فصلنامه علمی تخصصی فقه و حقوق معاصر

سال یازدهم- زمستان ۱٤۰٤- شماره ۳٤- ص۵۷-۷۸

محدودیت‌های حقوق عمومی در استفاده پلیس از فناوری‌های نظارتی هوشمند چالشِ حریم خصوصی و اصلِ تناسب

محمدپویا الماسی[۱]

چکیده

این تحقیق با عنوان «محدودیت‌های حقوق عمومی در استفاده پلیس از فناوری‌های نظارتی هوشمند: چالشِ حریم خصوصی و اصلِ تناسب»، به تحلیل جامع و عمیق ابعاد حقوقی و چالش‌های بنیادین ناشی از به‌کارگیری فناوری‌های نوین نظارتی توسط نهادهای پلیسی در جوامع معاصر می‌پردازد. با توجه به تحولات شگرف فناورانه و گذار به پارادایم «پلیس‌گری دیجیتال»، ابزارهایی نظیر سامانه‌های تشخیص چهره، پایش فراگیر تصویری، تحلیل کلان‌داده‌ها و الگوریتم‌های پیش‌بینی جرم، پارادایم‌های سنتی امنیت و نظارت عمومی را به طور اساسی دگرگون ساخته‌اند.در این راستا، پژوهش حاضر ابتدا مبانی مشروعیت حقوقی این اقدامات نظارتی را در چارچوب نظری «نظم عمومی» در حقوق عمومی مورد کنکاش قرار می‌دهد. سپس، به طور جدی به بررسی چالش‌های کلیدی پیش روی دو اصل بنیادین حقوق شهروندی، یعنی «حریم خصوصی» و «اصل تناسب»، می‌پردازد. در بخش حریم خصوصی، پیامدهای احتمالی نظارت فراگیر و مستمر بر زندگی فردی و اجتماعی، شکل‌گیری «جامعه تحت نظارت» و تلاش برای حفظ این حق اساسی در سپهر عمومی و خصوصی مد نظر قرار می‌گیرد. در بحث اصل تناسب، این اصل به عنوان یک معیار بنیادین حقوقی، در سنجش مشروعیت و میزان مداخله‌ی نظارتی پلیس، مورد ارزیابی دقیق قرار گرفته و بر ضرورت انطباق شدت اقدام با هدف امنیتی و پرهیز از هرگونه افراط یا تفریط تأکید می‌شود.فراتر از این دو محور اصلی، تحقیق حاضر به مداقه‌ی موشکافانه در ابعاد دیگری نیز می‌پردازد؛ از جمله، بررسی دقیق توازن میان منافع امنیتی جامعه و حقوق اساسی شهروندان، با تمرکز بر حق بر حریم خصوصی، آزادی بیان و رفت‌وآمد. همچنین، چالش‌های مربوط به ارتقاء شفافیت در به‌کارگیری فناوری‌های نظارتی و ایجاد سازوکارهای مؤثر پاسخگویی پلیس در قبال هرگونه سوءاستفاده یا خطای فنی، مورد تحلیل قرار می‌گیرد. در این میان، مبانی قانونی و الزامات حقوقی جمع‌آوری و پردازش داده‌های بیومتریک توسط پلیس، همراه با تأکید بر نقش حیاتی نظارت قضایی، به دقت بررسی می‌شود. پدیده‌ی تبعیض الگوریتمیک، یعنی احتمال بروز تبعیض ناخواسته یا هدفمند علیه گروه‌های خاص ناشی از عملکرد الگوریتم‌های نظارتی، نیز از دیگر موضوعات مورد کنکاش در این پژوهش است. در بخش مطالعه تطبیقی، رویکردها و تدابیر حقوقی در نظام‌های قضایی منتخب، خصوصاً اتحادیه اروپا (با تمرکز بر مقررات GDPR)، در جهت تحدید اختیارات پلیس و حفاظت از حقوق شهروندان در فضای دیجیتال، مورد ارزیابی قرار می‌گیرد.در نهایت، این تحقیق با ترسیم چشم‌اندازی واقع‌بینانه برای آینده، بر لزوم تدوین یک «منشور اخلاقی و حقوقی جامع برای پلیس هوشمند» تأکید ورزیده و

[۱] کارشناسی ارشد حقوق خصوصی

mohammadpouyaalmasi@gmail.com

چارچوب‌های تقنینی ضروری برای تضمین اجرای مسئولانه و قانون‌مند فناوری‌های نظارتی، ضمن صیانت از کرامت و حقوق بنیادین شهروندان را ارائه می‌دهد.

واژگان کلیدی: فناوری‌های نظارتی هوشمند، پلیس‌گری دیجیتال ،حقوق عمومی،پلیس هوشمند،اصل تناسب.

مقدمه

عصر حاضر، دوران گذار شگرفی را در نحوه‌ی اعمال اقتدار عمومی، به‌ویژه در حوزه‌ی اقدامات پلیسی، تجربه می‌کند. پیشرفت‌های خیره‌کننده در عرصه‌ی فناوری اطلاعات و ارتباطات، منجر به ظهور و گسترش «فناوری‌های نظارتی هوشمند» شده است؛ ابزارهایی که به طور بالقوه کارایی نهادهای امنیتی را در حفظ نظم و امنیت عمومی افزایش می‌دهند، اما همزمان، پرسش‌های بنیادینی را در باب حدود اختیارات دولت و حقوق بنیادین شهروندان مطرح می‌سازند. از سامانه‌های تشخیص چهره و تحلیل کلان‌داده‌ها گرفته تا پهپادهای مجهز به دوربین و الگوریتم‌های پیش‌بینی جرم، طیف وسیعی از فناوری‌ها، امکان نظارت بی‌سابقه بر زندگی فردی و عمومی را فراهم آورده‌اند. این تحول فناورانه، که از آن با عنوان «پلیس‌گری دیجیتال» یاد می‌شود، نظام حقوق عمومی را با چالش‌های جدی مواجه کرده است؛ چالش‌هایی که نیازمند بازنگری در اصول بنیادین و تدوین چارچوب‌های نوین تقنینی هستند.در این میان، دو اصل بنیادین حقوق عمومی و شهروندی، یعنی «حریم خصوصی» و «اصل تناسب»، بیش از هر اصل دیگری در معرض این چالش‌ها قرار گرفته‌اند. حق بر حریم خصوصی، به عنوان یکی از اساسی‌ترین حقوق فردی، در معرض تهدید جدی «نظارت فراگیر» قرار دارد؛ وضعیتی که در آن، داده‌های زندگی روزمره‌ی شهروندان به طور مداوم جمع‌آوری، پردازش و تحلیل می‌شوند، و این امر می‌تواند به فروپاشی مفهوم حریم خصوصی و شکل‌گیری «جامعه تحت نظارت» منجر گردد. از سوی دیگر، «اصل تناسب» به عنوان معیاری کلیدی در سنجش مشروعیت اقدامات اقتدار عمومی، در مواجهه با این فناوری‌ها، نیازمند بازتعریف و اعمال دقیق‌تر است. این اصل ایجاب می‌کند که هرگونه مداخله در حقوق شهروندان، از جمله حق بر حریم خصوصی، باید کاملاً ضروری، مؤثر و متناسب با هدف امنیتی مورد نظر باشد؛ امری که در عمل، با توجه به توانمندی‌های گسترده‌ی فناوری‌های نوین، حصول آن به چالشی جدی بدل گشته است.ضرورت پژوهش در این حوزه، از آن رو نشأت می‌گیرد که بدون درک عمیق محدودیت‌های حقوق عمومی و بدون ایجاد سازوکارهای قانونی و نظارتی کارآمد، خطر سوءاستفاده از این فناوری‌ها، نقض گسترده حقوق بنیادین شهروندان، و ایجاد اختلال در توازن حساس میان امنیت و آزادی، به طور جدی منافع عمومی و فردی را تهدید خواهد کرد. این تحقیق، با هدف روشن‌ساختن این چالش‌ها، به تحلیل مبانی مشروعیت حقوقی

نظارت پلیسی، پیامدهای فناورانه بر حریم خصوصی، و سازوکارهای اعمال اصل تناسب در این بستر نوین می‌پردازد. همچنین، به بررسی دقیق چالش‌های مربوط به شفافیت، پاسخگویی، جمع‌آوری داده‌های بیومتریک، نظارت قضایی، و پدیده‌ی تبعیض الگوریتمیک پرداخته و در نهایت، با الهام از تجارب بین‌المللی، راهکارهایی را برای تدوین چارچوب‌های تقنینی و اخلاقی مورد نیاز جهت هدایت مسئولانه «پلیس هوشمند» ارائه خواهد داد.

مفهوم گذر از پلیس‌گری سنتی به پلیس‌گریِ دیجیتال

در فضای مفهوم‌پردازی تحولات اخیر در حوزه‌ی اقدامات پلیسی، عبور از پارادایم سنتی به سوی «پلیس‌گری دیجیتال» یک دگردیسی بنیادین را نمایان می‌سازد. این دگردیسی صرفاً ناظر به جایگزینی ابزارهای فیزیکی با فناوری‌های نوین نیست، بلکه دلالت بر تغییر ماهیتِ خودِ نظارت، مداخله و پیش‌بینی در حوزه‌ی جرم دارد. اگر پلیس سنتی بیشتر به جمع‌آوری اطلاعات میدانی، بازجویی‌های حضوری و تحلیل‌های تجربی متکی بود، پلیس دیجیتال بر پایه‌ی داده‌های انبوه، الگوریتم‌های پیچیده و قابلیت‌های نظارتیِ فراگیر بنا شده است. این تحول، ابزارهای پلیسی را از واکنش‌گرایی صرف به سمت رویکردهای پیش‌دستانه و حتی پیش‌بینانه سوق داده است، که این خود پیامدهای عمیقی برای اصول حقوقی بنیادین و مفهوم شهروندی به همراه دارد (صفاری، ۱۳۹۸: ۶۵).

