پیشگیری از نقض حریم خصوصی در فرآیند دادرسی های الکترونیکی

چکیده

زمینه و هدف: دادرسی الکترونیکی به‌عنوان فرایندی نوین، توانسته است بسیاری از مشکلات موجود در روند دادرسی نظام حقوقی را کاهش دهد و نقشی کلیدی در تحقق هدف اساسی حقوق کیفری، یعنی برقراری عدالت و پاسخگویی قانونی در کوتاه‌ترین زمان ممکن ایفا نماید. این نوع دادرسی با کاهش محدودیت‌های زمانی و مکانی، کاهش هزینه‌های سیستم قضایی، افزایش سرعت انجام امور، انسجام در مدیریت اطلاعات قضایی و ارتقای امنیت قضایی و اداری، دستاوردهای مهمی برای نظام حقوقی به همراه داشته است. با وجود این مزایا، یکی از چالش‌های مهم دادرسی الکترونیکی، نقض حریم خصوصی افراد است. فناوری‌های دیجیتال، با فراهم کردن ابزارهای گسترده جمع‌آوری و پردازش داده‌ها، تهدیدات جدیدی برای امنیت اطلاعات شخصی و حرفه‌ای افراد ایجاد کرده و ضرورت توجه جدی به حفاظت از حریم خصوصی را افزایش داده است. مقاله حاضر، ضمن بررسی جلوه‌های نقض حریم خصوصی در نظام دادرسی الکترونیکی، به تحلیل راهکارهای پیشگیری از این تهدیدات در سه مرحله کلیدی دادرسی یعنی تعقیب، رسیدگی و اجرای حکم می‌پردازد و تلاش دارد چارچوبی جامع برای افزایش کارایی و امنیت سیستم دادرسی الکترونیکی ارائه نماید.

روش پژوهش: این مطالعه با استفاده از روش توصیفی-تحلیلی به بررسی ابعاد مختلف پیشگیری از نقض حریم خصوصی در دادرسی‌های الکترونیکی پرداخته و ضمن شناسایی راهکارهای وضعی، اجتماعی و تقنینی، سازوکارهای بهبود عملکرد و افزایش اعتماد عمومی را مورد تحلیل قرار می‌دهد.

یافته‌ها و نتایج: یافته‌های پژوهش نشان می‌دهد که حریم خصوصی در فضای الکترونیکی همانند حریم خصوصی در دنیای فیزیکی دارای اهمیت قانونی و اخلاقی است و حفاظت از اسناد، مدارک و اطلاعات شخصی و حرفه‌ای افراد ضرورت دارد. در زمینه پیشگیری وضعی، نظارت و مراقبت الکترونیکی از طریق ابزارهای نوین و کنترل قضایی از مؤثرترین راهکارهاست. پیشگیری اجتماعی نیز شامل ارتقای سواد دیجیتال، شفافیت در فرآیندها، افزایش اعتماد عمومی و مشارکت شهروندان در نظارت می‌شود. از منظر تقنینی، تدوین قانون مستقل و موثر برای حمایت از حریم خصوصی اهمیت بسزایی دارد. ایجاد یک سیستم دادرسی الکترونیکی امن و شفاف، نیازمند همکاری هماهنگ میان نهادهای قضایی و جامعه مدنی است و اقدامات پیشگیرانه در سه محور تقنینی، وضعی و اجتماعی باید به‌طور همزمان اجرا شوند تا از تهدیدات مرتبط با حریم خصوصی جلوگیری شده و اعتماد عمومی به سیستم قضایی الکترونیکی حفظ گردد.

واژگان کلیدی: حریم خصوصی، دادرسی الکترونیکی، سیستم قضایی، پیشگیری.

مقدمه

امروزه، نقش فناوری اطلاعات در افزایش سرعت و دقت فعالیت‌های سازمان‌ها و به تبع آن، بهبود بهره‌وری آن‌ها به وضوح نمایان است. این اهمیت به‌ویژه برای سازمان‌هایی که بخش‌های مختلف آن‌ها در نقاط جغرافیایی پراکنده و دور از هم واقع شده‌اند یا برای مؤسساتی که ملزم به انجام وظایف متنوع و متعدد هستند، مشخص‌تر است. این سازمان‌ها بسیاری از چالش‌های خود را با بهره‌گیری از فناوری اطلاعات برطرف می‌کنند که قوه قضاییه نیز یکی از این نهادها به شمار می‌آید.

حقوقدانان همواره در تلاش بوده اند تا با ارائه راهکارهای مناسب به دادرسی سرعت بخشند و اجرای عدالت را در کمترین زمان میسر سازند. در این راستا می توان از دادرسی الکترونیک جهت رفع اطاله دادرسی، تسریع در امور جاری محاکم، افزایش دقت و جلوگیری از سردرگمی اشخاص در پرونده ها، جلوگیری از طرح دعاوی تکراری و پیشگیری از جرم بهره جست. روند الکترونیکی شدن دادرسی‌ها بیش از یک دهه است که در کشورهای پیشرفته به کار گرفته می‌شود. دادرسی الکترونیکی

به معنای به کارگیری ابزارها و روش‌های الکترونیکی برای انجام فرآیند دادرسی است، از جمله ارائه دادخواست و شکواییه، ابلاغ اوراق قضایی، رسیدگی به دعوی و دلایل آن و صدور و اجرای حکم. برخی از مهم‌ترین این ابزارها شامل تلفن همراه، نشانی‌های رایانامه و وب‌سایت‌های اینترنتی هستند.

