشت اشتباه یک شهروند بی‌گناه شده بود.[4]

1..Crime Analysis

۲. ۲. قناد، فاطمه و الهام شریف، «**مطالعه اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا**»، دوفصل‌نامه حقوق فناوری‌های نوین، دوره دوم، شماره ۴، ۱۴۰۰.

3.. Police Chief Magazine. (2023). April 2023: Data-Driven Policing:www.policechiefmagazine.org/magazine-issues/april-2023-data-driven-policing.

4..AP News. (2023). Facial recognition technology jailed a man for days: www.apnews.com/article/b613161c56472459df683f-

در نهایت، می‌توان گفت که تحلیل جرم نه تنها ابزاری برای فهم بهتر رفتارهای مجرمانه در گذشته است، بلکه پلیس را قادر می‌سازد با استفاده از داده‌ها و پیش‌بینی‌های علمی، در مسیر «پیش‌گیری هوشمند» گام بردارد؛ رویکردی که امروزه در ادبیات جرم‌شناسی نوین با عنوان Predictive Policing شناخته می‌شود.[1]

گفتار چهارم. بانک‌های اطلاعاتی و چالش‌های حریم خصوصی

بانک‌های اطلاعاتی در عین حال که کارکردهای قابل توجهی در بهبود کارآمدی نهادهای امنیتی دارند، می‌توانند تهدیدی جدّی برای حریم خصوصی افراد محسوب شوند. پایگاه‌های داده الکترونیکی گرچه در ارتقای کارآمدی سازمان‌ها، توزیع منصفانه‌تر خدمات اجتماعی و تقویت نظارت مؤثر برای پیش‌گیری از وقوع جرایم نقش‌آفرین هستند، اما با خطرهایی همراهند که نمی‌توان از آن‌ها چشم پوشید. دولت‌ها در توجیه گردآوری و استفاده از این داده‌ها به مزایای یادشده استناد می‌کنند، اما این توجیه‌ها نتوانسته‌اند افکار عمومی را نسبت به نقض احتمالی حریم خصوصی شهروندان قانع سازند.

در واکنش به این نگرانی‌ها، در سال ۱۹۷۴، قانونی در ایالات متحده تصویب شد که به موجب آن، تشکیل پایگاه‌های داده‌ای متمرکز و جامع درباره افراد توسط نهادهای دولتی، مشروط به وضوح هدف و کارکرد قانونی آن‌ها شد. در غیر این صورت، چنین اقداماتی ممنوع اعلام گردید. با این حال، حوادثی چون حملات تروریستی به ویژه پس از واقعه ۱۱ سپتامبر موجب شد این محدودیت‌ها در پرتو منافع امنیت ملی نادیده گرفته شوند.[2] در ادامه همین روند، کشورهای ایالات متحده، انگلستان، کانادا، استرالیا و نیوزیلند با همکاری متقابل، از ظرفیت شبکه‌های اطلاعاتی موجود برای شنود، ردیابی و پردازش روزانه ارتباطات تلفنی، دورنگار و ایمیل در سطح جهانی بهره‌برداری می‌کنند. این شبکه‌ها عملاً امکان نظارت بر بخش زیادی از فعالیت‌های افراد در خانه، محل کار و دیگر عرصه‌های زندگی را فراهم کرده‌اند. این شرایط، ضرورت حمایت حقوقی از اطلاعات خصوصی و مقابله با سوء استفاده احتمالی دولت‌ها و بخش خصوصی از داده‌های محرمانه را دوچندان ساخته است.[3]

54320d08a7.

۱. شهریاری، حمید، «**حریم خصوصی اطلاعات**»، فصل‌نامه علمی و پژوهشی دانشگاه قم، سال هشتم، شماره ۳ و ۴، ۱۳۸۶.

۲. معتمدنژاد، کاظم، **اجلاس جهانی سران درباره جامعه اطلاعاتی**، تهران: پدیده گوتنبرگ، ۱۳۸۲، ص۳۳۴.

۳. شاه‌محمدی، غلامرضا و محمدتقی ساروخانی، «**نقش فناوری اطلاعات در پیش‌گیری از جرم**»، در: مجموعه مقالات ارسالی

در پی حادثه ۱۱ سپتامبر، مقررات سخت‌گیرانه‌تری در ایالات متحده وضع شد؛ از جمله قانون امنیت پرواز و حمل‌ونقل مصوب ۱۹ نوامبر ۲۰۰۱ و قانون پنجم می ۲۰۰۵ که به موجب آن، شرکت‌های هواپیمایی ملزم شدند از تاریخ ۵ مارس ۲۰۰۳، اطلاعات خاصی از مسافران را جمع‌آوری و ارائه کنند. این اطلاعات که با نام «PNR" (Passenger Name Record) شناخته می‌شوند، شامل داده‌هایی نظیر تاریخ پرواز، مسیر سفر، خدمات درخواستی، پرداخت‌ها، رزرو هتل و خودرو و نوع غذای انتخاب‌شده می‌شود. آشکار است که این حجم اطلاعات شخصی می‌تواند به سهولت، حریم خصوصی افراد را نقض کند[۱]. افزون بر آن، قانون موسوم به «فهرست ممنوعیت پرواز» در آمریکا باعث شده است برخی مسافران صرفاً به دلیل تشابه اسمی با افراد مظنون به اقدامات تروریستی، هدف بازرسی‌های شدید، بازجویی و حتی منع پرواز قرار گیرند؛ موضوعی که به ویژه برای شهروندان عرب‌تبار به دلیل تشابه اسامی، تبعاتی جدّی به همراه داشته و منجر به نقض حقوق مدنی آن‌ها شده است.[۲]

بیش‌تر کشورها نیز دارای بانک‌های اطلاعاتی وابسته به سرویس‌های امنیتی هستند که دسترسی آن‌ها در اختیار نهادهای امنیتی و پلیس قرار دارد. این بانک‌ها، اطلاعات مرتبط با فعالیت‌های اقتصادی و مالی شرکت‌ها به ویژه شرکت‌های چندملیتی را به صورت گسترده ذخیره می‌کنند؛ چون این اطلاعات، بیش‌تر با منافع ملی گره خورده‌اند. هم‌چنین با گسترش جرایمی نظیر پول‌شویی و کلاه‌برداری فراملی، سازمان‌های امنیتی به تبادل اطلاعات مالی و ردیابی گردش وجوه در بسترهای الکترونیکی روی آورده‌اند. از آن‌جایی که انتقال پول عمدتاً به صورت دیجیتال و نه از طریق اسناد فیزیکی صورت می‌گیرد، ناتوانی در شناسایی مسیرهای الکترونیکی نقل‌وانتقال به معنای از دست دادن ردّ پای منابع مالی مشکوک و تسهیل وقوع جرایم مالی خواهد بود.[۳]

به نخستین همایش ملی پیش‌گیری از جرم (جلد اول)، تهران: دفتر تحقیقات کاربردی پلیس پیش‌گیری ناجا، ۱۳۸۹.

۱. لطفیان، سعیده و حمید رهنورد، «**امنیت در برابر آزادی‌های فردی: تحلیل هزینه‌ها و منافع سیاست ضد تروریسم دولت بوش**»، فصل‌نامه سیاست، مجله دانشکده حقوق و علوم سیاسی، شماره ۴، ۱۳۸۴، ص۱۹۴.