ظهور و گسترش ابزارهای نظارتی نوین، ستون فقرات این گذار را تشکیل می‌دهد. فناوری «تشخیص چهره»، که قابلیت شناسایی افراد در اماکن عمومی و حتی برخط را فراهم می‌آورد، نمونه‌ای بارز از این دگرگونی است. این ابزار، با توانایی تحلیل و تطبیق چهره‌ها با پایگاه‌های داده‌ی عظیم، امکان شناسایی مظنونان، رصد تحرکات، و حتی پیش‌بینی احتمال وقوع جرم بر اساس الگوهای رفتاری را فراهم می‌آورد، هرچند خود به شدت با چالش‌های مربوط به دقت، حریم خصوصی و احتمال خطای الگوریتمی روبرو است (موسوی، ۱۳۹۹: ۷۵). این قابلیت، فراتر از محدوده‌ی عملیات‌های پلیسی سنتی، حوزه‌ی عمومی را به فضایی تحت نظارت مداوم تبدیل می‌کند.

در کنار تشخیص چهره، «پایش‌های پهپادی» نیز نقشی محوری در بسط قابلیت‌های نظارتی ایفا می‌کنند. پهپادها، با بهره‌گیری از دوربین‌های با وضوح بالا، حسگرهای حرارتی و سیستم‌های موقعیت‌یاب، قادرند مناطق وسیعی را از بالا پوشش داده و داده‌های تصویری و مکانیِ ارزشمندی را جمع‌آوری نمایند. این توانایی، امکان رصد

تجمعات، شناسایی مسیرهای احتمالی فرار، و حتی نظارت بر مناطق دورافتاده و صعب‌العبور را فراهم می‌آورد؛ امری که در عملیات‌های سنتی پلیسی با محدودیت‌های جدی عملیاتی و لجستیکی مواجه بود (کدخدایی، ۱۳۹۷: ۴۳). کارایی این ابزار در جمع‌آوری اطلاعاتِ میدانیِ لحظه‌ای، آن را به یکی از ارکان پلیس‌گری دیجیتال بدل کرده است.

علاوه بر این، «الگوریتم‌های پیش‌بینی جرم» که بر پایه‌ی تحلیل آماری داده‌های تاریخی جرم، الگوهای مکانی و زمانی وقوع جرایم، و حتی داده‌های جمع‌آوری شده از منابع مختلف (مانند شبکه‌های اجتماعی یا سوابق رفتاری)، عمل می‌کنند، افق جدیدی را در پلیس‌گری گشوده‌اند. این الگوریتم‌ها تلاش می‌کنند تا با پیش‌بینی زمان و مکان احتمالی وقوع جرایم، پلیس را قادر سازند تا منابع خود را به طور مؤثرتری تخصیص دهد و از وقوع جرایم جلوگیری کند. با این حال، این حوزه خود با انتقادات جدی در خصوص احتمال تعصبات الگوریتمی، تشدید نظارت بر جوامع خاص، و پیامدهای آن بر عدالت کیفری روبرو است (کاپل، ۲۰۰۵: ۳۲).

گذار به پلیس‌گری دیجیتال، صرفاً به معنای به‌کارگیری ابزارهای جدید نیست، بلکه مستلزم بازنگری در مبانی حقوقی ناظر بر نظارت، جمع‌آوری اطلاعات، و مداخله در حریم افراد است. فناوری‌هایی چون تشخیص چهره، پایش پهپادی و الگوریتم‌های پیش‌بینی، پارادایم‌های سنتی حقوق کیفری و دادرسی عادلانه را به چالش می‌کشند. این ابزارها، با قابلیت جمع‌آوری و تحلیل داده‌های عظیم و اغلب حساس، امکان دخالت در حریم خصوصی افراد را در سطحی بی‌سابقه فراهم می‌آورند. علاوه بر این، نحوه‌ی عملکرد الگوریتم‌های پیش‌بینی، که ممکن است بر اساس داده‌های تاریخیِ آلوده به سوگیری‌های اجتماعی بنا شده باشند، می‌تواند منجر به تشدید تبعیض علیه گروه‌های خاص و نقض اصل برابری در برابر قانون گردد.

از نظر نگارنده، این مجموعه از فناوری‌ها، ماهیتِ رابطه‌ی میان شهروند و دولت را دگرگون ساخته و مفهوم «نظارت» را از یک اقدام واکنشی و موردی، به یک فرآیند مستمر، فراگیر و پیش‌بینانه تبدیل کرده است. این تحول، مستلزم تحلیل عمیق حقوقی و فلسفی در خصوص مبانی مشروعیت این سطح از نظارت، حدود مجاز آن، و تضمین‌هایی است که باید برای صیانت از حقوق بنیادین افراد در برابر این قدرتِ فزاینده‌ی فناورانه اتخاذ گردد. چالش اصلی در این مرحله، یافتن تعادلی پایدار میان ضرورت‌های امنیتی و حقوق اساسی شهروندان است؛ تعادلی که بتواند ضمن بهره‌مندی از مزایای فناوری، از سقوط به ورطه‌ی استبداد نظارتی جلوگیری کند.

مفهوم «نظارتِ گسترده» و خطرِ فروپاشیِ حریم خصوصی در حقوق عمومی

مفهوم «نظارتِ گسترده» که به جمع‌آوری و پردازشِ سیستماتیک و فراگیرِ داده‌ها در موردِ تعدادِ کثیری از افراد اطلاق می‌شود، یکی از چالش‌برانگیزترین مسائلِ حقوق عمومی در عصرِ دیجیتال است. این پدیده، که عمدتاً توسطِ دولت‌ها و سازمان‌های اطلاعاتی، و گاهی نیز توسطِ شرکت‌های بزرگِ فناوری، پیگیری می‌شود، زنگِ خطری جدی برای «حریم خصوصی» به عنوان یکی از بنیادین‌ترین حقوقِ شهروندی به صدا درآورده است. پرسشِ اساسی این است که آیا استمرار و گستردگیِ این نظارت‌ها، که فضاهایِ عمومی را به طورِ دائم در معرضِ دید قرار می‌دهند، اساساً مفهومی به نام «حریم خصوصی» را در این فضاها از بین برده است؟ (موسوی، ۱۳۹۹: ۱۲۰).

نظارتِ گسترده، برخلافِ نظارتِ هدفمند که بر افراد یا گروه‌های خاصی متمرکز است، حجمِ عظیمی از اطلاعات را از طریقِ ابزارهایِ متنوعی مانندِ دوربین‌هایِ مداربسته ، تحلیلِ کلان‌داده‌ها ، پایشِ ارتباطاتِ اینترنتی، و فناوری‌هایِ بیومتریک (مانندِ تشخیصِ چهره) جمع‌آوری می‌کند. هدفِ اعلام شده‌ی این نظارت‌ها، معمولاً افزایشِ امنیتِ عمومی، پیشگیری از جرایم، و مقابله با تروریسم عنوان می‌شود. با این حال، منتقدان بر این باورند که گستردگیِ این نظارت‌ها، پیامدهایِ ناگواری برایِ حقوقِ فردی و آزادی‌هایِ مدنی دارد (Clarke, 2010: 34).

یکی از مهم‌ترین پیامدها، «اثرِ ارعاب» است؛ به این معنا که آگاهیِ دائمیِ افراد از تحتِ نظارت بودن، آنان را به سمتِ خودسانسوری سوق می‌دهد. شهروندان ممکن است از بیانِ عقایدِ مخالف، شرکت در تجمعاتِ اعتراضی، یا حتی جستجو در موردِ موضوعاتِ حساس، خودداری کنند، مبادا که این اقدامات، آنان را در معرضِ سوءظنِ نهادهایِ امنیتی قرار دهد. این پدیده، که به تضعیفِ آزادی بیان و آزادیِ تجمعاتِ مسالمت‌آمیز منجر می‌شود، به طورِ مستقیم، ارزش‌هایِ دموکراتیک را به مخاطره می‌اندازد (کدخدایی، ۱۳۹۷: ۸۸).

در فضایِ عمومی، مفهومی به نام «انتظارِ معقول از حریم خصوصی» مطرح است. به طورِ سنتی، افراد انتظار دارند که در فضاهایِ خصوصیِ خود (مانندِ منزل)، از مصونیتِ بیشتری در برابرِ دخالتِ دیگران برخوردار باشند، اما در فضاهایِ عمومی، این انتظار، محدودتر است. با این حال، نظارتِ گسترده و دائمی، این تمایز را کمرنگ می‌سازد. اگر هر قدم، هر گفتگو، و هر تعاملِ ما در فضایِ عمومی، توسطِ دوربین‌ها یا الگوریتم‌ها ثبت و تحلیل شود، آیا هنوز می‌توان از وجودِ «فضایِ عمومیِ بدونِ نظارت» سخن گفت؟ (Nissenbaum, 2010: 56).