مقدار حقوق و آزادی‌های اساسی شهروندان به مجموعه‌ای از عناصر و مفاهیم مختلف وابسته است که حریم خصوصی به‌عنوان یکی از مفاهیم بنیادین در این میان قرار دارد. از منظر حقوقی، هرچه دامنه و مفهوم حریم خصوصی به‌طور دقیق‌تری تعیین شود، حقوق شهروندان در برابر قدرت حاکمه، امنیت بیشتری خواهد داشت و از خطر تضییق و نقض مصون می‌ماند. برای تحقق این هدف، نیاز به مداخله قانون‌گذار و تدوین سیاست‌های کیفری و غیرکیفری منسجم و مؤثر احساس می‌شود.

دادرسی الکترونیکی به معنای استفاده از سیستم‌های الکترونیکی و انجام فعالیت‌ها به روشی غیر از شیوه‌های سنتی است. در این دادرسی الکترونیکی به نوع متفاوتی از رسیدگی ماهیتی اشاره ندارد، بلکه به توان قضایی نوین دادگاه‌ها در استفاده از ابزارهای مدرن در فرآیندهای قضایی مربوط می‌شود. این تحول به معنای تغییر ماهیت رسیدگی نیست، بلکه تنها تفاوتی در ساختار خارجی رویه‌ها مشاهده می‌شود. حقوقدانان همواره در تلاشند تا با تسریع روند دادرسی، اجرای عدالت را در کمترین زمان ممکن تضمین کنند و اعتماد عمومی را به دستگاه قضایی افزایش دهند. تسریع به معنای حرکت سریع در دادرسی‌هاست، بدون اینکه حقوق اساسی افراد، از جمله اصل برائت، حق دفاع و نظم قضایی آسیب ببیند. بدین ترتیب، اهمیت فناوری اطلاعات در افزایش سرعت و دقت فعالیت‌های سازمان‌ها و بهبود بهره‌وری آن‌ها همواره در حال رشد است، به‌ویژه برای سازمان‌هایی مانند قوه قضاییه که با چالش‌های متعددی مواجه‌اند(عشق‌پور و اکبرپور، ۱۳۹۵، ۱٤٤).

در تعریفی جامع تر می توان گفت دادرسی الکترونیکی عبارت است از فرایند جامع رسیدگی تمام مراحل تحقیق و دادرسی و امور مرتبط با آن اعم از تنظیم و تقدیم شکواییه، ارجاع، ابلاغ، احضار، استعلام، صدو و اجرای حکم به صورت الکترونیکی با کمک فناوری IT و شبکه مجازی بدون نیاز به ضبط نسخه فیزیکی پرونده که رسیدن به این امکان نیاز به تکمیل زیرساخت ها و گسترش استفاده از فناوری اطلاعات دارد. لذا دادرسی الکترونیکی همان داده ای کردن اطلاعات کاغذی و شفاهی مرتبط با پرونده ها و بهره گیری از فناوری اطلاعات در کل امور حقوقی و قضایی است(موذن زادگان و روستا، ۱۳۹٦، ۱۷۲).

بدین ترتیب در این مقاله، مقصود از دادرسی الکترونیکی استفاده از ابزارها و بسترهای دیجیتال در تمامی مراحل رسیدگی قضایی (اعم از حقوقی و کیفری) است که شامل ارائه دادخواست و شکواییه، ابلاغ اوراق قضایی، جلسات رسیدگی مجازی، صدور حکم و حتی اجرای تصمیمات قضایی در بستر الکترونیک می گردد. پس دادرسی الکترونیکی تنها به معنای دادرسی از راه دور و بدون حضور فیزیکی اصحاب دعوی نیست، بلکه دامنه آن گسترده‌تر است و می تواند ابزارهایی نظیر دستبندهای الکترونیک یا دوربین‌های نظارتی را نیز ـ که بیشتر به مراحل پسادادرسی مربوط‌اند، شامل شود. بر این اساس، دادرسی الکترونیکی به سه مرحله ۱) تعقیب، ۲) رسیدگی و صدور حکم و ۳) اجرای حکم تقسیم بندی شده و ضمن اشاره به خطرات حریم خصوصی در هر سه مرحله به ترتیب راهکارهای پیشگیری از نقض حریم خصوصی در مرحله بررسی می شود.

نوآوری‌ها و فناوری‌های نوین هرچند که معمولاً به سهولت زندگی انسان‌ها می‌افزایند، اما همچنین می‌توانند مشکلات جدی نیز ایجاد کنند. این فناوری‌ها می‌توانند با فراهم کردن آسایش، به سوء استفاده‌هایی منجر شوند که آثار منفی بر روی جنبه‌های اقتصادی، اجتماعی و فرهنگی زندگی داشته باشند. در واقع، سوء استفاده از این ابزارها می‌تواند به ارتکاب جرایم متعدد منجر

شود. استفاده از فناوری‌ها به دوران معاصر مختص نیست و ردپای آن را می‌توان در تاریخ نیز مشاهده کرد. باوجود گذشت سال‌ها از انقلاب صنعتی، روند صنعتی شدن امروز به صورت پیشرفته‌تری در انقلاب فناوری‌های ارتباطات و اطلاعات تجلی یافته و تأثیرات منفی این فناوری‌ها به نظام حقوق کیفری راه یافته است (آشوری و میرزایی، ۱۳۹۱، ٤). توسعه سریع و بی‌حد و حصر فناوری‌های نوین و سوء استفاده از آن، منجر به افزایش استفاده از تکنولوژی در ارتکاب جرایم و تسریع در وقوع آنها شده و در عین حال فضای جدیدی برای جرایم مدرن فراهم آورده است. از این رو، باید توجه داشت که جرم، موضوعی هزینه‌بر و نگران‌کننده است که بر همگان تأثیر می‌گذارد. قربانیان جرم ممکن است از آسیب‌های جسمی، خسارت‌های مالی و ترس رنج ببرند. جرایم به افزایش هزینه‌های تولید، مالیات، هزینه‌های بیمه و احساس ناامنی منجر می‌شوند و تأثیرات آن به تمامی افراد جامعه گسترش می‌یابد.