۲. شعبانلی، عمران، محمد میرزایی و سید محمد هاشمی، «**چالش‌های تقنینی تحقیقات پلیس در جرایم امنیتی**»، فصل‌نامه پژوهش‌های جرم شناختی پلیس، تابستان ۱۴۰۲، شماره ۱۱.

۳. ستوده، مجتبی، «**نقش اطلاعات در تحقیقات جنایی**»، فصل‌نامه کارآگاه، سال سوم، شماره ۹، ۱۳۸۹.

در نتیجه، برخی کشورها ناگزیر شده‌اند در شرایط خاص، مجوز بازرسی از بانک‌های اطلاعاتی مؤسسات مالی و اعتباری خود را صادر کنند. با این حال، برخی حوزه‌های اطلاعاتی هم‌چون اسرار بانکی به عنوان حریم غیر قابل تعرض شهروندان محسوب می‌شوند. حتی شهروندان قانون‌مدار نیز انتظار دارند که دسترسی به اطلاعات حساب‌های بانکی‌شان تنها با توجیه حقوقی روشن صورت پذیرد. در عین حال، آگاهی شهروندان از تهدیدهای بالقوه و سازوکارهای حفاظتی موجود، لازمه صیانت از اعتماد عمومی در چنین شرایطی است.

در این زمینه، چالش‌های حقوق بشری متعددی مطرح می‌شود. بسیاری از سازمان‌های امنیتی با استناد به منافع ملی به داده‌هایی دسترسی پیدا می‌کنند که این کارشان یا مبنای حقوقی شفاف ندارد یا مشمول هیچ‌گونه نظارت مؤثری نیست. گاه از مفهوم «منافع ملی» به عنوان ابزاری برای فرار از پاسخ‌گویی حقوقی و سیاسی بهره‌برداری می‌شود و این امر، خطر نادیده‌گرفتن قواعد حمایتی در حوزه حقوق شهروندی و استثنا کردن سوابق پلیسی را به همراه دارد. تجاوزهای پنهان الکترونیکی همانند بازرسی‌های فیزیکی مخفیانه، مسائل حقوقی عمیقی را برمی‌انگیزد. فناوری‌های نوین اطلاعاتی، مرز میان فضاهای خصوصی و عمومی را کم‌رنگ ساخته‌اند و امکان ورود به حریم شخصی افراد را بدون حضور فیزیکی در منازل آنان فراهم کرده‌اند. در حال حاضر، هرچند این داده‌ها محرمانه فرض می‌شوند، اما دسترسی به آن‌ها توسط نهادهای امنیتی در عمل، به صورت موردی و گاه بدون نظارت قانونی کافی انجام می‌پذیرد.[1]

گفتار پنجم. رویکردهای بین‌المللی به حفاظت از داده‌های شخصی

حق برخورداری از حریم خصوصی در برابر دخالت دولت‌ها، شرکت‌ها یا اشخاص دیگر، در بسیاری از کشورها به عنوان بخشی از قوانین ملی و گاه در سطح قانون اساسی شناسایی شده است. در بیش‌تر کشورهای توسعه‌یافته، قوانین مشخصی برای حمایت از اطلاعات شخصی شهروندان تصویب شده‌اند. برای نمونه، فرانسه در سال ۱۹۷۸، آلمان در سال ۱۹۷۷ و سوئیس در سال ۱۹۹۲، قوانین فدرالی در زمینه حفاظت از داده‌ها وضع کردند. ایالات متحده از سال ۱۹۷۴، کانادا از ۱۹۸۳، مالزی از ۲۰۱۰، کره جنوبی از ۲۰۱۱، ترکیه از ۲۰۱۶ و عربستان سعودی از ۲۰۲۱ دارای مقرراتی در این زمینه هستند.

۱. تدین، عباس، «**اصل مشروعیت تحصیل دلیل**»، در: **تازه‌های علوم جنایی** (مجموعه مقاله‌ها)، تهران: میزان، ۱۳۸۸.

البته باید توجه داشت که در بسیاری از کشورها، قوانین خاصی نیز وجود دارد که به طور محدودکننده‌ای بر حریم خصوصی تأثیر می‌گذارد. برای مثال، قوانین مالیاتی معمولاً مستلزم افشای اطلاعات درآمدی و سود شخصی افراد هستند. هم‌چنین در مواردی، حق حریم خصوصی ممکن است با آزادی بیان یا منافع عمومی در تعارض قرار گیرد. افزون بر این، تعاریف فرهنگی از حریم خصوصی بسیار متفاوتند و به بافت فرهنگی، شرایط اقتصادی و تحولات فناورانه جوامع بستگی دارند.[1]

حریم خصوصی اطلاعاتی یا حفاظت از داده‌ها، مفهومی است که در مورد شیوه جمع‌آوری، نگه‌داری و استفاده از داده‌ها در بسترهای فناورانه و غیر فناورانه تعریف می‌شود. این موضوع از منظر قانونی، سیاسی و اجتماعی، زمانی اهمیت ویژه می‌یابد که اطلاعات جمع‌آوری‌شده منجر به شناسایی افراد گردد. ریشه مسئله را در افشای کنترل‌نشده داده‌های شخصی می‌دانند. منابع اطلاعاتی مرتبط با این موضوع شامل سوابق پزشکی، پرونده‌های کیفری، داده‌های مکانی، قومیتی و خدمات مبتنی بر موقعیت جغرافیایی هستند. چالش اصلی، اطمینان از ناشناسی افراد هنگام اشتراک‌گذاری داده‌هایشان است.

در ماده ۸ کنوانسیون اروپایی حقوق بشر، حق افراد نسبت به حریم خصوصی، زندگی شخصی، مسکن و مکاتبات به رسمیت شناخته شده و تنها در موارد استثنایی مانند امنیت ملی، سلامت عمومی، پیش‌گیری از جرم و رعایت حقوق دیگران و آن هم به شرط قانونی بودن و ضرورت در یک جامعه دموکراتیک قابل تحدید است. دیوان اروپایی حقوق بشر نیز تأکید دارد که جزئیات قوانین مرتبط باید شفاف باشد و استفاده مداوم از فناوری‌ها تنها در صورت وجود ضرورت دموکراتیک مشروع خواهد بود.

کنوانسیون شورای اروپا در ۲۸ ژانویه ۱۹۸۱ با عنوان «حمایت از اشخاص در برابر پردازش خودکار داده‌های شخصی»، پس از تصویب توسط پنج کشور، در سال ۱۹۸۵ لازم‌الاجرا شد. این کنوانسیون، هدف خود را ایجاد استانداردهای حداقلی برای حفاظت از داده‌ها در سطح ملی و بین‌المللی اعلام کرده است که در آن، نه تنها از حریم خصوصی افراد، بلکه از انتقال فرامرزی داده‌ها نیز حمایت می‌شود.

1. Stanford Encyclopedia of Philosophy First published Tue May 14, 2002; substantive revision Mon Sep 18, 2006:www.plato.stanford.edu/entries/privacy/#PriRel.