به نظر می‌رسد که «نظارتِ گسترده»، نه تنها «حریمِ خصوصی» را در فضایِ عمومی از بین نمی‌برد، بلکه آن را به شکلی بنیادین «دگرگون» می‌سازد. حریمِ خصوصی دیگر صرفاً به معنایِ مصونیت از تجسسِ مستقیم نیست، بلکه شاملِ کنترلِ فرد بر اطلاعاتِ مربوط به خود و جلوگیری از تجمیعِ نامحدودِ این اطلاعات توسطِ نهادهایِ قدرت است. در این معنا، حتی اگر فرد در یک پارک عمومی قدم بزند، انتظار دارد که این اقدام، لزوماً به ثبتِ دائمی، تحلیلِ جامع، و ایجادِ پروفایلی از عادات و علایقِ او منجر نشود.

چارچوب‌هایِ حقوقیِ موجود، مانندِ مقرراتِ مربوط به حفاظت از داده‌ها ، تلاش می‌کنند تا با تعیینِ قواعدی برایِ جمع‌آوری، پردازش، و نگهداریِ داده‌ها، حریمِ خصوصی را در برابرِ نظارتِ گسترده محافظت کنند. در اتحادیه اروپا، مقرراتِ عمومیِ حفاظت از داده‌ها (GDPR) یکی از مهم‌ترین دستاوردهایِ حقوقی در این زمینه محسوب می‌شود که بر اصولی چون ضرورت، تناسب، شفافیت، و محدودیتِ هدف تأکید دارد (Zuboff, ۲۰۱۹: ۳۳۵). این مقررات، اگرچه در وهله‌ی اول برایِ حفاظت از داده‌ها در فضایِ خصوصی تدوین شده‌اند، اما می‌توانند چارچوبی برایِ ارزیابیِ مشروعیتِ نظارتِ گسترده در فضاهایِ عمومی نیز فراهم آورند.

با این حال، چالشِ اصلی همچنان باقی است: چگونه می‌توان میانِ نیازِ مشروعِ دولت به ابزارهایِ نظارتی برایِ حفظِ امنیت، و حقِ بنیادینِ شهروندان بر حریمِ خصوصی و آزادی‌هایِ مدنی، تعادل برقرار کرد؟ پاسخِ قطعی به این پرسش، نیازمندِ بازنگریِ مداوم در قوانین، توسعه‌ی سازوکارهایِ نظارتیِ مستقل و مؤثر (به‌ویژه نظارتِ قضایی)، و افزایشِ آگاهیِ عمومی در موردِ پیامدهایِ نظارتِ گسترده است. بدونِ این تلاش‌ها، خطرِ فروپاشیِ تدریجیِ مفهومِ حریمِ خصوصی، و تبدیلِ جوامع به «دنیایِ تحتِ نظارتِ کامل»، امری دور از دسترس نخواهد بود.

اصلِ تناسب در اقداماتِ نظارتی پلیس

اصل تناسب (Proportionality)، به مثابه ستون فقرات مشروعیت‌بخشی به اختیارات محدودکننده‌ی دولت در حقوق عمومی، ایجاب می‌نماید که هرگونه اقدام اقتدارآمیز مقامات، از جمله پلیس، نه تنها دارای هدف مشروع باشد، بلکه شدت و گستره‌ی آن نیز باید در حد ضرورت برای دستیابی به آن هدف باقی بماند. در عصری که فناوری‌های دیجیتال، ابزارهای نظارتی پلیس را قادر به نفوذ در حریم خصوصی افراد با سرعتی بی‌سابقه ساخته‌اند، این پرسش بنیادین مطرح می‌گردد که آیا شدتِ این نظارت‌های دیجیتال، با میزانِ تهدیداتِ امنیتیِ واقعی و ملموس، تناسبی منطقی و حقوقی دارد؟ (کریمی، ۱۴۰۰: ۹۰).

فناوری‌های نوین نظارتی، از جمله سامانه‌های تشخیص چهره، پایش‌های پهپادی، تحلیل کلان‌داده‌ها ، و الگوریتم‌های پیش‌بینی جرم، قابلیت‌هایی را در اختیار پلیس قرار داده‌اند که می‌تواند منجر به شکل‌گیری «جامعه‌ی تحت نظارت» گردد. این ابزارها، اگر بدون رعایت اصل تناسب به کار گرفته شوند، می‌توانند به نقض گسترده‌ی حریم خصوصی شهروندان، ایجاد جوّ ارعاب و خودسانسوری، و در نهایت، تضعیف بنیادهای جامعه‌ی دموکراتیک منجر شوند. به عنوان مثال، به‌کارگیری گسترده‌ی سامانه‌های تشخیص چهره در تمامی اماکن عمومی، ممکن است در ظاهر به افزایش کشف جرایم یاری رساند، اما اگر این اقدام، بدون ارزیابی دقیق از ضرورت، ملاءمت، و سنجشِ میان منفعتِ حاصل از کشف جرم و زیان ناشی از نقض حریم خصوصی افراد بیگناه صورت پذیرد، اصل تناسب را نقض خواهد کرد (محمدی و احمدی، ۱۳۹۷: ۵۵).

برای اطمینان از رعایت اصل تناسب در اقدامات نظارتی پلیس، سه معیار کلیدی مورد بررسی قرار می‌گیرد: نخست، «ضرورت» ؛ بدین معنا که آیا توسل به ابزار نظارتیِ دیجیتال، برای دستیابی به هدف امنیتیِ مورد نظر، تنها راه ممکن است و ابزارهای کم‌تهاجمی‌تر برای رسیدن به همان نتیجه وجود ندارد؟ دوم، «ملاءمت» ؛ یعنی آیا ابزار نظارتیِ به‌کارگرفته شده، واقعاً قادر به تحقق هدف امنیتی اعلام شده است و رابطه‌ی منطقی و سببی میان ابزار و هدف وجود دارد؟ و سوم، «تناسبِ سنجیده» ؛ که در آن، منافع حاصل از اقدام نظارتی (مانند حفظ امنیت عمومی یا پیشگیری از جرایم جدی) باید بر زیان‌های ناشی از آن (مانند نقض حریم خصوصی، تحمیل هزینه‌های اقتصادی، و ایجاد تبعات روانی و اجتماعی) برتری داشته باشد (قاسمی، ۱۴۰۰: ۱۱۲).

در عمل، تحقق این معیارها، به‌ویژه در مواجهه با تهدیدات امنیتیِ احتمالی یا کلی، چالش‌برانگیز است. نهادهای امنیتی و پلیسی غالباً بر ضرورتِ اقدامات خود ذیل عنوان «حفظ نظم و امنیت عمومی» تأکید می‌ورزند، اما این ادعا باید با شواهد و قرائنِ کافی مبنی بر وجود تهدیدِ واقعی و متناسب با شدتِ نظارتِ اعمال شده، همراه باشد. به عنوان مثال، صرفِ ادعای مبارزه با «جرایم سایبری» به صورت کلی، نمی‌تواند توجیهی برای نظارتِ فراگیر و بدون تفکیک بر کلیه‌ی ارتباطات اینترنتی شهروندان باشد. قانون‌گذار باید در قوانین، چارچوب‌های دقیقی برای تحدید این اختیارات تعیین نماید تا از سوءاستفاده‌ی احتمالی جلوگیری شود (حبیبی، ۱۴۰۰: ۷۸).

اگرچه ممکن است در برخی موارد، فناوری‌های نظارتی دیجیتال، ابزارهای کارآمدی برای مقابله با تهدیدات امنیتیِ جدی و سازمان‌یافته باشند، اما توسل به آن‌ها باید همواره تابع قواعد حقوقی و اصول بنیادین باشد. در این راستا، مطالعه‌ی تطبیقی و بهره‌گیری از تجربیات نظام‌های حقوقی پیشرو، مانند اتحادیه اروپا، که با وضع مقرراتی چون ، چارچوب‌های سخت‌گیرانه‌ای برای جمع‌آوری و پردازش داده‌های شخصی وضع کرده‌اند،

می‌تواند راهگشا باشد. این مقررات، بر لزوم تناسب میان هدف و ابزار، و رعایت اصل حداقل داده تأکید دارند (رایجیان اصلی، ۱۳۹۸: ۱۵۰).

از منظر نگارنده، چالش اساسی در اعمال اصل تناسب بر نظارت‌های دیجیتال پلیس، عبور از کلی‌گویی در تعریف تهدیدات امنیتی و ارائه‌ی سازوکارهای شفاف و قابل راستی‌آزمایی برای اطمینان از تناسبِ میان شدتِ نظارت و میزانِ تهدیدِ واقعی است. این امر نیازمند شفافیتِ هرچه بیشترِ نهادهای امنیتی در خصوص فناوری‌های مورد استفاده، حدود اختیارات پلیس، و وجود سازوکارهای نظارتیِ مؤثر، به‌ویژه نظارتِ قضاییِ مستقل و بی‌طرف، می‌باشد. بدون چنین سازوکارهایی، خطرِ تبدیل شدنِ فناوری‌های نظارتی به ابزاری برای نقضِ گسترده‌ی حقوق بنیادین شهروندان، تحت لوای حفظ امنیت، همواره وجود خواهد داشت (پوربافر، ۱۳۹۷: ۶۵).