مطابق رهنمود پیشگیری از جرم سازمان ملل، پیشگیری از جرم مجموعه اقدامات و راهبردهایی است که به منظور کاستن از خطر ارتکاب جرم و تاثیرات بالقوه زیانبار جرایم بر افراد و جامعه انجام می گیرد و از طریق مداخله یا تاثیر بر عوامل ایجاد کننده جرایم به انجام می رسد. امروزه ظهور فناوری های جدید فرصت های منحصر به فردی را برای کمک به سازمان های حوزه پیشگیری از جرم ایجاد کرده است(ابوذری، ۱٤۰۳، ۳۸). برخی معتقدند اصول حاکم بر سیاستگذاری پیشگیرانه از جرم عبارتند از اصل علمی بودن، حقوق بشری بودن، پایداری، قابلیت محاسبه، فراگیر بودن و مشارکت محور بودن که مداقه در آنها زمینه ساز تحولات قابل توجه در امر سیاست گذاری و تدبیراندیشی با محوریت پیشگیری از جرم خواهد بود(پوربافرانی، حیدرپور و قاسمی، ۱٤۰٤، ۱۵). با گسترش دادرسی الکترونیکی و بهره‌گیری از فناوری‌های نوین در فرآیندهای قضایی نیز فرصت‌های جدیدی برای افزایش سرعت و دسترسی به عدالت فراهم شده است اما این تحول دیجیتال خود زمینه‌ساز ظهور تهدیدهای تازه‌ای همچون نفوذ سایبری و نقض حریم خصوصی اصحاب دعوا شده است. از این‌رو، پیشگیری از جرم در این عرصه مستلزم طراحی سیاست‌ها و تدابیر حفاظتی ویژه است.

یکی از اصول دادرسی عادلانه در دادرسی الکترونیکی، اصل رعایت حریم خصوصی است که در قانون اساسی نیز مورد احترام بوده ولی مصادیق نقض آن در دادرسی الکترونیکی تصریح نشده است؛ لیکن برخی از جلوه های رعایت حریم خصوصی اشخاص از جمله حریم خصوصی منزل، حریم خصوصی جسمانی و حریم خصوصی ارتباطات و مکاتبات و اسناد و ادله الکترونیکی مورد توجه قرار گرفته است. لذا با وجود مزایای متعدد، دادرسی الکترونیکی چالش‌های خاص خود را نیز به همراه دارد که از جمله مهم‌ترین آن‌ها می‌توان به نقض حریم خصوصی افراد اشاره کرد. استفاده گسترده از فناوری‌های دیجیتال و جمع‌آوری داده‌های شخصی و اطلاعات محرمانه، تهدیدات جدیدی برای امنیت داده‌ها و حفاظت از حریم خصوصی ایجاد کرده است. دسترسی غیرمجاز به اطلاعات دیجیتال، افشای اطلاعات شخصی و سوءاستفاده از داده‌ها می‌تواند پیامدهای جدی حقوقی، اجتماعی و روانی برای متهمان، شاهدان و سایر ذینفعان پرونده داشته باشد.

با عنایت به مطالب مذکور، مقاله حاضر با روش توصیفی-تحلیلی به بررسی راهکارها و تدابیر پیشگیرانه کیفری، وضعی و اجتماعی از نقض حریم خصوصی در بستر دادرسی های الکترونیکی می پردازد و نهایتاً پیشنهادات عملی برای بهبود عملکرد و افزایش اعتماد عمومی به سیستم قضایی ارائه می دهد.

۱-تدابیر پیشگیرانه تقنینی از طریق تعیین ضمانت اجراهای موثر

برای رفع مشکلات مربوط به حفظ حقوق متهمان و تضمین رعایت حقوق شهروندی در فضای الکترونیکی، علاوه بر تدوین قوانین متناسب با فناوری‌های نوین، ضرورت دارد که قوانین و مقررات موجود مدیریت و سازماندهی شوند تا از انباشت و پیچیدگی آنها جلوگیری و کار دستگاه‌های قضایی، حقوق‌دانان و مجریان قانون در حمایت از حقوق افراد تسهیل گردد. این امر با تدوین و اصلاح دقیق قوانین و مقررات امکان‌پذیر است و همچنین شهروندان نیز می‌توانند با مراجعه به این مستندات نسبت به حقوق و تکالیف خود آگاهی یابند. راهکار مهم دیگر، ایجاد نهادهای کارآمد و مؤثر در فضای سایبری است، چرا که فقدان این نهادها مشکلاتی برای حکومت و شهروندان ایجاد می‌کند.

خسارت ناشی از نقض حریم خصوصی باید متناسب با نوع و شدت آن جبران شود و تمامی جنبه‌های مادی و معنوی ضررها در نظر گرفته شود. عدم دقت در تدوین ضمانت اجراهای موثر، مانع از تحقق بازدارندگی قوی و تأمین عدالت کامل می‌شود. بنابراین، چند راهکار ضروری برای تضمین حقوق افراد در مواجهه با نقض حریم خصوصی در دادرسی الکترونیکی مطرح است:

۱. برای کسانی که حریم خصوصی را نقض می‌کنند، باید مجازات‌هایی همچون انفصال از خدمت به همراه جریمه نقدی در نظر گرفته شود. در صورت رضایت قربانی، جبران تنبیهی مناسب نیز باید پیش‌بینی گردد.