اصل پردازش منصفانه و هدف‌مند داده‌ها، کیفیت داده‌ها، تناسب و روزآمدی اطلاعات، و جلوگیری از نگه‌داری غیر ضروری، از جمله اصول بنیادین این سند هستند. هم‌چنین برای پردازش داده‌های حساس مانند نژاد، مذهب، سلامت و سوابق کیفری، تضمین‌های بیش‌تری در نظر گرفته شده است.[1]

دستورالعمل ۲۴ اکتبر ۱۹۹۵ اتحادیه اروپا نیز با هدف هماهنگ‌سازی سطح حمایت از داده‌های شخصی در میان کشورهای عضو به تصویب رسید. هرچند این دستورالعمل، حداقل حمایت را الزام‌آور می‌دانست، اما ارتقای سطح حمایت را نیز تشویق می‌کرد. با پیشرفت شگرف فناوری‌های ارتباطی در اواخر دهه ۹۰، تهدیدهایی نوین متوجه حریم خصوصی کاربران شد؛ به ویژه در حوزه داده‌های ارتباطی خصوصی شهروندان. در پاسخ، اتحادیه اروپا در ۱۲ ژوییه ۲۰۰۲، دستورالعمل شماره ۲۰۰۲/۵۸/EC موسوم به «دستورالعمل حریم خصوصی و ارتباطات الکترونیکی» را تصویب کرد.[2]

در نهایت، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) در سال ۲۰۱۶ جای‌گزین دستورالعمل ۱۹۹۵ شد. این مقررات، تمامی کسب‌وکارهایی را که با شهروندان اتحادیه اروپا تعامل دارند، مشمول می‌کند، حتی اگر در خارج از این منطقه مستقر باشند. رویکرد GDPR مبتنی بر حفاظت اطلاعات «از طریق طراحی و به صورت پیش‌فرض» است. داده‌ها باید مستعارسازی یا بی‌نام‌سازی شوند و تنها با رضایت صریح و آگاهانه افراد قابل پردازش باشند. هم‌چنین صاحبان داده‌ها حق دارند رضایت خود را در هر زمانی پس بگیرند.[3]

از جمله مواردی که اجازه پردازش داده‌ها بدون رضایت فرد را می‌دهند، عبارتند از:

- تأمین منافع مشروع کنترل‌کننده یا شخص ثالث (با رعایت منشور حقوق بنیادین اتحادیه اروپا)
- انجام وظایف عمومی یا مأموریت رسمی
- پای‌بندی به الزامات قانونی
- تحقق تعهدات قراردادی با شخص موضوع داده
- حفاظت از منافع حیاتی شخص موضوع داده یا فردی دیگر

1. www.eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

2.. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981/108):www.rm.coe.int/1680078b37.

3.. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data

این مقررات از ۲۵ مه ۲۰۱۸ اجرایی شده و در تمامی کشورهای عضو بدون نیاز به تصویب مجدد لازم‌الاجراست.[۱]

اصول بنیادین حمایت از داده‌های شخصی در GDPR شامل این مفاد است:

۱. پردازش داده‌ها باید به صورت منصفانه، قانونی و شفاف صورت گیرد.
۲. داده‌ها باید با هدفی مشخص، مشروع و شفاف جمع‌آوری شوند و برای اهداف دیگر استفاده نشوند.
۳. اطلاعات گردآوری‌شده باید متناسب، مرتبط و محدود به اهداف مورد نظر باشند.
۴. داده‌ها باید دقیق و در صورت لزوم به‌روز باشند و داده‌های نادرست حذف یا اصلاح شوند.
۵. داده‌ها باید به گونه‌ای ذخیره شوند که امکان شناسایی افراد تنها در مدت زمان لازم برای هدف مشخص فراهم باشد.
۶. پردازش داده‌های حساس (مانند: نژاد، مذهب و سلامت) ممنوع است، مگر با رضایت صریح و آگاهانه شخص.
۷. اشخاص باید از حق اطلاع و دسترسی به داده‌هایشان برخوردار باشند.
۸. افراد می‌توانند با پردازش داده‌های مرتبط با خود مخالفت کنند.
۹. اشخاصی که به نمایندگی از سازمان‌ها، داده‌ها را پردازش می‌کنند، ملزم به رعایت محرمانگی اطلاعات هستند.

مستثنیات از حمایت داده‌ها (علاوه بر رضایت فردی) نیز عبارتند از:

۱. حفظ امنیت ملی
۲. دفاع ملی و امنیت عمومی
۳. پیش‌گیری، تحقیق و تعقیب جرایم
۴. منافع اقتصادی یا مالی مهم
۵. وظایف حاکمیتی مانند تنظیم مقررات یا نظارت عمومی

---

۱. نقشینه، نادر و همکاران، «**ارائه چارچوبی برای داده‌گان ملی با تمرکز بر توسعه حاکمیت داده . محورهای موضوعی**»، فصل‌نامه فناوری اطلاعات و ارتباطات ایران، دوره سیزدهم، شماره ۴۹، پاییز و زمستان ۱۴۰۰.

گفتار پنجم. جایگاه حریم خصوصی در ایران

نقض حریم خصوصی دیگران، ذاتاً و اصالتاً از منظر فقهی و حقوقی قابل پذیرش نیست. در نظام حقوقی ایران، مصادیق حق بر حریم خصوصی اطلاعات شناسایی و حمایت شده‌اند. با نگاهی به قوانین داخلی مشخص می‌شود که در موارد استثنایی مانند کشف جرم، تأمین امنیت، تعارض با حقوق دیگران یا مصالح عمومی، امکان تجسس و نقض حریم خصوصی افراد پذیرفته شده است. برخی از جنبه‌های حق بر حریم خصوصی اطلاعات، مانند ممنوعیت تفتیش عقاید و افکار، بازرسی نامه‌ها و مکاتبات شخصی و منع هتک حیثیت متهمان و زندانیان، در قانون اساسی جمهوری اسلامی ایران تصریح شده‌اند. هم‌چنین برخی حمایت‌های کیفری ـ هرچند ناکامل ـ در قبال نقض حقوق و آزادی‌های فردی توسط مأموران دولتی پیش‌بینی شده‌اند.

در همین راستا، قانون آیین دادرسی کیفری ۱۳۹۲ نیز پیشرفت‌های قابل ملاحظه‌ای در حمایت از حریم خصوصی اطلاعاتی افراد داشته است.[۱] مطابق ماده ۴۰ این قانون، افشای اطلاعات مربوط به هویت و محل اقامت بزه‌دیدگان، شهود، مطلعان و دیگر اشخاص مرتبط با پرونده، توسط ضابطان دادگستری جز در موارد مشخص‌شده قانونی ممنوع است. ماده ۹۶ نیز انتشار تصویر و مشخصات متهم در همه مراحل تحقیقات مقدماتی توسط رسانه‌ها و مراجع انتظامی و قضایی را ممنوع اعلام کرده است، مگر در موارد خاصی که به تشخیص بازپرس و دادستان شهرستان این اقدام ضروری باشد. ماده ۱۰۱، بازپرس را مکلف کرده است تدبیرهای لازم را برای جلوگیری از دسترسی اشخاص به اطلاعاتی در نظر بگیرد که افشای آن‌ها ممکن است تمامیت جسمی یا حیثیت بزه‌دیده را به خطر اندازد. هم‌چنین طبق ماده ۱۵۱، ضابطان قضایی، مجاز به دسترسی به حساب‌های بانکی افراد نیستند، مگر با درخواست بازپرس و تأیید رئیس کل دادگستری استان.[۲]

---

۱. در مواد۵۷۰، ۵۷۲، ۵۷۳، ۵۷۴ و ۵۷۵ کتاب تعزیرات در قانون مجازات اسلامی و مواد ۶۰۴ و ۶۴۸ به حریم خصوصی اطلاعات و ماده ۵۸۲ به حریم خصوصی ارتباطات توجه شده و برای نقض‌کنندگان آن، ضمانت اجراهای کیفری پیش‌بینی کرده است. علاوه بر آن، در مواد ۵۸ تا ۶۲ قانون تجارت الکترونیکی (۱۳۸۲) به حمایت از داده‌های شخصی پرداخته و ضمانت اجراهایی در مواد ۷۱ تا ۷۴ پیش‌بینی شده است.