تحلیلِ تقابلِ امنیتِ جمعی و حقوقِ بنیادینِ شهروندی

یکی از منازعات بنیادین در فلسفه‌ی حقوق عمومی و سیاست‌گذاری جنایی، تنشِ دائمی میان ضرورتِ حفظ «امنیت جمعی» و صیانت از «حقوق بنیادین شهروندی» است. پلیس، به عنوان بازوی اجرایی دولت، وظیفه‌ی خطیرِ تأمین امنیت و نظم عمومی را بر عهده دارد؛ وظیفه‌ای که غالباً مستلزم اعمال محدودیت‌هایی بر برخی از آزادی‌های فردی، از جمله حق بر حریم خصوصی و آزادی رفت‌وآمد، می‌باشد. این تقابل، به ویژه در عصر حاضر که فناوری‌های نوین، امکان نظارت و مداخله در حریم خصوصی افراد را به سطوح بی‌سابقه‌ای گسترش داده‌اند، اهمیت و پیچیدگی بیشتری یافته است. درک این تنش، مستلزم واکاویِ عمیقِ مبانی حقوقی و فلسفی هر دو سوی این معادله است (رضایی، ۱۳۹۸: ۷۵).

حق بر «امنیت» به عنوان یکی از کارکردهای اساسی دولت، صرفاً به معنای فقدانِ هرج‌ومرج و آسایش ظاهری نیست، بلکه شامل حفاظت از جان، مال، و کرامت انسانی شهروندان در برابر تهدیداتِ داخلی و خارجی نیز می‌شود. دولت‌ها، از جمله پلیس، برای ایفای این وظیفه، از اختیاراتی نظیر بازرسی، توقیف، شنود، و محدودسازیِ موقتِ دسترسی به برخی اماکن یا اطلاعات برخوردارند. این اختیارات، در صورتی که بر مبنای قانونی صریح، با هدفِ مشروعِ حفظ امنیت، و به صورت متناسب اعمال شوند، می‌توانند مشروع تلقی گردند (کاتوزیان، ۱۳۹۹: ۲۱۲). با این حال، توسل به «امنیت» نباید به بهانه‌ای برای نادیده گرفتنِ حقوق بنیادین شهروندان تبدیل شود.

در مقابل، حقوق بنیادین شهروندی، از جمله حق بر «حریم خصوصی» و «آزادی رفت‌وآمد» ، به مثابه سنگ بنای جوامع دموکراتیک، از جایگاهی والا برخوردارند. حق بر حریم خصوصی، که شامل مصونیتِ فرد از تجسسِ بی‌اجازه‌ی دولت در زندگی شخصی، خانوادگی، و ارتباطات اوست، یکی از مهم‌ترین ارکانِ کرامت انسانی و آزادی فردی محسوب می‌شود. به همین ترتیب، آزادی رفت‌وآمد، به معنای حقِ هر فرد بر ترکِ تابعیتِ خود، خروج از کشور، ورود به کشور، و همچنین حقِ اقامت و تعیین محل سکونت در داخلِ کشور، از اصولِ مسلمِ حقوق بشر است (گریفیث، ۲۰۱۸: ۴۵).

تنش میان این دو مقوله، زمانی آشکارتر می‌شود که اقدامات پلیسی برای حفظ امنیت، به مداخله در حریم خصوصی یا محدودسازیِ غیرضروریِ آزادی رفت‌وآمد منجر گردد. به عنوان مثال، نصب دوربین‌های نظارتیِ گسترده در معابر عمومی، اجرای طرح‌های ایست بازرسیِ مستمر و بدون تفکیک، یا اعمال محدودیت‌های پروازی و مرزی در شرایطی که ضرورتی واقعی برای آن وجود ندارد، نمونه‌هایی از اقداماتی هستند که می‌توانند این تقابل را برجسته سازند. در چنین مواردی، وظیفه‌ی پلیس در حفظ امنیت، نباید به قیمتِ سلبِ بی‌رویه یا نامتناسبِ حقوق بنیادین شهروندان تمام شود. اصل تناسب در اینجا نقشِ حیاتی ایفا می‌کند و ایجاب می‌نماید که هرگونه محدودیت بر حقوق فردی، صرفاً در حدِ ضرورتِ مطلق برای تأمینِ امنیتِ جمعی، و با کمترین میزانِ مداخله، اعمال گردد (حبیب‌زاده، ۱۳۹۹: ۱۸۰).

در حقوق ایران، قانون اساسی، به صراحت، ضمن تأکید بر حقوق بنیادین شهروندان، از جمله حق مصونیتِ اقامتگاه (اصل ۲۲)، حق بر حریم خصوصی مکاتبات (اصل ۲۵)، و آزادی رفت‌وآمد (ذیل اصل ۴۳)، تنها در مواردِ خاص و به موجب قانون، اجازه‌ی محدودسازی این حقوق را برای حفظ نظم عمومی و یا در مقامِ اجرایِ حدود و مقرراتِ قانونی (مانند احکام قضایی) صادر نموده است. این بدان معناست که هرگونه مداخله‌ی پلیس در این حقوق، جز در چارچوبِ قانون و با رعایتِ تشریفاتِ مقرر، فاقد مشروعیت بوده و نقضِ صریحِ قانون اساسی تلقی می‌گردد (مرکز پژوهش‌های مجلس شورای اسلامی، ۱۴۰۰: ۳۰).

از منظر نگارنده، راهبردی‌ترین رویکرد در مدیریت این تنش، اتخاذِ سیاستی است که ضمن تضمینِ حداکثریِ امنیتِ جمعی، کمترین تعدی را به حقوق بنیادین شهروندان روا دارد. این امر مستلزم شفافیتِ حداکثریِ نهادهای امنیتی و پلیسی در خصوصِ اقداماتِ نظارتی و محدودیت‌های اعمالی، وجودِ سازوکارهایِ مؤثرِ نظارتی (به‌ویژه نظارتِ قضاییِ مستقل)، و همچنین پذیرشِ مسئولیتِ احتمالیِ نهادهای امنیتی در قبالِ نقضِ ناروای حقوق

شهروندان است. صرفِ استناد به «امنیت» به عنوان یک مفهومِ کلی و انتزاعی، نمی‌تواند توجیهی برای نادیده گرفتنِ حقوقِ مکتسب و بنیادینِ افراد در یک جامعه‌ی قانون‌مدار باشد (Sornarajah, 2017: 115).

چالشِ «شفافیت» و «پاسخگویی» در عملیات پلیسِ هوشمند

گذارِ پلیس به استفاده از فناوری‌هایِ هوشمند، از جمله الگوریتم‌هایِ پیش‌بینیِ جرم و سامانه‌هایِ تشخیصِ چهره، گرچه وعده‌یِ افزایشِ کارایی و دقت در عملیاتِ انتظامی را می‌دهد، اما چالش‌هایِ عمیقی را در عرصه‌هایِ «شفافیت» و «پاسخگویی» پدید آورده است. پرسشِ کلیدی این است که هنگامی که تصمیم‌گیری در موردِ شناساییِ افرادِ مشکوک یا ارزیابیِ ریسکِ وقوعِ جرم، به الگوریتم‌ها واگذار می‌شود، سازوکارهایِ سنتیِ پاسخگوییِ پلیس در برابرِ خطاها و سوءاستفاده‌هایِ احتمالی، چگونه باید بازتعریف شوند؟ (صفاری، ۱۳۹۸: ۱۱۰).

یکی از بزرگترین موانعِ موجود در این زمینه، «ابهامِ ذاتیِ الگوریتم‌ها» یا «جعبه‌یِ سیاه بودن» آن‌هاست. بسیاری از این الگوریتم‌ها، به‌ویژه آن‌هایی که بر پایه‌یِ یادگیریِ ماشینی بنا شده‌اند، به گونه‌ای پیچیده عمل می‌کنند که حتی توسعه‌دهندگانِ اولیه‌یِ آن‌ها نیز قادر به تبیینِ دقیقِ منطقِ تصمیم‌گیریِ جزئیِ الگوریتم در هر موردِ خاص نیستند. این فقدانِ شفافیت، امرِ بازرسیِ مستقلِ این الگوریتم‌ها توسطِ نهادهایِ نظارتی یا قضایی را به شدت دشوار می‌سازد و پرسشگری در موردِ مبنایِ شناساییِ یک فرد به عنوانِ «مشکوک» را با موانعِ جدی مواجه می‌کند (محمدی و احمدی، ۱۳۹۷: ۷۵).

پیامدِ مستقیمِ این ابهام، چالش در تعیینِ «مسئولیتِ حقوقی» است. در نظام‌هایِ حقوقیِ سنتی، هنگامی که خطایی از سویِ پلیس سر می‌زند (مانندِ بازداشتِ اشتباهی یا استفاده‌یِ بیش از حد از زور)، مسئولیتِ فردی یا سازمانیِ مشخصی قابلِ تعیین است. اما در موردِ خطاهایِ ناشی از الگوریتم‌ها، این امر پیچیده‌تر می‌شود: آیا مسئولیت متوجهِ برنامه‌نویسِ الگوریتم است؟ شرکتِ سازنده‌یِ نرم‌افزار؟ یا نهادی که الگوریتم را به کار گرفته است؟ و یا شاید خودِ «الگوریتم» به عنوانِ یک عاملِ مستقل در نظر گرفته شود؟ (کاپل، ۲۰۰۵: ۱۸۰).