۲. اعاده حیثیت باید با رعایت مصالح افراد آسیب‌دیده انجام شود.

۳. با توجه به اهمیت حریم خصوصی در فضای سایبری، زمانی که احتمال فوری برای کشف جرم یا شناسایی متهم از طریق دسترسی به داده‌ها وجود دارد، پرونده باید به شعبه‌های ویژه استانی ارجاع شود و رسیدگی توسط هیئتی متشکل از قضات متخصص انجام گیرد. همچنین، افراد دارای مجوز دسترسی، جستجو و پایش اطلاعات باید محدود گردند.

٤. از آنجا که عمدتاً نقض حریم خصوصی از سوی مقامات دولتی نسبت به افراد تحت نظر آنها ساده‌تر انجام می‌شود، اقداماتی مانند تدابیر امنیتی پیشگیرانه، آموزش شهروندان و اعمال مجازات‌های شدیدتر می‌تواند مانع بروز این مشکلات گردد. در کشور ما نیز مواردی از نقض حریم خصوصی و دسترسی غیرمجاز به داده‌ها وجود دارد.

٥. باید قانونی لحاظ شود که حضور مقام قضایی در زمان دسترسی و بازرسی داده‌ها ضروری باشد، چراکه نقض حریم خصوصی به عنوان یک حق بنیادی ممکن است منجر به جرایمی چون قتل و کلاهبرداری شود و همچنین زندگی خصوصی و خانوادگی افراد که از اهداف کلان نظام قضایی برای حفظ و تقویت آن است، تحت تهدید قرار گیرد. حضور مقام قضایی مانند دادیار می‌تواند به کاهش احتمال سوءاستفاده و افزایش امنیت و حیثیت کاربران کمک کند. همچنین لازم است در قانون دادرسی الکترونیکی، امکان نظارت رایگان توسط ذینفعان در نظر گرفته شود تا میزان دسترسی به داده‌ها به‌طور دقیق و شفاف تعیین گردد و امکان پیشگیری از نقض حریم داده‌ها با هزینه و آسیب کمتر فراهم شود (رئیسی درکی، قاسم‌زاده الیاسی، ۱۳۹۹، ۱۳۸).

همچنین در هنگامه تفتیش و توقیف داده‌های شخصی، رعایت نکات دقیق و حسن تدبیر ضروری است؛ زیرا عواقب ناشی از دسترسی به اطلاعات و حریم شخصی می‌تواند عمیقاً آسیب‌زده و غیرقابل جبران باشد. ازاین‌رو، تأکید می‌شود که:

۱. شرایط ایجابی و سلبی برای افرادی که اقدام به تفتیش و توقیف داده‌ها می‌کنند، به‌وضوح در مصوبات قانونی مشخص شود.

۲. ضابطین خاص و معین برای انجام این کار تعیین شده و داشتن گواهینامه‌ای جداگانه و مختص به تفتیش و توقیف داده‌ها الزامی باشد.

۳. این افراد باید قابلیت ایفای تعهدات و جبران خسارات ناشی از نقض غیرضروری حریم خصوصی و داده‌ها را دارا باشند.

٤. اخذ تضمین‌های مؤثر می‌تواند در جلوگیری از نقض حریم خصوصی توسط ضابطین، تأثیرگذار باشد.

۵. انجام این فرآیندها باید در حضور مقام قضایی صورت گیرد.

هرچند در حقوق ایران قانون مستقل و جامع درباره حمایت از داده‌ها و حریم خصوصی به شکل مشخص وجود ندارد اما ضمانت اجراهای پراکنده ای در ارتباط با نقض حریم خصوصی پیش بینی شده است. مثلاً دسترسی غیرمجاز به سامانه رایانه ای دیگران و افشای اسرار و تصاویر یا فیلم های خصوصی دیگران در قانون جرایم رایانه ای جرم تلقی شده است. با این حال، خلأ قانونی و نبود یک نظام نظارتی مستقل باعث شده است که ضمانت اجراهای مشخص و بازدارنده برای بسیاری از موارد نقض حریم خصوصی در ایران کافی نباشد.

در مرحله تعقیب، ضمانت اجراهای قانونی می‌توانند شامل تعیین مسئولیت کیفری یا اداری برای مأموران یا کاربرانی باشد که بدون مجوز یا فراتر از اختیارات قانونی به اطلاعات دیجیتال متهم دسترسی پیدا می‌کنند. علاوه بر این، تدوین دستورالعمل‌های روشن درباره نوع اطلاعات قابل جمع‌آوری، مدت زمان نگهداری و نحوه استفاده از داده‌ها، همراه با نظارت قضایی، می‌تواند تضمین کند که اقدامات تعقیبی، متناسب و قانونی باقی بمانند. از منظر اجتماعی، اطلاع‌رسانی به متهمان و وکلا درباره حقوق دیجیتال آنان و پیامدهای قانونی نقض حریم خصوصی، نقش بازدارنده قوی‌ای ایفا می‌کند.