۲. وروایی، اکبر و همکاران، «**ملاحظات حقوقی تأسیس بانک‌های اطلاعاتی ژنتیکی جنایی در پرتو الزامات حقوق شهروندی**»، دانش انتظامی، شماره ۳، ۱۳۸۸.

علاوه بر این موارد، در قوانین دیگری نیز به حفظ حریم خصوصی اطلاعات توجه شده است، از جمله مواد ۵۸ و ۵۹ و مواد ۶۴ و ۶۵ قانون تجارت الکترونیک (۱۳۸۲) درباره حمایت از اسرار تجاری و مواد ۱۵ و ۱۶ قانون شرکت پست جمهوری اسلامی ایران (۱۳۶۶). با این حال، در خصوص تجمیع و به‌اشتراک‌گذاری داده‌ها در سامانه‌های اطلاعاتی پلیس، تصریحات قانونی کافی وجود ندارد. این خلأهای قانونی و نبود چارچوب جامع و منسجم برای صیانت از داده‌ها و اطلاعات شخصی سبب شده است که در سال‌های اخیر، تلاش‌هایی برای تدوین لوایح و قوانین تکمیلی در این حوزه صورت گیرد.

در این راستا، سه سند مهم و قابل توجه مطرح شده‌اند که هر یک از زاویه‌ای خاص به موضوع حفاظت از حریم خصوصی اطلاعاتی و داده‌های شخصی پرداخته‌اند: پیش‌نویس لایحه حمایت از حریم خصوصی، قانون مدیریت داده‌ها و اطلاعات ملی (دوام) و پیش‌نویس لایحه حفاظت از داده‌ها. در ادامه، هر یک از این اسناد به صورت جداگانه بررسی می‌شود تا ابعاد مختلف تلاش قانون‌گذار برای حفاظت از حریم خصوصی و داده‌های اشخاص تحلیل گردد.

بند اول. پیش‌نویس لایحه حمایت از حریم خصوصی

تعریف دقیق و جامعی از مفهوم «حریم خصوصی» همواره با چالش مواجه بوده است و برخی، آن را مفهومی مبهم قلمداد کرده‌اند. با این حال، می‌توان گفت که حریم خصوصی به طور کلی، ناظر بر حوزه‌ای از زندگی فردی است که شخص نمی‌خواهد دیگران بدون رضایت او وارد آن شوند یا از آن اطلاع یابند. این حریم، نوعی منطقه امن و شخصی در زندگی فردی است که دسترسی به آن، نیازمند رضایت صریح یا ضمنی شخص است.

در بند ۱ ماده ۲ پیش‌نویس لایحه حمایت از حریم خصوصی، این حریم چنین تعریف شده است: «قلمرویی از زندگی هر شخص که وی به طور متعارف یا با اعلام قبلی در چارچوب قانون انتظار دارد دیگران بدون رضایت او وارد آن نشوند، آن را مشاهده یا نظارت نکنند و به اطلاعات مرتبط با آن دسترسی نداشته باشند یا در آن حوزه، تعرضی به وی صورت نگیرد».[1]

---

۱. هوسمن، کارل، «**حمایت از حریم خصوصی افراد در برابر حق آگاهی**»، ترجمه: داوود حیدری، فصل‌نامه رسانه، سال هفتم، شماره ۳، ۱۴۰۰، ص ۴۲.

حریم خصوصی اطلاعاتی و داده‌ای شامل اطلاعاتی است که فرد تمایلی به افشای آن ندارد و تلاش می‌کند از طرق مختلف از دسترسی دیگران به آن جلوگیری کند؛ چون این داده‌ها با هویت و شخصیت انسانی وی ارتباط مستقیم دارند. برخی حقوق‌دانان از این حوزه به عنوان «حق پنهان داشتن حقایق زندگی شخصی» یاد می‌کنند.

در تبیین دقیق‌تر این حق، باید به چند نکته کلیدی اشاره کرد:

۱. حریم خصوصی ناظر بر اطلاعاتی است که ماهیتی صرفاً شخصی دارند و افشای آن‌ها از نظر فرد نامطلوب است؛ ولی چنان‌چه این اطلاعات با مسائل اجتماعی یا عمومی درهم‌آمیزد، دیگر نمی‌توان آن را صرفاً در قلمرو حقوق شخصی دانست.
۲. افشای بخشی از اطلاعات خصوصی یک فرد، مجوزی برای افشای دیگر اطلاعات یا توزیع مجدد اطلاعات منتشرشده محسوب نمی‌شود، مگر آن‌که آن اطلاعات دیگر ویژگی خصوصی خود را از دست داده باشند.
۳. هر داده‌ای که به صورت آشکار و عمومی در دسترس نباشد و برای دست‌یابی به آن به تلاش یا ابزار خاص نیاز باشد، در قلمرو حریم خصوصی داده‌ای قرار می‌گیرد.

باید توجه داشت که حق بر حریم خصوصی عمدتاً ناظر بر اشخاص حقیقی است. با این حال، برخی معتقدند که اشخاص حقوقی نیز دارای نوعی حریم خصوصی هستند، اگرچه سطح انتظار از این حریم محدودتر است. برای نمونه، حریم جنسی که در اشخاص حقیقی موضوعیت دارد، در مورد اشخاص حقوقی قابل طرح نیست، اما اسرار تجاری، اطلاعات مالی و حرفه‌ای شرکت‌ها می‌توانند در این قلمرو قرار گیرد.[۱]

بند دوم. قانون مدیریت داده‌ها و اطلاعات ملی

بر اساس قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱، داده‌ها و اطلاعات ملی با رعایت اصول امنیتی و محرمانگی اطلاعات اشخاص، در اختیار دولت جمهوری اسلامی ایران قرار دارد. دستگاه‌ها و نهادهای مشمول این قانون و ارائه‌دهندگان خدمات زیرمجموعه تنظیم‌گران بخشی موظفند

۱. جعفری، علی و محمدرضا رهبرپور، «**مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه**»، پژوهش حقوق خصوصی، سال پنجم، شماره ۱۸، ۱۳۹۶.

صرفاً بر اساس سطوح دسترسی تعیین‌شده توسط کارگروه تعامل‌پذیری دولت الکترونیکی، امکان دسترسی و تبادل این داده‌ها را فراهم کنند (ماده ۴).

مطابق ماده ۵ این قانون، دستگاه‌ها مکلفند در فرآیند تولید، نگه‌داری، پردازش، حفظ امنیت و صیانت از داده‌های شخصی و تبادل، اشتراک‌گذاری، به‌روزرسانی و تکمیل داده‌ها، سیاست‌های مصوب شورای عالی فضای مجازی و مصوبات کارگروه تعامل‌پذیری دولت الکترونیکی را به‌کار گیرند. بر اساس ماده ۶ نیز اعمال تدابیر حفاظتی و امنیتی برای صیانت از داده‌ها و محرمانگی اطلاعات اشخاص بر عهده دستگاه‌ها و نهادهای مسئول تولید، نگه‌داری یا پردازش این داده‌هاست.