علاوه بر این، الگوریتم‌ها، مانندِ هر داده‌ای که بر اساسِ آن آموزش دیده‌اند، می‌توانند «سوگیری» را بازتولید و حتی تشدید کنند. اگر داده‌هایِ تاریخیِ موردِ استفاده برایِ آموزشِ الگوریتم، منعکس‌کننده‌یِ تبعیض‌هایِ نژادی، اجتماعی، یا اقتصادیِ موجود در جامعه باشند (مانندِ شیوه‌هایِ سنتیِ اعمالِ قانون که ممکن است گروه‌هایِ خاصی را بیش از حد هدف قرار داده باشند)، الگوریتمِ حاصل، این تبعیض‌ها را در تصمیم‌گیری‌هایِ

خود لحاظ خواهد کرد. این امر می‌تواند به ایجادِ چرخه‌هایِ معیوبِ تبعیضِ الگوریتمیک منجر شود، جایی که گروه‌هایِ اقلیت به طورِ نامتناسبی به عنوانِ «مشکوک» شناسایی شده و تحتِ نظارتِ شدیدتر قرار گیرند، بدونِ آنکه مبنایِ این طبقه‌بندی، شفاف یا قابلِ دفاع باشد (résident, 2021: 67).

برایِ مقابله با این چالش‌ها، رویکردهایِ مختلفی در حالِ بررسی و اجرا هستند. نخست، «الزام به شفافیتِ الگوریتمی»؛ بدین معنا که نهادهایِ پلیسی ملزم شوند تا در موردِ الگوریتم‌هایی که به کار می‌گیرند، اطلاعاتِ کافی (هرچند نه لزوماً کدِ منبعِ کامل) را در موردِ منطقِ عملکرد، داده‌هایِ موردِ استفاده، و معیارهایِ ارزیابیِ ریسک، در اختیارِ نهادهایِ نظارتی و قضایی قرار دهند. دوم، «ارزیابیِ مستقلِ الگوریتم‌ها»؛ تأسیسِ نهادهایی که بتوانند پیش از به‌کارگیریِ رسمیِ این فناوری‌ها، عملکردِ آن‌ها را از منظرِ دقت، بی‌طرفی، و رعایتِ حقوقِ شهروندی موردِ سنجش قرار دهند.

سوم، «تدوینِ معیارهایِ حقوقیِ مشخص برایِ مسئولیت»؛ قانون‌گذاران باید چارچوب‌هایِ روشنی را برایِ تعیینِ مسئولیتِ ناشی از خطاهایِ الگوریتمی تدوین کنند که شاملِ مسئولیتِ مدنی، کیفری، و اداریِ احتمالیِ توسعه‌دهندگان، تأمین‌کنندگان، و کاربرانِ این فناوری‌ها باشد. این امر، ضمنِ تضمینِ جبرانِ خسارت برایِ زیان‌دیدگان، می‌تواند انگیزه‌ای برایِ توسعه و به‌کارگیریِ مسئولانه‌ترِ این فناوری‌ها فراهم آورد. در نهایت، «نظارتِ مستمر و تطبیقی»؛ با توجه به ماهیتِ پویا و در حالِ تحولِ فناوری‌هایِ هوشمند، نیاز به سازوکارهایِ نظارتیِ مستمر و قابلیتِ انطباقِ قوانین و مقررات با پیشرفت‌هایِ فناورانه، امری ضروری است (Reid, 2020: ۹۰).

صلاحیتِ قانونیِ پلیس در جمع‌آوری داده‌های بیومتریک

جمع‌آوری و پردازشِ داده‌هایِ بیومتریک ، که شاملِ اطلاعاتِ منحصربه‌فردِ فیزیولوژیکی یا رفتاریِ افراد مانندِ اثرِ انگشت، چهره، عنبیه‌یِ چشم، یا الگوهایِ صدا می‌شود، به یکی از ابزارهایِ کلیدیِ نهادهایِ انتظامی و امنیتی در عصرِ دیجیتال بدل گشته است. این فناوری‌ها، پتانسیلِ بالایی برایِ شناساییِ افراد، کشفِ جرایم، و تأمینِ امنیتِ عمومی دارند. با این حال، ماهیتِ حساس و غیرقابلِ تغییرِ این داده‌ها، چالش‌هایِ حقوقیِ قابلِ توجهی را در خصوصِ «صلاحیتِ قانونیِ پلیس» برایِ جمع‌آوری، ذخیره‌سازی، و استفاده از آن‌ها پدید آورده است. پرسشِ اساسی این است که حدود و ثغورِ این اختیارات تا کجاست و چگونه می‌توان از سوءاستفاده از این داده‌ها جلوگیری کرد؟ (پوربافر، ۱۳۹۷: ۹۵).

در نظامِ حقوقیِ ایران، اصلِ کلی حاکم بر جمع‌آوریِ اطلاعاتِ فردی، از جمله داده‌هایِ بیومتریک، اصلِ «قانونی بودنِ جرم و مجازات» و اصلِ «حفظِ حریمِ خصوصی» است که در قانونِ اساسی (اصول ۲۲، ۲۵، و ۳۲) موردِ تأکید قرار گرفته‌اند. بر این اساس، هرگونه مداخله در حریمِ خصوصیِ افراد، از جمله جمع‌آوریِ داده‌هایِ بیومتریک، باید مستند به قانون، دارایِ هدفِ مشروع، و در چارچوبِ ضرورت و تناسب باشد. پلیس به طورِ کلی، در چارچوبِ تحقیقاتِ کیفری و به موجبِ دستورِ قضایی، می‌تواند اقدام به جمع‌آوریِ برخی داده‌هایِ بیومتریکِ متهمان یا مجرمان نماید.

قانونِ آیینِ دادرسیِ کیفری، در مواردی مانندِ اخذِ اثرِ انگشت از متهمان، گرفتنِ عکس از آنان، و در صورتِ لزوم، اخذِ نمونه‌هایِ دیگرِ بیومتریک، در چارچوبِ تحقیقاتِ مقدماتی، اختیاراتی را به بازپرس یا قاضیِ تحقیق اعطا کرده است که پلیس مجریِ آن است. همچنین، در برخی قوانینِ خاص، مانندِ قانونِ گذرنامه یا قوانینِ مربوط بهِ ورود و خروجِ اتباعِ خارجی، مقرراتی در خصوصِ اخذِ داده‌هایِ بیومتریک (مانندِ اثرِ انگشت و تصویرِ چهره) برایِ مقاصدِ کنترلی و امنیتی پیش‌بینی شده است (مرکز پژوهش‌های مجلس شورای اسلامی، ۱۴۰۰: ۴۵).

با این حال، چالشِ اصلی در خصوصِ «نظارتِ گسترده» و جمع‌آوریِ داده‌هایِ بیومتریک از شهروندانِ عادی و «غیرِ مشکوک» است. آیا پلیس صلاحیت دارد به طورِ سیستمی و دائمی، چهره‌یِ شهروندان را در اماکنِ عمومی با استفاده از سامانه‌هایِ تشخیصِ چهره ثبت و ذخیره کند، یا اثرِ انگشتِ تمامِ اتباعِ بالایِ سنِ قانونی را در پایگاه‌هایِ داده‌یِ خود نگهداری نماید، صرفاً با این توجیهِ کلی که «این اقدام ممکن است در آینده برایِ کشفِ جرم مفید باشد»؟ اغلبِ نظام‌هایِ حقوقیِ پیشرفته، چنین اقداماتی را بدونِ داشتنِ دستورِ قضاییِ مشخص، یا عدمِ وجودِ مظنونیتِ معقول، غیرِ قانونی و مغایر با حقِ حریمِ خصوصی می‌دانند.

مفهومِ «داده‌هایِ حساسِ بیومتریک» در برخی نظام‌هایِ حقوقی، مانندِ در اتحادیه اروپا، اهمیتِ ویژه‌ای دارد. این داده‌ها، به دلیلِ قابلیتِ شناساییِ قطعیِ فرد و ماهیتِ غیرقابلِ تغییرشان، مشمولِ حمایت‌هایِ شدیدتری هستند و جمع‌آوری و پردازشِ آن‌ها تنها در شرایطِ استثنایی و با رضایتِ صریحِ فرد یا وجودِ ضرورتِ قانونیِ قوی مجاز است (Mell, 2017: 78). در حقوقِ ایران، اگرچه تفکیکِ صریحی تحتِ این عنوان وجود ندارد، اما اصلِ لزومِ وجودِ دستورِ قضایی و هدفِ مشخص برایِ جمع‌آوریِ داده‌ها، همچنان لازم‌الرعایه است.

چالشِ دیگر، «ذخیره‌سازیِ بلندمدت» و «امنیتِ پایگاه‌هایِ داده‌یِ بیومتریک» است. حجمِ عظیمِ داده‌هایِ بیومتریک که توسطِ پلیس یا سایرِ نهادها جمع‌آوری می‌شود، هدفِ جذابی برایِ هکرها و مجرمانِ سایبری محسوب می‌گردد. نقضِ امنیتیِ این پایگاه‌ها می‌تواند منجر به افشایِ اطلاعاتِ حیاتیِ میلیون‌ها شهروند و سوءاستفاده‌هایِ گسترده، از جمله سرقتِ هویت، شود. بنابراین، پلیس نه تنها باید صلاحیتِ قانونیِ جمع‌آوریِ این داده‌ها را داشته باشد، بلکه مکلف است تدابیرِ امنیتیِ لازم را برایِ حفاظتِ فیزیکی و سایبریِ این اطلاعات اتخاذ نماید.