در مرحله دادرسی، ضمانت اجراهای قانونی می‌توانند شامل ممنوعیت قانونی نشر یا استفاده غیرمجاز از اطلاعات جلسه دادرسی آنلاین و اعمال مجازات‌های مشخص برای هرگونه افشای غیرمجاز باشند. این ممنوعیت شامل تمام افراد دارای دسترسی به اطلاعات پرونده، از جمله قضات، وکلا، مأموران اجرای حکم و کارکنان موقت یا قراردادی می‌شود. قانون باید به‌صورت صریح، هرگونه افشای غیرمجاز اطلاعات جلسات دادرسی آنلاین، اسناد دیجیتال یا داده‌های شخصی را منع کرده و محدوده مسئولیت هر فرد را مشخص نماید.

در مرحله اجرای حکم نیز تعیین ضمانت اجراهای قانونی اهمیت ویژه‌ای دارد. به عنوان مثال، هرگونه استفاده غیرمجاز از داده‌های متهم در طول اجرای حکم یا سوءاستفاده از اطلاعات برای اهداف فراتر از حکم، باید با مجازات‌های قانونی مشخص مواجه شود. تدوین دستورالعمل‌های داخلی و نظارت بر مأموران اجرای حکم، همراه با ایجاد سازوکارهای شکایت و رسیدگی به تخلفات، امکان پاسخگویی مؤثر را فراهم می‌کند. این اقدامات، علاوه بر بعد قانونی، به اعتماد عمومی نسبت به سیستم قضایی و رعایت حقوق شهروندان کمک می‌کند.

بنابراین، اعمال ضمانت اجراهای قانونی در مرحله دادرسی، علاوه بر جلوگیری از نقض حریم خصوصی، اعتماد عمومی به سیستم دادرسی الکترونیکی را تقویت کرده و با ایجاد پیامدهای بازدارنده، از سوءاستفاده احتمالی از اطلاعات جلوگیری می‌کند. این اقدامات، در کنار دیگر راهکارهای پیشگیری وضعی و اجتماعی، چارچوبی جامع و مؤثر برای حفاظت از حقوق شهروندان فراهم می‌آورند.

۲-تدابیر پیشگیرانه وضعی

پیشگیری وضعی از جرم برای نخستین بار در سال ۱۹۸۳ توسط کلارک به این شکل تعریف شد: «اقداماتی هدفمند و دائمی که به اشکال خاصی از جرم مربوط می‌شود و شامل مدیریت طراحی یا تغییر محیط به منظور کاهش فرصت‌های ارتکاب جرم و افزایش خطرات آن است» (رزنبام، لوریسیو و داویس، ۱۳۷۹، ۱٤۷). در این رویکرد، تلاش بر این است که با دخالت در شرایط محیطی و کنترل آن‌ها، از وقوع رفتارهای مجرمانه توسط مجرمان بالقوه و افراد با ویژگی‌های خطرناک پیشگیری شود.

هدف اصلی پیشگیری وضعی، تهدید موقعیت‌های ارتکاب جرم است؛ یعنی این روش می‌کوشد تا با کاهش فرصت‌های مجرمان برای ارتکاب جرم، از طریق اقداماتی نظیر اجرای قوانین، اعمال مجازات‌ها و تأمین امنیت مالی و شخصی، اهداف خود را محقق کند. این اصطلاح به معنای سخت‌تر کردن اهداف است و پیشگیری وضعی با کاهش و تقلیل فرصت‌های مجرمانه و ارتکاب جرم محقق می‌شود. این رویکرد به دنبال افزایش امنیت عمومی و کاهش نگرانی از وقوع جرم از طریق طراحی مناسب محیطی، شامل ساختمان‌ها، فضاهای مسکونی و تجاری است. پیشگیری وضعی بر این فرض استوار است که بروز عمل جنایی نه تنها به انگیزه مرتکب وابسته است بلکه ویژگی‌های وضعی نیز تأثیرگذارند. بنابراین، با مدیریت محیط می‌توان از وقوع برخی جرایم جلوگیری کرد (حیدر نژاد و تقی‌زاده، ۱٤۰۱، ۵).

اقدامات وضعی برای جلوگیری از جرم، سابقه‌ای طولانی در تاریخ بشر دارد. انسان‌ها همواره در تلاش بوده‌اند تا خود را از حملات دیگران مصون دارند و اقداماتی در این زمینه اتخاذ کرده‌اند. مفهوم حرز در حقوق جزا، نماد پیشگیری وضعی محسوب می‌شود. با اینکه پیشگیری وضعی از دوران‌های گذشته به صورت طبیعی وجود داشته است، امروزه با توسعه فناوری‌های جدید، این نوع پیشگیری جنبه‌های فنی به خود گرفته است.

اگر پیشگیری وضعی را به عنوان مجموعه‌ای از اقدام‌ها و تدابیری برای کنترل محیط و شرایط پیرامون جرم تعریف کنیم، می‌توان با اتخاذ تدابیر مناسب، امکان ارتکاب جرم را کاهش یا دشوار کرد. این امر از یک سو با کاهش وضعیت‌های پیش‌جنایی که وقوع جرم را تسهیل می‌کند، و از سوی دیگر با افزایش خطر شناسایی و دستگیری بزهکاران انجام می‌شود. بنابراین، پیشگیری وضعی بیشتر بر حمایت از هدف‌های جرم و بزه‌دیدگان بالقوه و اجرای تدابیر فنی برای جلوگیری از آسیب به افراد تمرکز دارد که به طور غیرمستقیم به کاهش بزهکاری منجر خواهد شد.