حق دسترسی به اطلاعات، حقی همگانی تلقی شده و به کاهش هزینه‌ها، افزایش بهره‌وری و صرفه‌جویی در منابع منجر می‌شود، اما همین دسترسی می‌تواند تهدیدهایی مانند نقض حریم خصوصی شهروندان در پی داشته باشد. ایجاد بانک‌های اطلاعاتی توسط پلیس و اشتراک‌گذاری اطلاعات تنها در صورتی مشروع است که اطلاعات منتشرشده دقیقاً مشخص، مخاطبان آن محدود و دلایل دسترسی معتبر باشند.

با ایجاد هرگونه سامانه یا خدمت الکترونیکی، اطلاعات کاربران ذخیره می‌شود و با تجمیع و پردازش آن، ارزش اطلاعات افزایش می‌یابد. این فرآیند از سه جهت اهمیت دارد:

۱. حفاظت اطلاعات در برابر حملات سایبری
۲. نظارت بر دسترسی و حفظ حریم خصوصی
۳. بهره‌برداری مجاز و مشروع از داده‌ها

ماده ۱ قانون انتشار و دسترسی آزاد به اطلاعات (مصوب ۱۳۸۷)، اطلاعات را به شخصی و عمومی تقسیم کرده و بدون ارائه تعریف جامع از اطلاعات شخصی، مصادیقی مانند نام و نام خانوادگی، نشانی، شماره حساب بانکی و رمز عبور را برشمرده است. اطلاعات عمومی نیز شامل ضوابط، آمار ملی، اسناد و مکاتبات اداری است، مشروط بر آن‌که جزو مستثنیات فصل چهارم این قانون (مانند اسرار دولتی یا حریم خصوصی) نباشد. شیوه‌نامه تشخیص اطلاعات شخصی از عمومی (مصوب ۱۳۹۷)، مصادیق رایج اطلاعات مربوط به حریم خصوصی و داده‌های شخصی را مشخص کرده است.

بند سوم. لایحه حفاظت از داده‌ها

نبود قانون جامع برای حفاظت از داده‌های شخصی در ایران، یکی از چالش‌های مهم در مسیر تحقق حق بر حریم خصوصی محسوب می‌شود. بیش‌تر قوانین موجود دارای رویکردی واکنشی هستند و تنها در زمان وقوع رخدادهای خاص قابل اجرایند، در حالی که مقرراتی مانند GDPR اتحادیه اروپا بر پیش‌گیری و آموزش تأکید دارند.

در قوانین GDPR، سازمان‌ها موظفند حتی‌الامکان از دریافت داده‌های غیر ضروری بپرهیزند و داده‌های دریافتی را به صورت دوره‌ای حذف کنند. هم‌چنین نهادهای دارنده داده موظف به آموزش کارکنان برای حفظ امنیت اطلاعات هستند. در مقابل، قوانین ایران بیش‌تر کلی‌اند و وارد جزئیات فنی و اجرایی نشده‌اند که این موضوع می‌تواند زمینه‌ساز برداشت‌های متفاوت یا حتی سوء استفاده باشد.

برای مثال، پرسش‌هایی اساسی هم‌چنان بی‌پاسخ مانده‌اند، از جمله:

۱. چه نوع اطلاعاتی مشمول عنوان «داده شخصی» یا «حریم خصوصی» می‌شود؟
۲. آیا اطلاعات بیولوژیکی، ژنتیکی، سیاسی، عقیدتی یا عضویت‌های صنفی نیز جزو اطلاعات حساسند؟
۳. سرویس‌های اینترنتی و اپلیکیشن‌ها تا چه حد مجاز به ذخیره و اشتراک‌گذاری اطلاعاتی مانند IP و موقعیت مکانی کاربران هستند؟

لایحه حفاظت از داده‌های شخصی به صورت مستقیم، مسئولیت کسب‌وکارها، دولت و اشخاص حقیقی و حقوقی را در حفاظت از داده‌های شخصی مشخص می‌کند. با تصویب این لایحه و تبدیل آن به قانون در صورت هک و نشت اطلاعات و مشخص شدن تقصیر کسب‌وکارها، برای آن‌ها جریمه مشخص شده‌است. هم‌چنین طبق آن‌چه در پیش‌نویس این لایحه آمده است، هر کسی می‌تواند به داده‌های شخصی خود دسترسی داشته باشد و بر هرنوع پردازش داده روی داده‌های خود نظارت کند. تغییر جریان داده از سمت دولت به کسب‌وکارها در بسیاری از مواقع، منتظر تصویب این قانون است؛ چون باید مسئولیت کسب‌وکارها در قبال داده‌ها مشخص و نحوه ذخیره آن مشخص شود.

گفتار ششم. حفاظت‌های پیش رو در برابر سوء استفاده از بانک‌های اطلاعاتی

با رشد روزافزون فناوری‌های دیجیتال و استفاده گسترده از داده‌های شخصی، بانک‌های اطلاعاتی پلیس به یکی از حساس‌ترین و مهم‌ترین ابزارهای نهادهای امنیتی تبدیل شده‌اند. این بانک‌ها، حاوی اطلاعات گسترده‌ای از شهروندان هستند؛ از هویت فردی گرفته تا سوابق کیفری، اطلاعات مالی، رفت‌وآمدهای جغرافیایی و حتی روابط اجتماعی. استفاده از این اطلاعات می‌تواند نقش مهمی در شناسایی مجرمان، پیش‌بینی جرایم و مقابله با تهدیدهای امنیتی داشته باشد. در کنار این کاربردهای مفید، خطرهای مهمی نیز وجود دارد که نباید از آن‌ها غفلت کرد.

یکی از اصلی‌ترین نگرانی‌ها، احتمال سوء استفاده از این داده‌ها توسط افرادی است که به آن‌ها دسترسی دارند. اگرچه فناوری‌های نظارتی امکان ردیابی و کنترل کاربران را فراهم کرده‌اند، اما این ابزارها زمانی مؤثر خواهند بود که در کنار آن، اصول اخلاقی و الزامات قانونی رعایت شود. دسترسی به اطلاعات باید محدود، هدفمند و بر اساس مجوزهای مشخص صورت گیرد. این‌که چه کسانی به بانک‌های اطلاعاتی دسترسی دارند، چه نوع داده‌هایی را مشاهده می‌کنند، به چه هدفی از آن استفاده می‌کنند و تحت چه شرایطی اجازه این دسترسی را پیدا کرده‌اند، از جمله سؤالات مهمی است که باید به صورت شفاف پاسخ داده شود.

برخی کارشناسان بر این باورند که تنها اعتماد به فناوری برای محافظت از داده‌ها کافی نیست، بلکه باید فرهنگ مسئولیت‌پذیری و پاسخ‌گویی در میان کارکنان نهادهای امنیتی نهادینه شود. به عبارتی، اگر فردی که به اطلاعات دسترسی دارد، وجدان حرفه‌ای نداشته باشد، پیشرفته‌ترین سامانه‌های نظارتی هم قادر به جلوگیری از تخلف نخواهند بود. از طرف دیگر، یکی از چالش‌های مهم دیگر، صحت و دقت اطلاعات موجود در بانک‌های داده‌ای است. پلیس باید بداند که داده‌ها همواره مطلق و بی‌نقص نیستند و تکیه کورکورانه بر آن‌ها می‌تواند منجر به تصمیم‌گیری نادرست شود. مقایسه و تطبیق اطلاعات با دیگر منابع مستقل مانند نتایج حاصل از مصاحبه با شهروندان یا بررسی‌های میدانی می‌تواند در افزایش اعتبار داده‌ها مؤثر باشد.