در نهایت، «هدفمندی» یکی از اصولِ بنیادین در پردازشِ داده‌هایِ بیومتریک است. داده‌هایِ جمع‌آوری شده برایِ یک منظورِ خاص (مانندِ شناساییِ مظنون در یک پرونده‌یِ کیفری)، نباید بدونِ مجوزِ قانونیِ جدید، برایِ مقاصدِ دیگر (مانندِ نظارتِ عمومیِ دائمی) موردِ استفاده قرار گیرند. تعیینِ شفافِ اهدافِ جمع‌آوریِ داده‌هایِ بیومتریک توسطِ پلیس، و وجودِ سازوکارهایِ نظارتی برایِ اطمینان از رعایتِ این اصل، امری حیاتی است.

نظارت قضایی بر عملیاتِ فنی پلیس؛ ضامنِ عدالت یا مانعِ سرعت

پیشرفت‌هایِ شگرف در حوزه‌یِ فناوری، ابزارهایِ قدرتمندی را در اختیارِ نهادهایِ انتظامی و امنیتی قرار داده است؛ ابزارهایی که توانایِ جمع‌آوریِ اطلاعاتِ گسترده و ظریف از شهروندان را فراهم می‌آورند. سامانه‌هایِ شنودِ پیشرفته، نرم‌افزارهایِ تحلیلِ داده‌هایِ کلان، فناوریِ تشخیصِ چهره، پهپادهایِ نظارتی، و ابزارهایِ نفوذ به سیستم‌هایِ رایانه‌ای، تنها بخشی از این فناوری‌هایِ نوین هستند. در حالی که این ابزارها می‌توانند در کشفِ جرایمِ پیچیده و تأمینِ امنیتِ عمومی بسیار مؤثر باشند، اما در عینِ حال، پتانسیلِ بالایی برایِ نقضِ حقوقِ بنیادینِ شهروندان، به‌ویژه حقِ حریمِ خصوصی، را نیز دارا هستند. در این میان، پرسشِ کلیدی این است که «نظارتِ قضایی» بر استفاده از این عملیاتِ فنیِ پلیس، چه جایگاهی دارد؟ آیا این نظارت، ضامنی برایِ اجرایِ عدالت و حفظِ حقوقِ شهروندی است، یا مانعی در برابرِ سرعتِ عملِ پلیس در مقابله با تهدیداتِ امنیتی؟ (Randel, ۲۰۱۶: ۵۵).

در اکثرِ نظام‌هایِ حقوقیِ مدرن، از جمله نظامِ حقوقیِ ایران، اصل بر این است که پلیس برایِ انجامِ تحقیقاتِ فنیِ مداخله‌جویانه، مانندِ شنودِ مکالمات، بازرسیِ منازل، یا دسترسی به داده‌هایِ ارتباطیِ افراد، نیازمندِ اخذِ مجوزِ قضایی است. این اصل، ریشه در ضرورتِ تفکیکِ قوا و لزومِ وجودِ یک مرجعِ بی‌طرف و مستقل (قوه قضاییه) برایِ مجوز دادن به اقداماتی دارد که حقوقِ بنیادینِ شهروندان را محدود می‌کنند. هدف از این مجوزِ

قضایی، اطمینان از این است که مداخلاتِ پلیس، «ضروری»، «متناسب»، و «مستند به دلایلِ کافی» باشد. این امر، از تبدیلِ اختیاراتِ پلیس به ابزاری برایِ خودکامگی و نظارتِ فراگیر و بی‌رویه جلوگیری می‌کند (Griffith, ۲۰۱۸: ۱۲۰).

ضرورتِ اخذِ مجوزِ قضایی برایِ استفاده از ابزارهایِ نظارتیِ نوین، به دلایلِ متعددی قابلِ توجیه است:

۱. حفاظت از حریمِ خصوصی: داده‌هایِ بیومتریک، ارتباطاتِ خصوصی، و اطلاعاتِ شخصیِ افراد، هسته‌یِ اصلیِ حقِ حریمِ خصوصی را تشکیل می‌دهند. استفاده از ابزارهایِ نظارتیِ نوین، مانندِ سامانه‌هایِ تشخیصِ چهره در اماکنِ عمومی یا دسترسی به تاریخچه‌یِ مرورِ اینترنت، بدونِ مجوزِ قضایی، نقضِ آشکارِ این حق محسوب می‌شود. مجوزِ قضایی، تضمین می‌کند که این مداخلات، تنها در مواردِ استثنایی و برایِ اهدافِ بسیار جدی (مانندِ مبارزه با جرایمِ سازمان‌یافته یا تروریسم) صورت پذیرد.

۲. اصلِ تناسب (Proportionality): ابزارهایِ نظارتیِ نوین، به دلیلِ توانایی جمع‌آوریِ اطلاعاتِ گسترده، ممکن است تناسبِ لازم را با تهدیدِ امنیتیِ موجود نداشته باشند. مجوزِ قضایی، به قاضی اجازه می‌دهد تا شدتِ مداخله را با جرمی که تحقیق در موردِ آن جریان دارد، بسنجد و اطمینان حاصل کند که پلیس از ابزارهایِ نامتناسب یا بیش از حدِ مداخله‌جویانه استفاده نمی‌کند (Schulz, 2023: 45).

۳. مقابله با سوگیریِ الگوریتمی و تبعیض: بسیاری از ابزارهایِ نظارتیِ نوین، بر پایه‌یِ الگوریتم‌ها عمل می‌کنند که ممکن است دچارِ سوگیری (Bias) باشند و گروه‌هایِ خاصی از جامعه را به طورِ نامتناسبی هدف قرار دهند. نظارتِ قضایی می‌تواند به عنوانِ یک لایه‌یِ دفاعی در برابرِ این سوگیری‌ها عمل کند، به این معنا که قاضی پیش از صدورِ مجوز، ممکن است در موردِ دقت و بی‌طرفیِ الگوریتمِ موردِ نظر، پرس‌وجو کند.

۴. ایجادِ اعتبارِ شواهدِ جمع‌آوری شده: شواهدی که از طریقِ عملیاتِ فنیِ غیرِ قانونی و بدونِ مجوزِ قضایی به دست آمده باشند، در بسیاری از نظام‌هایِ حقوقی، «مسموع» (Inadmissible) تلقی شده و قابلِ استناد در دادگاه نخواهند بود. اخذِ مجوزِ قضایی، اعتبارِ قانونیِ شواهدِ جمع‌آوری شده را تضمین می‌کند و از تضعیفِ روندِ عدالت جلوگیری می‌نماید.

در مقابلِ این استدلال‌ها، گاهی این نگرانی مطرح می‌شود که فرآیندِ اخذِ مجوزِ قضایی، زمان‌بر بوده و می‌تواند منجر به «مانعِ سرعت» در عملیاتِ پلیس گردد، به‌ویژه در شرایطِ اضطراری یا زمانی که نیاز به واکنشِ سریع

وجود دارد. این امر می‌تواند به از دست رفتنِ فرصتِ کشفِ جرم، فرارِ مجرمان، یا از بین رفتنِ شواهدِ حیاتی منجر شود.

برایِ رفعِ این نگرانی، بسیاری از نظام‌هایِ حقوقی، سازوکارهایی را پیش‌بینی کرده‌اند:

- مجوزهایِ اضطراری: در مواردِ استثنایی و با اثباتِ ضرورتِ اقدامِ فوری، پلیس ممکن است بتواند عملیاتِ فنیِ محدودی را بدونِ مجوزِ قبلی انجام دهد، مشروط بر اینکه بلافاصله پس از آن (مثلاً ظرفِ ۲۴ یا ۴۸ ساعت) نسبت به اخذِ تأییدیه یا مجوزِ قضاییِ بعدی اقدام نماید. عدمِ اخذِ تأییدیه، می‌تواند منجر به غیرِ قانونی تلقی شدنِ شواهدِ جمع‌آوری شده گردد.
- تعریفِ شفافِ حدودِ اختیارات: قانون‌گذاریِ روشن در خصوصِ اینکه کدام‌یک از ابزارهایِ نظارتی، نیازمندِ مجوزِ قضاییِ قبلی هستند و کدام‌یک (مانندِ مشاهده‌یِ عمومیِ فضاهایِ باز) در صلاحیتِ کلیِ پلیس قرار دارند، به رفعِ ابهام کمک می‌کند.
- فرآیندهایِ سریعِ صدورِ مجوز: قوه قضاییه می‌تواند با ایجادِ سازوکارهایِ الکترونیکی یا خطوطِ ارتباطیِ ویژه، فرآیندِ صدورِ مجوز را تسریع بخشد، بدونِ آنکه الزاماتِ محتواییِ آن (مانندِ اثباتِ دلیلِ کافی) نادیده گرفته شود.