حفظ حقوق و حریم خصوصی افراد در فرآیند دادرسی یکی از ملاحظات مهم حقوق بشری است که نیاز به توجه قانون‌گذار برای پیش‌بینی ضمانت‌اجرای کارآمد برای حفاظت از حقوق افراد در این زمینه را ایجاب می‌کند. این نگرانی‌ها در دادرسی الکترونیکی که بر اساس تجهیزات الکترونیکی است، نیز وجود دارد. هدف دادرسی، اجرای عدالت و هدف حقوق، پیشگیری

از جرم است. قانون‌گذار سیاست‌های کیفری خود را از طریق قوانینی نظیر قانون مجازات اسلامی، قانون آیین دادرسی کیفری و مقررات مربوط به جرایم رایانه‌ای تنظیم کرده است(فرهادی آلاشتی، ۱۳۹۵، ۳۵)

۱-۲- مراقبت الکترونیکی

یکی از مسائل اساسی و چالش‌برانگیز که جوامع بشری همواره با آن روبه‌رو بوده‌اند و در طول تاریخ نظم و امنیت اجتماعی را به خطر انداخته است، موضوع پیچیده ناهنجاری‌های بزه و بزهکاری است. در این راستا، دولت‌ها به منظور مقابله با هرج‌ومرج و برقراری نظم در جوامع خود، همواره اقدام به اتخاذ تدابیر و راهکارهای مختلفی کرده‌اند. از میان این تدابیر، یکی از استراتژی‌های تأثیرگذار، از میان بردن زمینه‌های ارتکاب جرم و تلاش برای جلوگیری از هنجارشکنی و بروز اعمال مجرمانه است.

در این زمینه، ابزارهای نوین فناوری به ویژه تکنولوژی‌های نظارت الکترونیکی می‌توانند به عنوان ابزاری کارآمد و مؤثر، دولت‌ها را در راستای پیشگیری از جرم یاری دهند. اصطلاح «نظارت الکترونیکی» در واقع ترکیبی از دو واژه «نظارت» و «الکترونیک» است. به اختصار، نظارت به معنای شناخت و متوجه شدن به فعالیت‌های افراد در جامعه است. این نوع کنترل و نظارت به واسطه ابزار و وسایل الکترونیکی صورت می‌گیرد و به عبارتی شامل مراقبت از تمام فعالیت‌های مشکوک در مکان‌های عمومی و خصوصی می‌شود. کاربردهای نظارت الکترونیکی در مدیریت منابع انسانی در کارخانه‌ها و ادارات، همچنین در کنترل ترافیک، نظارت بر تجمعات و حفاظت از تأسیسات و اماکن حیاتی، بسیار گسترده و متنوع است.

پیشگیری از جرم با استفاده از ابزاری نظیر نظارت الکترونیکی می‌تواند به عنوان یک روش مؤثر در پیشگیری وضعی شناخته شود. در این رویکرد، با استعمال تکنیک‌ها و شیوه‌های مختلف، امکان شناسایی و دستگیری مرتکبین جرم افزایش می‌یابد و در نتیجه، احتمال ارتکاب جرم کاهش می‌یابد. این امر بدین معناست که نظارت الکترونیکی باعث می‌شود رفتارهای ناقض هنجار اجتماعی و تهدیدکننده نظم عمومی به سادگی شناسایی و به اثبات برسند و این خود موجب ایجاد ممانعت‌های مؤثری در برابر بزهکاری خواهد شد.

ظهور ابزارهای جدید و پیشرفته با توجه به تحولات تکنولوژیکی نه‌تنها گامی مؤثر در دگرگونی زندگی بشر محسوب می‌شود، بلکه زندگی آسان‌تری را برای انسان‌ها به ارمغان آورده است. این فناوری‌ها در تمامی ابعاد زندگی بشر تأثیرگذار بوده و انسان مدرن را بدون در نظر گرفتن این تکنولوژی‌ها نمی‌توان تصور کرد. در این راستا، نظارت و مراقبت الکترونیکی به عنوان محصولی از مطالعات جرم‌شناسی و کیفرشناسی که همگام با پیشرفت‌های علمی و اختراعات بشری در قرن بیست و یکم شکل گرفته، قابل شناسایی و تحلیل است(Back and LaPrade, 2020, 26)

در مرحله تعقیب، مراقبت الکترونیکی معمولاً در قالب شنود و ردیابی ارتباطات دیجیتال، رهگیری مکانی و جمع‌آوری داده‌های الکترونیکی نمود می‌یابد. این اقدامات هرچند می‌تواند در کشف جرم و شناسایی متهمان مؤثر باشد، اما چالش اصلی آن در نقض حریم خصوصی شهروندان نهفته است. به ویژه هنگامی که داده‌ها فراتر از نیاز پرونده گردآوری شوند یا بدون حکم قضایی مورد استفاده قرار گیرند، خطر ورود به حریم خصوصی افراد به شدت افزایش می‌یابد. راهکار پیشگیرانه در این مرحله، محدودسازی ابزارهای نظارتی به موارد ضروری و با مجوز قضایی مشخص است.

مرحله رسیدگی، به دلیل استفاده از جلسات دادرسی آنلاین و ویدئوکنفرانس‌ها، بیش از دیگر مراحل در معرض تهدیدهای مربوط به حریم خصوصی است. خطر اصلی در این مرحله، ضبط و انتشار غیرمجاز تصاویر و اظهارات اصحاب دعوی و یا نفوذ افراد غیرمجاز به جلسات مجازی است که می‌تواند پیامدهای جدی برای محرمانگی دادرسی داشته باشد. برای پیشگیری وضعی از این تهدیدات، ضروری است که دادگاه‌ها صرفاً از پلتفرم‌های اختصاصی و رمزگذاری‌شده استفاده نمایند و ضبط جلسات صرفاً با دستور مقام قضایی مجاز باشد. در مرحله اجرای حکم، مراقبت الکترونیکی عمدتاً در قالب دستبندهای الکترونیک و سامانه‌های GPS برای ردیابی محکومان به کار گرفته می‌شود.