در بسیاری از کشورها مانند آلمان و سوئد، قوانینی برای تنظیم شیوه استفاده از اطلاعات در بانک‌های داده‌ای تصویب شده است. این قوانین بر مواردی چون مدت نگه‌داری اطلاعات، سطح

محرمانگی داده‌ها، نحوه ثبت دسترسی‌ها و پاسخ‌گویی به سوء استفاده‌ها تأکید دارند. حتی در شرایطی که بانک اطلاعاتی میان چند نهاد به اشتراک گذاشته می‌شود، باید سازوکار مشخصی برای ثبت فعالیت کاربران وجود داشته باشد تا بتوان تشخیص داد چه کسی به چه داده‌ای دسترسی داشته و با آن چه کرده است.[1] مطالعات اخیر نیز بر اهمیت این موضوع تأکید دارند. این مطالعات بر لزوم ایجاد «معماری‌های نظارتی پاسخ‌گو» در سیستم‌های داده‌ای پلیس تأکید می‌کنند که نه تنها نظارت فنی، بلکه نظارت انسانی و حقوقی را نیز شامل می‌شود.[2]

در نهایت باید گفت حفظ توازن میان امنیت عمومی و حقوق حریم خصوصی، تنها از طریق شفاف‌سازی فرآیندهای جمع‌آوری، ذخیره و استفاده از داده‌ها امکان‌پذیر است. در نهایت، حفاظت از بانک‌های اطلاعاتی پلیس نیازمند نگاهی ترکیبی به حقوق بشر، امنیت عمومی و پیشرفت‌های فناورانه است. این حفاظت‌ها تنها زمانی اثربخش خواهند بود که بر پایه شفافیت، پاسخ‌گویی، آموزش کارکنان و نظارت قانونی شکل گرفته باشند؛ زیرا شهروندان حق دارند بدانند اطلاعاتی را که درباره آن‌ها گردآوری شده است، چه کسی چگونه و برای چه منظوری استفاده می‌کند.[3]

نتیجه گیری

این پژوهش با هدف بررسی ابعاد نظری، حقوقی و عملی بهره‌برداری پلیس از داده‌های تجمیع‌شده و بانک‌های اطلاعاتی در فرآیند پیش‌گیری از جرم انجام شد. در بطن این هدف تلاش شد به مسئله‌ای بنیادین پاسخ داده شود: چگونه می‌توان در عصری که اطلاعات، منبع قدرت شناخته می‌شوند، تعادلی معقول و مشروع میان حق بر امنیت و حق بر حریم خصوصی شهروندان برقرار ساخت؟ این مسئله امروزه بیش از هر زمان دیگر، در فضای دیجیتال و شبکه‌ای‌شده امروز، حساسیت‌برانگیز و نیازمند واکاوی حقوقی و اخلاقی است.

---

۱. قمری، اسماعیل، اکبر وروایی و مسعود قاسمی، «**توسل به اقدامات غیر مشروع جهت تحصیل دلیل جزایی**»، فصل‌نامه تحقیقات حقوقی آزاد، دوره سیزدهم، شماره ۴۸، ۱۳۹۹.

2.. Kitchin, R., & Dodge, M. (2023). Code/Space: Software and Everyday Life. MIT Press.

3.. Zwitter, A., & Hummel, P. (2022). "Big Data Governance: Between Security, Ethics, and the Law", Journal of Big Data & Society, 9(1), 1-14.

یافته‌های حاصل از این پژوهش نشان داد که گرچه اطلاعات و داده‌های شخصی، ابزار ضروری برای کشف جرم و پیش‌گیری محسوب می‌شوند، اما می‌توانند به ابزاری برای نقض حقوق شهروندی، تضعیف اعتماد عمومی و گسترش دامنه کنشگری‌های بدون ضابطه بدل شوند. داده‌ها زمانی می‌توانند در خدمت امنیت باشند که گردآوری، نگه‌داری، پردازش و بهره‌برداری از آن‌ها در چارچوبی روشن، مبتنی بر قانون و نظارت‌پذیر صورت گیرد. دسترسی پلیس به اطلاعات حساس مانند هویت دیجیتال، سوابق کیفری، داده‌های رفتاری و ارتباطات خصوصی اگر بدون شفافیت حقوقی و پاسخ‌گویی باشد، تهدیدی بالقوه برای حقوق بنیادین فردی خواهد بود.

در جهان امروز که داده‌ها به آسانی تولید، ذخیره، اشتراک‌گذاری و پردازش می‌شوند، مرزهای سنتی میان حوزه عمومی و خصوصی به شدت مخدوش شده است. این تغییر بنیادین، ضرورت بازنگری در چارچوب‌های حقوقی و رویه‌های اجرایی نهادهای حافظ امنیت به ویژه پلیس را دوچندان کرده است. پژوهش نشان می‌دهد که اگرچه حق بر امنیت، یکی از ارکان حقوق بشری محسوب می‌شود، اما این حق، در تعارض یا تعادل با حقوق دیگری مانند حریم خصوصی، آزادی ارتباطات و کرامت انسانی قرار می‌گیرد و نباید بهانه‌ای برای نقض آن‌ها باشد.

یکی از مهم‌ترین چالش‌هایی که در مسیر بهره‌برداری از داده‌ها توسط پلیس وجود دارد، نبود مرزهای دقیق و شفاف در تعیین این است که چه اطلاعاتی باید گردآوری شود، در چه سطحی از سازمان نگه‌داری شود، چه کسانی به آن دسترسی داشته باشند و تحت چه شرایطی امکان بهره‌برداری از آن‌ها وجود دارد. نبود قوانین جامع و یک‌پارچه در این زمینه، زمینه‌ساز تفسیرهای سلیقه‌ای، مداخله‌های فراقانونی و در برخی موارد، سوء استفاده‌های اطلاعاتی است. هم‌چنین ضعف پاسخ‌گویی در برابر افشای داده‌های شخصی یا بهره‌برداری ناموجه از اطلاعات به تزلزل اعتماد عمومی منجر می‌شود و این در حالی است که اعتماد، رکن اساسی در رابطه پلیس با شهروندان به شمار می‌رود.

پیش‌گیری از جرم به ویژه در قالب پیش‌گیری کنشی، پیش از ورود رفتارها به دایره جرم، بیش از هر حوزه دیگری نیازمند دقت، ظرافت و نظارت‌های چندلایه است. در این مرحله، هرگونه اقدام بدون چارچوب مشخص قانونی، احتمال نقض حقوق بنیادین را افزایش می‌دهد. هم‌چنین نظام

پاسخ‌گویی کارآمد و شفاف، یکی از ارکان بنیادین در بهره‌گیری مشروع و مسئولانه از اطلاعات است. صرف بهره‌گیری از داده‌ها بدون طراحی فرآیندهای گزارش‌دهی، بررسی شکایات، ثبت سوابق دسترسی و پی‌گیری سوء استفاده‌ها به گسترش فضای بی‌اعتمادی و خودکامگی خواهد انجامید.