در عصرِ دیجیتال، توانایی پلیس برایِ جمع‌آوری، پردازش، و تحلیلِ حجمِ عظیمی از داده‌هایِ شهروندان، از طریقِ فناوری‌هایِ نوینِ نظارتی، قدرتِ قابلِ توجهی را به این نهادها بخشیده است. این قدرت، اگرچه می‌تواند در راستایِ تأمینِ امنیتِ عمومی و مبارزه با جرایمِ پیچیده مفید باشد، اما پتانسیلِ بالایی برایِ نقضِ حقوقِ بنیادین، به‌ویژه حقِ حریمِ خصوصی و حفاظت از داده‌هایِ شخصی، را نیز در خود دارد. نظام‌هایِ حقوقیِ پیشرو، در مواجهه با این چالش، تلاش کرده‌اند تا با وضعِ مقرراتِ سخت‌گیرانه در زمینه‌یِ حفظِ داده‌ها، قدرتِ پلیس را مهار کرده و از سوءاستفاده‌هایِ احتمالی جلوگیری نمایند. «مقرراتِ عمومیِ حفاظت از داده‌ها» (در اتحادیه اروپا، به عنوانِ یکی از جامع‌ترین و تأثیرگذارترین چارچوب‌هایِ قانونی در این زمینه، نمونه‌ای برجسته از این تلاش‌هاست. (Danner, 2018: 76).

اصولِ بنیادینِ GDPR و کاربردِ آن در نظارتِ پلیسی بر پایه‌یِ اصولی استوار است که محدودیت‌هایِ مهمی را بر پردازشِ داده‌هایِ شخصی، از جمله توسطِ نهادهایِ انتظامی، اعمال می‌کند:

قانونی بودن، انصاف و شفافیت (Lawfulness, Fairness, and Transparency): هرگونه پردازشِ داده‌هایِ شخصی باید مبنایِ قانونیِ مشخصی داشته باشد، منصفانه صورت گیرد، و افراد از نحوه‌یِ پردازشِ اطلاعاتِ خود آگاه باشند. این اصل، پلیس را ملزم می‌کند تا دلایلِ قانونیِ روشنی برایِ جمع‌آوری و استفاده از داده‌هایِ شهروندان، به‌ویژه داده‌هایِ حساسِ بیومتریک یا ارتباطاتِ خصوصی، داشته باشد و این رویه‌ها را تا حدِ امکان شفاف سازد.

محدودیتِ هدف (Purpose Limitation): داده‌هایِ شخصی باید برایِ اهدافِ مشخص، صریح، و مشروع جمع‌آوری شده و نباید به گونه‌ای پردازش شوند که با آن اهداف مغایرت داشته باشد. این اصل، از استفاده‌یِ پلیس از داده‌هایِ جمع‌آوری شده برایِ یک منظورِ خاص (مانندِ تحقیقاتِ کیفری)، در مقاصدِ دیگر (مانندِ نظارتِ عمومیِ فراگیر) بدونِ مبنایِ قانونیِ جدید، جلوگیری می‌کند.

حداقل‌سازیِ داده (Data Minimisation): داده‌هایِ پردازش شده باید مناسب، مرتبط، و محدود به آن چیزی باشند که برایِ دستیابی به اهدافِ پردازش، ضروری است. این اصل، پلیس را تشویق می‌کند تا تنها داده‌هایی را جمع‌آوری کند که به طورِ مستقیم برایِ تحقیقاتِ ضروری هستند و از جمع‌آوریِ داده‌هایِ اضافی و غیرِ مرتبط پرهیز نماید.

دقت (Accuracy): داده‌هایِ شخصی باید دقیق و در صورتِ لزوم، به‌روز باشند. داده‌هایِ نادرست باید بدونِ تأخیرِ موجه، اصلاح یا پاک شوند. این امر، اهمیتِ صحتِ اطلاعاتِ جمع‌آوری شده توسطِ پلیس، به‌ویژه در سامانه‌هایِ تشخیصِ چهره یا تحلیلِ داده، را دوچندان می‌کند.

محدودیتِ نگهداری (Storage Limitation): داده‌هایِ شخصی نباید بیش از حدِ لازم برایِ اهدافِ پردازش، نگهداری شوند. این اصل، پلیس را ملزم می‌کند تا سیاست‌هایِ روشنی برایِ دوره‌یِ نگهداریِ داده‌هایِ جمع‌آوری شده (مانندِ اثرِ انگشت یا تصاویرِ ویدئویی) تدوین کرده و پس از انقضایِ مدتِ قانونی، نسبت به حذفِ یا بی‌نام‌سازیِ آن‌ها اقدام کند.

یکپارچگی و محرمانگی (Integrity and Confidentiality): داده‌هایِ شخصی باید به گونه‌ای پردازش شوند که امنیتِ آن‌ها تضمین گردد، از جمله حفاظت در برابرِ پردازشِ غیرِ مجاز یا از دست رفتنِ ناخواسته‌یِ داده‌ها. این اصل، مسئولیتِ پلیس را در قبالِ حفاظتِ سایبری و فیزیکی از پایگاه‌هایِ داده‌یِ اطلاعاتِ حساسِ شهروندان، برجسته می‌سازد.

۲. استثنائاتِ مرتبط با اجرایِ قانون در نظر گرفته است که اجرایِ قانون، یکی از حوزه‌هایی است که ممکن است نیاز به پردازشِ داده‌هایِ شخصی فراتر از اصولِ کلی داشته باشد. با این حال، حتی در این موارد نیز، محدودیت‌هایِ مهمی اعمال می‌شود:

- وجودِ مبنایِ قانونیِ مشخص: پردازشِ داده‌ها توسطِ پلیس باید بر اساسِ یک مبنایِ قانونیِ الزام‌آور در سطحِ اتحادیه اروپا یا کشورهایِ عضو صورت گیرد.
- ضرورت و تناسب: اقداماتِ پردازشی باید ضروری و متناسب با هدفِ مشخصِ اجرایِ قانون (مانندِ پیشگیری، تحقیق، کشف، یا تعقیبِ جرایمِ کیفری) باشد.
- تدابیرِ حمایتی: مقرراتِ GDPR، کشورهایِ عضو را ملزم می‌کند تا تدابیرِ حقوقی و فنیِ مناسبی را برایِ حفاظت از حقوق و آزادی‌هایِ افراد، از جمله حقِ دسترسی به داده‌ها و حقِ اعتراض، پیش‌بینی کنند.

مطالعه‌یِ موردی: GDPR و نظارتِ پلیسی در عمل:

- تشخیصِ چهره در اماکنِ عمومی: استفاده از فناوریِ تشخیصِ چهره توسطِ پلیس، به طورِ گسترده‌ای در کشورهایِ عضو GDPR تحتِ نظارتِ دقیق قرار دارد. در بسیاری از موارد، جمع‌آوریِ گسترده و پردازشِ داده‌هایِ چهره‌یِ شهروندانِ عادی بدونِ رضایتِ صریح یا مبنایِ قانونیِ قوی، ممنوع است. برخی کشورها، مانندِ فرانسه، مقرراتِ ملیِ خاصی را برایِ استفاده از این فناوری توسطِ پلیس وضع کرده‌اند که نیازمندِ مجوزِ قضایی یا مبتنی بر ضرورتِ بالایِ امنیتی است.
- دسترسی به داده‌هایِ ارتباطی: پلیس برایِ دسترسی به کلان‌داده‌هایِ ارتباطی (مانندِ داده‌هایِ مکان‌یابیِ تلفنِ همراه یا تاریخچه‌یِ ارتباطات)، ملزم به اخذِ مجوزِ قضاییِ مشخص و ارائه دلیلِ کافی برایِ ضرورتِ این دسترسی است. GDPR، چارچوبی کلی برایِ این امر فراهم می‌کند، اما جزئیاتِ اجرایی در قوانینِ ملیِ هر کشور عضو تعریف می‌شود.
- پایگاه‌هایِ داده‌یِ بیومتریک: نگهداریِ طولانی‌مدتِ داده‌هایِ بیومتریکِ افرادِ غیرِ مجرم، یا استفاده از آن‌ها برایِ مقاصدِ غیر از هدفِ اولیه‌یِ جمع‌آوری، تحتِ نظارتِ سخت‌گیرانه‌یِ GDPR قرار دارد.

در حالی که GDPR یک چارچوبِ جامع و الزام‌آور برایِ تمامِ کشورهایِ عضو اتحادیه اروپا فراهم می‌کند، در نظامِ حقوقیِ ایران، مقرراتِ مربوط بهِ حفاظت از داده‌ها و نظارتِ پلیسی، پراکنده و عمدتاً در قوانینِ عادی (مانندِ قانونِ آیینِ دادرسیِ کیفری) و در برخی قوانینِ خاص (مانندِ قانونِ جرایمِ رایانه‌ای) یافت می‌شود. اگرچه اصلِ حاکمیتِ قانون و ضرورتِ اخذِ مجوزِ قضایی در بسیاری از موارد رعایت می‌شود، اما فقدانِ یک قانونِ جامعِ حفاظت از داده‌ها (مانندِ GDPR) و نبودِ نهادِ نظارتیِ مستقل و قدرتمند، خلاءهایی را در مهارِ قدرتِ پلیس در استفاده از فناوری‌هایِ نوینِ نظارتی پدید آورده است.