در قوانین موضوعه ایران، به‌ویژه در مواد ٦٢ قانون مجازات اسلامی (١٣٩٢) و بند ج ماده ٢١٧ قانون آیین دادرسی کیفری مصوب (١٣٩٢)، اشاره شده است که متهمان و مجرمان تحت نظارت سیستم‌های الکترونیکی قرار می‌گیرند. در این مواد قانونی، در صورتی که شرایط مقرر فراهم باشد، اقدام به نظارت و کنترل بر روی این افراد به همراه رضایت خودشان امکان‌پذیر است تا بدین ترتیب از فرار یا مخفی شدن آنان جلوگیری شود. بر اساس متن این مواد، می‌توان نتیجه‌گیری کرد که هدف از سیستم‌های نظارت الکترونیکی در فرایند دادرسی، بهره‌برداری از دوربین‌های مداربسته و دستبندهای الکترونیکی است که در طول مراحل دادرسی از جلسات دادگاه تا صدور رأی و اجرای احکام نقش‌آفرینی می‌کنند. با این حال، لازم به ذکر است که رعایت حریم خصوصی متهمان و مجرمین در این فرآیند ضروری است و تنها در چنین شرایطی است که می‌توان ادعا کرد که این اقدامات عادلانه و قانونی است.

١-١-٢- نظارت الکترونیکی با استفاده از دوربین‌های مداربسته

از دیرباز و در طول تاریخ، انسان‌ها برای حفظ امنیت خویشتن، مال و اعتبار اجتماعی خود، به استفاده از تدابیر پیشگیرانه روی آورده‌اند. یکی از مهم‌ترین این تدابیر، نظارت و مراقبت مستقیم یا غیرمستقیم بر رفتارهای فردی و اجتماعی بوده که در راستای پیشگیری از ارتکاب جرایم و ناهنجاری‌های اجتماعی به کار گرفته شده است. در این میان، نظارت به عنوان یکی از فنون کلیدی پیشگیری وضعی از جرم شناخته شده است. چنان‌که رونالد کلارک، نظریه‌پرداز برجسته در حوزه پیشگیری وضعی، نظارت را ابزاری تعیین‌کننده می‌داند که با ایجاد حسی از مواجهه دائمی با ناظر یا ابزارهای کنترلی، مجرمان بالقوه را از اقدام به رفتار مجرمانه باز می‌دارد. این بازدارندگی عمدتاً ناشی از آگاهی مجرمین از اینکه فعالیت‌هایشان تحت رصد و قابل رهگیری است و احتمال دستگیری آن‌ها بسیار بالاست، می‌باشد (Newman, , & Clarke, 2016, 77).

سیر تحول نظارت و حراست در طول دوران مختلف تاریخی نیز قابل توجه است؛ از مراقبت‌های ساده همچون نگهبانی سنتی و حفاظت فیزیکی از اموال و دارایی‌ها به شکل حرزگذاری گرفته تا تکنولوژی‌های پیشرفته امروزی که نظارت و کنترل را به صورت گسترده، دقیق و غیرحضوری ممکن ساخته‌اند. ظهور فناوری‌های نوین، به ویژه سیستم‌های نظارتی الکترونیکی، تحول شگرفی در قابلیت‌های پیشگیری وضعی به وجود آورده است. این فناوری‌ها امکان نظارت مداوم و بدون نیاز به حضور فیزیکی و مستمر افراد در محل را فراهم کرده‌اند؛ بدین معنی که از راه دور می‌توان به صورت لحظه‌ای و مستمر رفتارها و تحرکات افراد و وضعیت مطلوب حفظ امنیت را کنترل نمود. یکی از برجسته‌ترین نمادهای این تحول، کاربرد گسترده دوربین‌های مداربسته است که در اغلب کشورهای جهان به عنوان ابزاری مؤثر در پیشگیری و کشف جرم مورد استفاده قرار گرفته‌اند و با کاهش نیاز به نیروی مراقب فیزیکی، توانسته‌اند بار سنگینی از وظایف پلیس و دستگاه قضایی را کاهش دهند.

با توسعه و گسترش نظریات پیشگیری وضعی و پیشگیری مبتنی بر موقعیت، استفاده از دوربین‌های مداربسته به عنوان سازوکاری موثر در افزایش ریسک ارتکاب جرم و بالا بردن هزینه‌های انجام رفتار مجرمانه رواج یافت. این رویکرد بر این فرض استوار است که مجرمین در فرایند تصمیم‌گیری عقلانی خود، با بررسی میزان منافع و زیان‌های احتمالی جرم، زمان و مکان ارتکاب جرم را انتخاب می‌کنند. اگر حضور دوربین‌های مداربسته احتمال شناسایی و مجازات را افزایش دهد، آن‌ها از ارتکاب جرم در آن مناطق اجتناب خواهند کرد. به عبارتی، قابلیت رؤیت و رصد دائم فعالیت‌های افراد توسط دوربین‌های نظارتی، جریان فرآیند انتخاب مجرم را به گونه‌ای تغییر می‌دهد که ریسک و بهای جرم بر منافعی که ممکن است از آن به دست آید غالب می‌گردد.