با وجود اهمیت یافته‌ها، این پژوهش با محدودیت‌هایی نیز مواجه بود. از جمله مهم‌ترین آن‌ها، دسترسی نداشتن به اسناد طبقه‌بندی‌شده یا رویه‌های اجرایی پلیس در زمینه استفاده از داده‌ها و کمبود ادبیات بومی‌شده درباره حق بر حریم خصوصی در نظام حقوقی ایران بود. هم‌چنین امکان پژوهش میدانی در این حوزه به‌دلیل ماهیت امنیتی و محرمانه اطلاعات عملاً محدود بود و تحلیل‌ها بر اساس اسناد و ادبیات نظری صورت گرفت.

بر پایه تحلیل‌های انجام‌شده روشن است که اگر هدف، بهره‌گیری مؤثر و مشروع از اطلاعات برای پیش‌گیری از جرم باشد، ناگزیر باید قلمرو حقوقی حریم خصوصی بازتعریف شود و محدوده اختیارات پلیس به صورت شفاف، محدود و نظارت‌پذیر تعیین گردد. هم‌چنین قانون‌گذار باید نسبت به تدوین مقررات اجرایی صریح، تعیین رویه‌های قانونی برای گردآوری، ثبت، نگه‌داری، دسترسی و ویرایش اطلاعات اقدام کند و هم‌زمان، نهادهای نظارتی مستقلی برای ارزیابی عملکرد نهادهای امنیتی و انتظامی شکل گیرد. این اقدامات در کنار طراحی سازوکارهای پاسخ‌گویی به افکار عمومی، موجب ارتقای اعتماد عمومی، شفافیت عملکرد پلیس و در نهایت، تقویت سرمایه اجتماعی خواهد شد. در چنین شرایطی است که امنیت نه در تقابل با آزادی، بلکه در تعاملی سازنده با آن معنا خواهد یافت.

پیشنهادهای این پژوهش به این شرح است:

یک. تدوین چارچوب قانونی جامع برای جمع‌آوری و بهره‌برداری از داده‌ها

پیشنهاد می‌شود قوانین مستقلی با موضوع صیانت از داده‌های شخصی در اختیار نهادهای انتظامی و امنیتی تدوین شود. این قوانین باید:

۱. به صراحت، نوع اطلاعات مجاز برای گردآوری، مدت زمان نگه‌داری، نحوه استفاده و شرایط اشتراک‌گذاری با دیگر نهادها را مشخص کنند.

۲. دسترسی به اطلاعات را محدود به سطوح مشخص سازمانی کنند و دسترسی‌های غیر مجاز را مشمول ضمانت اجراهای کیفری و اداری قرار دهند.

دو. ایجاد نظام نظارت مستقل و پاسخ‌گو بر بانک‌های اطلاعاتی پلیس

ضروری است نهاد یا کمیته‌ای مستقل (مثلاً زیر نظر قوه قضاییه یا نهادهای حقوق بشری) برای نظارت بر عملکرد بانک‌های اطلاعاتی پلیس و رسیدگی به شکایات شهروندان تأسیس شود. این نهاد باید:

۱. مجاز به انجام ممیزی‌های دوره‌ای از نحوه بهره‌برداری پلیس از داده‌ها باشد.
۲. سازوکاری برای گزارش‌دهی عمومی و شفاف درباره موارد تخلف یا سوء استفاده احتمالی فراهم آورد.

سه. ارتقای فرهنگ سازمانی و آموزش تخصصی برای کارکنان پلیس

آموزش منظم و هدفمند کارکنان پلیس در زمینه اخلاق حرفه‌ای، حفظ حریم خصوصی و الزامات قانونی مرتبط با اطلاعات شخصی باید به برنامه‌ای ساختاریافته و الزام‌آور تبدیل شود. این آموزش‌ها باید:

۱. با سناریوهای واقعی همراه باشند تا درک عملیاتی مأموران نسبت به حقوق شهروندی افزایش یابد.

۲. با نظارت مستمر و آزمون‌های ارزیابی برای حفظ کیفیت اجرا شوند.

فهرست منابع

۱. فارسی

الف) کتاب

۱. بیابانی، غلام‌حسین، **اطلاعات جنایی**، تهران: کارآگاه، پلیس آگاهی ناجا، ۱۴۰۱.

۲. محمدی، زهرا، **نظام نظارت اداری در ایران**، تهران: پژوهشکده قوه قضاییه، ۱۳۹۸.

۳. معتمدنژاد، کاظم، **اجلاس جهانی سران درباره جامعه اطلاعاتی**، تهران: پدیده گوتنبرگ، ۱۳۸۲.

۴. یورگنسون، رایکه فرانک، **حقوق بشر در جامعه جهانی اطلاعات**، ترجمه: بهرام مستقیمی، قم: آیین احمد، ۱۳۸۶.

ب) مقاله

۱. تدین، عباس، «اصل مشروعیت تحصیل دلیل»، در: **تازه‌های علوم جنایی (مجموعه مقاله‌ها)**، تهران: میزان، ۱۳۸۸.

۲. جعفری، علی و محمدرضا رهبرپور، «**مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه**»، پژوهش حقوق خصوصی، سال پنجم، شماره ۱۸، ۱۳۹۶.

۳. ستوده، مجتبی، «**نقش اطلاعات در تحقیقات جنایی**»، فصل‌نامه کارآگاه، سال سوم، شماره ۹، ۱۳۸۹.

۴. شاه‌محمدی، غلامرضا و محمدتقی ساروخانی، «**نقش فناوری اطلاعات در پیش‌گیری از جرم**»، در: مجموعه مقالات ارسالی به نخستین همایش ملی پیش‌گیری از جرم (جلد اول)، تهران: دفتر تحقیقات کاربردی پلیس پیش‌گیری ناجا، ۱۳۸۹.

۵. شعبانلی، عمران، محمد میرزایی و سید محمد هاشمی، «**چالش‌های تقنینی تحقیقات پلیس در جرایم امنیتی**»، فصل‌نامه پژوهش‌های جرم شناختی پلیس، تابستان ۱۴۰۲، شماره ۱۱.

۶. شهریاری، حمید، «**حریم خصوصی اطلاعات**»، فصل‌نامه علمی و پژوهشی دانشگاه قم، سال هشتم، شماره ۳ و ۴، ۱۳۸۶.

۷. قاضی‌زاده، محمدعلی، «**پلیس و تحدید حریم خصوصی شهروندان از منظر حقوق اداری**»، پژوهش‌نامه حقوق عمومی، سال چهارم، شماره ۲، ۱۳۹۷.