نتیجه‌گیری

پژوهش حاضر با کاوش در محدودیت‌های حقوق عمومی در استفاده پلیس از فناوری‌های نظارتی هوشمند، آشکار ساخت که گذار به عصر «پلیس‌گری دیجیتال» ضمن ارائه‌ی ظرفیت‌های نویدبخش برای ارتقاء امنیت و نظم عمومی، چالش‌های بنیادینی را برای اصول کلیدی حقوق شهروندی، به‌ویژه «حریم خصوصی» و «اصل تناسب»، پدید آورده است. تحلیل‌ها نشان داد که بدون چارچوب‌بندی دقیق حقوقی و اخلاقی، خطر «نظارت فراگیر»، نقض گسترده‌ی حقوق بنیادین، و خدشه‌دار شدن اعتماد عمومی، منافع امنیتی مورد ادعا را تحت‌الشعاع قرار داده و حتی به تضعیف پایه‌های مشروعیت اقتدار پلیسی منجر خواهد شد.

در این راستا، ضرورت تدوین یک «منشور اخلاقی و حقوقی پلیس هوشمند» نه تنها احساس می‌شود، بلکه به یک الزام انکارناپذیر در نظام حقوقی معاصر بدل گشته است. این منشور باید به عنوان یک چارچوب تقنینی جامع، ضمن پذیرش واقعیت‌های فناورانه، به طور مؤثر قدرت پلیس را در بهره‌گیری از این ابزارها مهار نموده و همزمان، حقوق بنیادین شهروندان را در برابر هرگونه تعدی احتمالی تضمین نماید.

برای دستیابی به این هدف، منشور پیشنهادی باید بر پایه‌های زیر استوار گردد:

۱. تعریف شفاف و محدوده‌ی اختیارات: تعیین دقیق انواع فناوری‌های نظارتی مجاز برای استفاده پلیس، حدود قانونی به‌کارگیری آن‌ها، و معیارهای مشخص برای تشخیص ضرورت و تناسب هر اقدام نظارتی. این امر مستلزم تدوین فهرست‌های روشن و قابل به‌روزرسانی از فناوری‌ها و کاربردهای مجاز و ممنوع است.

۲. حفاظت حداکثری از حریم خصوصی: الزامات سخت‌گیرانه‌ی مربوط به جمع‌آوری، نگهداری، پردازش، و اشتراک‌گذاری داده‌های شهروندان، با تأکید بر اصل «حداقل داده لازم» و ضرورت رضایت آگاهانه در موارد غیرضروری برای نظم عمومی.

۳. شفافیت و پاسخگویی: الزام پلیس به اطلاع‌رسانی عمومی (در حدود مقتضیات امنیتی) درباره‌ی فناوری‌های مورد استفاده، اهداف نظارت، و نحوه‌ی پردازش داده‌ها. همچنین، ایجاد سازوکارهای مؤثر پاسخگویی و جبران خسارت در صورت بروز خطا، سوءاستفاده، یا نقض حقوق شهروندان.

۴. نظارت قضایی مستقل و مؤثر: تأکید بر نقش حیاتی نظارت قضایی پیش از اجرای عملیات‌های نظارتی حساس، و همچنین نظارت پس از آن، به منظور اطمینان از رعایت قانون و اصول اخلاقی. این نظارت باید مستقل، تخصصی، و برخوردار از اختیارات کافی باشد.

۵. مقابله با تبعیض الگوریتمیک: تدوین پروتکل‌هایی برای ارزیابی مداوم الگوریتم‌های مورد استفاده توسط پلیس، به منظور شناسایی و رفع هرگونه تبعیض ناخواسته یا هدفمند علیه گروه‌های خاص.

۶. آموزش و فرهنگ‌سازی: الزامی‌نمودن آموزش‌های تخصصی و مستمر برای نیروهای پلیس در زمینه‌ی مبانی حقوقی، اخلاقی، و فنی استفاده از فناوری‌های نظارتی، و همچنین ارتقاء فرهنگ رعایت حقوق شهروندی در میان کلیه‌ی کارکنان.

۷. بازنگری و به‌روزرسانی مستمر: با توجه به سرعت تحولات فناورانه، منشور باید به گونه‌ای طراحی شود که قابلیت بازنگری و به‌روزرسانی دوره‌ای را داشته باشد تا همواره با آخرین دستاوردهای علمی و تحولات حقوقی همگام بماند.

در نهایت، تدوین و اجرای مؤثر چنین منشوری، گامی اساسی در جهت برقراری تعادل پایدار میان «امنیت» و «آزادی» در جوامع دیجیتال خواهد بود. این چارچوب، نه تنها مانع از سوءاستفاده از قدرت پلیس در عصر فناوری شده، بلکه با تضمین حقوق شهروندان، اعتماد عمومی را نسبت به نهادهای امنیتی تقویت کرده و به حفظ پایه‌های دموکراسی و حاکمیت قانون در دنیای نوین کمک شایانی خواهد نمود.

منابع و ماخذ:

الف : کتب

۱. پوربافر، جان. (۱۳۹۷). «هوش مصنوعی و حقوق جزا؛ چالش‌ها و راهکارها». نشر حقوقدانان.

۲. پوربافر، محمد. (۱۳۹۷). «حقوق اداری؛ کلیات و تشکیلات». نشر کتاب آوا.

۳. قانون آیین دادرسی کیفری ایران، مصوب ۱۳۹۲ با اصلاحات و الحاقات بعدی.

٤. قانون اساسی جمهوری اسلامی ایران.

٥. حبیب‌زاده، توفیق. (۱۳۹۹). «حقوق اداری؛ سازمان و فعالیت‌های اداری». نشر میزان.

٦. حبیبی، رضا. (۱۴۰۰). «مسئولیت کیفری اشخاص حقوقی». نشر دادمهر.

۷. رایجیان اصلی، بهرام. (۱۳۹۸). «حقوق ارتباطات؛ اینترنت و فضای مجازی». نشر حقوقدان.

۸. رضایی، مجید. (۱۳۹۸). «نظریه‌های امنیت در روابط بین‌الملل». نشر سمت.

۹. صفاری، سعید. (۱۳۹۸). «حقوق کیفری تطبیقی». نشر میزان.

۱۰. کاتوزیان، ناصر. (۱۳۹۹). «مبانی حقوق عمومی». انتشارات گنج دانش.

۱۱. کاپل، آلن. (۲۰۰۵). «حقوق بشر و نظم نوین جهانی». ترجمه حسین شریفی طرازکوهی. نشر دادگستر.

۱۲. کریمی، عباس. (۱۴۰۰). «اصول حقوق جزا». نشر میزان.

۱۳. مرکز پژوهش‌های مجلس شورای اسلامی. (۱۴۰۰). «گزارش تحلیلی درباره‌ی حریم خصوصی در حقوق ایران». دفتر مطالعات حقوقی.

۱٤. مرکز پژوهش‌های مجلس شورای اسلامی. (۱۴۰۰). «گزارش تحلیلی درباره‌ی داده‌های بیومتریک و حریم خصوصی». دفتر مطالعات حقوقی.

ب: مقاله ها

۱٥. احمدی، سارا؛ محمدی، علی. (۱۳۹۷). «حریم خصوصی در عصر دیجیتال». فصلنامه مطالعات حقوقی معاصر، دوره ۱۰، شماره ۲.

۱٦. صفاری، محمد. (۱۳۹۸). «حقوق فناوری‌های نوین؛ مباحث کاربردی». مجله پژوهش‌های حقوقی نوین، دوره ۷، شماره ۴.

۱۷. قاسمی، محسن. (۱۴۰۰). «حقوق اداری؛ سازمان و فعالیت اداری». فصلنامه حقوق عمومی ایران، دوره ۱۲، شماره ۱.

۱۸. کدخدایی، عباسعلی. (۱۳۹۷). «حقوق اداری؛ کلیات». نشریه حقوق اداری، دوره ۵، شماره ۳.

۱۹. کدخدایی، گودرز. (۱۳۹۷). «حقوق عمومی در عصر دیجیتال». مجله حقوق عمومی، دوره ۸، شماره ۱.

۲۰. موسوی، سید علی. (۱۳۹۹). «مبانی حقوقی فناوری‌های نوین». فصلنامه دیدگاه‌های حقوقی، دوره ۱۴، شماره ۳.

۲۱. موسوی، سیدمهدی. (۱۳۹۹). «حقوق فناوری اطلاعات و ارتباطات». نشریه حقوق فناوری اطلاعات، دوره ۱۱، شماره ۲.

ج: منابع لاتین

۲۲. B résident, J. (2021). The Algorithmic State: Governance and Power in the Digital Age. MIT Press.

۲۳. Clarke, R. (2010). “The Impact of the Digital Economy on Privacy”. In Digital Economy: Promise and Peril (pp. 55-78). Edited by M. F. O’Neill. Oxford University Press.

۲۴. (General Data Protection Regulation (GDPR) - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016).

۲۵. Danner, A. (2018). The European General Data Protection Regulation (GDPR): A Practical Guide. Kogan Page Publishers.

۲۶. Gasser, U. & Mell, P. (2017). Biometrics and Privacy: A Matter of Trust. In Handbook of Biometrics: Improved, Expanded, and Updated (pp. 77-98). Springer.

۲۷. Geiger, C. (2022). Data Protection Law Enforcement: A Comparative Analysis. Springer.

۲۸. Griffith, John. (2018). The Politics of Security. Cambridge University Press.

۲۹. Kolb, D. (2018). Privacy and Data Protection Law. Cambridge University Press.

۳۰. Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

۳۱. Reid, R. J. (2020). Algorithmic Accountability: Towards a Legal Framework. Oxford University Press.
۳۲. Sornarajah, M. (2017). The International Law on Foreign Investment. Cambridge University Press.
۳۳. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.