۸. قمری، اسماعیل، اکبر وروایی و مسعود قاسمی، «**توسل به اقدامات غیر مشروع جهت تحصیل دلیل جزایی**»، فصل‌نامه تحقیقات حقوقی آزاد، دوره سیزدهم، شماره ۴۸، ۱۳۹۹.
۹. قناد، فاطمه و الهام شریف، «**مطالعه اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا**»، دوفصل‌نامه حقوق فناوری‌های نوین، دوره دوم، شماره ۴، ۱۴۰۰.
۱۰. لطفیان، سعیده و حمید رهنورد، «**امنیت در برابر آزادی‌های فردی: تحلیل هزینه‌ها و منافع سیاست ضد تروریسم دولت بوش**»، فصل‌نامه سیاست، مجله دانشکده حقوق و علوم سیاسی، شماره ۴، ۱۳۸۴.
۱۱. لطیف‌زاده، مهدیه و همکاران، «**تبیین اسباب مشروعیت پردازش داده‌های شخصی از منظر حقوق اتحادیه اروپا و ایران**»، فصل‌نامه مطالعات حقوقی، دوره چهاردهم، شماره سوم، ۱۴۰۱.
۱۲. لطیف‌زاده، مهدیه و همکاران، «**تحلیل بستر قانونی داده‌های شخصی در اتحادیه اروپا و ایران**»، پژوهش‌نامه پردازش و مدیریت اطلاعات، دوره سی و هفتم، شماره ۳، ۱۴۰۰.
۱۳. محسنی، فرید، «**تحولات کیفری در قانون میهن‌پرستی آمریکا**»، دیدگاه‌های حقوق قضایی، شماره ۱۸، ۱۳۹۱.
۱۴. محمدی، حسن، «**چالش‌های حقوقی بهره‌برداری پلیس از اطلاعات شخصی در ایران**»، فصل‌نامه حقوق فناوری اطلاعات، دوره اول، شماره ۴، ۱۳۹۸.
۱۵. محمدی، رضا، «**نقش نظارت اداری در پیش‌گیری از سوء استفاده از اطلاعات شخصی در ساختارهای پلیسی**»، پژوهش‌نامه حقوق عمومی، سال هفتم، شماره ۳، ۱۳۹۸.
۱۶. موذن‌زادگان، حسن‌علی، «**تضمینات حقوق دفاعی متهمان و امر بازجویی در مرحله تحقیقات مقدماتی**»، پژوهش حقوق و سیاست، شماره ۲۸، ۱۳۸۹.
۱۷. نقشینه، نادر و همکاران، «**ارائه چارچوبی برای داده‌گان ملی با تمرکز بر توسعه حاکمیت داده. محورهای موضوعی**»، فصل‌نامه فناوری اطلاعات و ارتباطات ایران، دوره سیزدهم، شماره ۴۹، پاییز و زمستان ۱۴۰۰.
۱۸. هوسمن، کارل، «**حمایت از حریم خصوصی افراد در برابر حق آگاهی**»، ترجمه: داوود حیدری، فصل‌نامه رسانه، سال هفتم، شماره ۳، ۱۴۰۰.
۱۹. وروایی، اکبر و همکاران، «**ملاحظات حقوقی تأسیس بانک‌های اطلاعاتی ژنتیکی جنایی در پرتو الزامات حقوق شهروندی**»، دانش انتظامی، شماره ۳، ۱۳۸۸.

۲۰. وفادار، حسین، «**فناوری اطلاعات و تأثیرات آن در رفتار سازمانی پلیس**»، دانش انتظامی، شماره ۳۵، ۱۳۸۶.
۲۱. یعقوبی، محدثه و همکاران، «**تبیین چالش‌های قانون دسترسی آزاد به اطلاعات از منظر اساتید ارتباطات و اصحاب رسانه**»، فصل‌نامه مطالعات رسانه‌های نوین، سال ششم، شماره ۲۱، ۱۳۹۹.

2. Latin Source

1. Adams, C. "Classification of Privacy Techniques." University of Ottawa Law & Technology Journal 3, no. 1 (2006).

2. AP News. Facial Recognition Technology Jailed a Man for Days :www.apnews.com/article/b613161c56472459df683f54320d08a7 (last visited on 21/04/2025).

3. Braga, Anthony A., and David L. Weisburd, Police Innovation and Crime Prevention: Lessons Learned from Police Research over the Past 20 Years. Paper presented at the National Institute of Justice (NIJ), Policing Research Workshop: Planning for the Future, Washington DC, 2007.

4. Dolunay, A., F. Kaspa, and G. Kececi, "Freedom of Mass Communication in the Digital Age in the Case of the Internet: 'Freedom House' and the USA Example." Journal of Sustainability 12, No. 18 (2017): 124–138.

5. GAO (U.S. Government Accountability Office). Facial Recognition Services: Federal Law Enforcement Agencies Should Better Assess Privacy and Accuracy Risks. 2023. Available at: www.gao.gov/products/gao-23-105607

6. Gonzales, Alberto R., and Regina B. Schofield, Intelligence-Led Policing: The New Intelligence Architecture. U.S. Department of Justice, Office of Justice Programs, 2005. Available at: www.ojp.usdoj.gov

7. Kitchin, Rob, and Martin Dodge, Code/Space: Software and Everyday Life. MIT Press, 2023.

8. Nouwt, Sjaak, et al. Reasonable Expectation of Privacy?. The Hague: T.M.C. Asser Press, 2005

9. Police Chief Magazine. April 2023: Data-Driven Policing. www.policechiefmagazine.org/magazine-issues/april-2023-data-driven-policing (last visited on 21/04/2025).

10. Solove, Daniel J., Understanding Privacy, Cambridge, MA: Harvard University Press, 2008.

11. Stanford Encyclopedia of Philosophy First published Tue May 14, 2002; substantive revision Mon Sep 18, 2006: www.plato.stanford.edu/entries/privacy/#PriRel.

12. Taylor, Nick, State Surveillance and the Right to Privacy:www.surveillance-and-socity.org (last visited on 21/04/2025).

13. Zuboff, Shoshana, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York: PublicAffairs, 2019.

14. Zuboff, Shoshana, The Age of Surveillance Capitalism. PublicAffairs. 2019

15. Zwitter, A., and P. Hummel, "Big Data Governance: Between Security, Ethics, and the Law", Big Data & Society 9, No. 1 (2022): 1–14.

Title: Police Databases: Balancing the Right to Security and Informational Privacy

Mohsen Soofi Zomorrod[1], Mohsen Rezaei[2]

Abstract

Background and Objective: As a central institution responsible for maintaining public order and safety, the police frequently engage with citizens' personal data. These data, consolidated into large-scale databases, not only enhance service delivery and crime detection efficiency but also pose significant challenges to individual privacy. In today's world, where information is considered a source of power, the fundamental question arises: How can a proper balance be maintained between the right to public security and the protection of individual privacy?

Methodology: This study adopts a descriptive-analytical approach based on library resources. Through a comparative lens, it examines the relationship between security interests and the fundamental rights of citizens in the collection and utilization of personal data within police databases.

Findings: Aggregated data play a vital role in identifying crime patterns, analyzing criminal behavior, and informing preventive strategies. However, legal gaps in the processes of data collection, storage, and utilization -combined with the absence of robust oversight and accountability mechanisms- can lead to violations of civil rights, erosion of public trust, and intrusive breaches of privacy. Moreover, in the absence of transparent accountability systems, the risk of data misuse or unauthorized disclosure significantly increases.

Conclusion: Ensuring security must not come at the cost of violating fundamental freedoms. Accordingly, legal and operational frameworks governing data aggregation and usage should be re-evaluated. The development of clear legal standards, the introduction of criminal penalties for unauthorized use, stakeholder awareness initiatives, institutional oversight, and mechanisms for redress are essential steps toward achieving a balance between security and individual freedoms within the legal system governing police databases.

KeyWords: Security, Personal Data, Database, Police, Informational Privacy

1. Law department police university, (Corresponding Author), m.sufi61@gmail.com

2. Assistant Professor, Department of Law and Criminology, University of Police Sciences, mohsenrezaee3492@gmail.com