از سوی دیگر، نصب دوربین‌های مداربسته در فضاهایی نظیر فروشگاه‌ها، اماکن تجاری، محلات مسکونی و همچنین اماکن حساس و حیاتی مانند زندان‌ها و دادگاه‌ها، نقش چشمگیری در ارتقای امنیت مکانی و کاهش رفتارهای نابهنجار ایفا می‌کند. این مسئله از منظر جرم‌شناسی اجتماعی قابل تحلیل است؛ چراکه مشاهده مکرر وجود سیستم‌های نظارتی باعث ایجاد احساس کنترل و نظارت دائمی در میان افراد جامعه شده و بنابراین آن‌ها را در بازدارندگی از رفتارهای کج‌روانه و غیرقانونی، به ویژه افراد کم‌رو و مستعد ارتکاب جرم، تحت تأثیر قرار می‌دهد. بدین ترتیب، باوجود نظارت و کنترل الکترونیکی ایجاد شده، این افراد انگیزه خود را برای ارتکاب اعمال خلاف کاهش داده و به تدریج سعی می‌کنند از بروز چنین رفتارهایی در مناطق تحت نظارت اجتناب ورزند.

در مرحله تعقیب، دوربین‌های مداربسته عموماً در بازداشتگاه‌ها، محل‌های بازجویی و یا هنگام انتقال متهم مورد استفاده قرار می‌گیرند. هرچند هدف اصلی آن‌ها تضمین سلامت متهم و مأموران و جلوگیری از رفتارهای خشونت‌آمیز است، اما ضبط پیوسته تصاویر می‌تواند به افشای رفتارها و اطلاعات شخصی منجر شود. به‌ویژه اگر دسترسی به فیلم‌ها بدون محدودیت یا بدون دستور قضایی صورت گیرد، نقض آشکار حریم خصوصی خواهد بود. بنابراین، پیشگیری وضعی در این مرحله مستلزم محدودسازی حوزه و زمان ضبط تصاویر، تعیین سطح دسترسی مشخص برای مراجع ذی‌صلاح، و ممنوعیت استفاده از تصاویر در خارج از چارچوب پرونده قضایی است.

در مرحله رسیدگی، دوربین‌های مداربسته نقش دوگانه‌ای دارند: از یک سو، در جلسات دادرسی آنلاین یا ویدئوکنفرانس به ثبت روند رسیدگی کمک می‌کنند و می‌توانند ابزار شفافیت باشند؛ از سوی دیگر، خطر ضبط و انتشار غیرمجاز محتوای جلسات یا افشای هویت اصحاب دعوی و شهود را به همراه دارند. این موضوع به‌ویژه در پرونده‌های کیفری حساس، تهدیدی مستقیم برای امنیت روانی و اجتماعی طرفین محسوب می‌شود. راهکار پیشگیرانه در این مرحله عبارت است از: استفاده از سامانه‌های رمزگذاری‌شده و اختصاصی، ممنوعیت ضبط توسط اشخاص ثالث، و اعمال کنترل فنی بر ورود و خروج داده‌ها.

در مرحله اجرای حکم کاربرد دوربین‌های مداربسته عمدتاً در نظارت بر زندان‌ها، مراکز بازپروری و همچنین محیط اجرای مجازات‌های جایگزین حبس مشاهده می‌شود. هرچند وجود این دوربین‌ها می‌تواند از سوءرفتار با محکومان و نیز از وقوع درگیری و فرار جلوگیری نماید، اما در صورت استفاده بی‌رویه، منجر به نظارت دائمی و تمام‌عیار بر زندگی روزمره محکومان می‌شود که با اصل کرامت انسانی و حق بر حریم خصوصی ناسازگار است. پیشگیری وضعی در این مرحله، مستلزم تناسب‌سنجی میان ضرورت نظارت و حفظ حریم خصوصی است.

نظارت الکترونیکی در جمهوری اسلامی ایران از اواخر دهه ۱۳۷۰ شمسی و در امتداد روند گسترش فناوری‌های نوین اطلاعات و ارتباطات در ابتدای قرن بیست و یکم مطرح و به تدریج وارد عرصه امنیتی و انتظامی کشور شد. با رشد زیرساخت‌های فناوری اطلاعات در این دوره، مباحث مربوط به کاربرد دوربین‌های مداربسته به عنوان ابزاری نوین برای نظارت دقیق و مستمر بر فضاهای مختلف اجتماعی و اماکن حساس در داخل ایران شکل گرفت. نخستین تجارب به‌کارگیری این فناوری، به دوره‌ای برمی‌گردد که به طور مشخص در بیمارستان‌های تهران مورد آزمون قرار گرفت؛ نصب دوربین‌های مداربسته در بخش‌های مختلف از جمله ایستگاه‌های پرستاری، واکنش‌هایی اعتراضی را از جانب پرستاران به همراه داشت که دلیل آن درک مسئله حریم خصوصی و دغدغه‌های حرفه‌ای در آن فضای خاص بود. این واکنش‌ها نمایانگر تضاد میان نیاز به افزایش امنیت و پیشگیری از وقایع ناخوشایند، از یک سو، و نگرانی نسبت به نظارت بیش از حد و محدودیت آزادی‌های مشهود در محیط کار از سوی دیگر بود. با گذشت زمان، این فناوری، به دلیل اثربخشی مشاهده شده، جایگاه خود را در ساختارهای امنیتی، تجاری و عمومی ایران پیدا کرد و امروزه استفاده از دوربین‌های مداربسته در بسیاری از اماکن، به امری مرسوم و پذیرفته شده تبدیل شده است.

از منظر جرم‌شناسی، نحوه نصب و بهره‌برداری از دوربین‌های مداربسته یکی از عوامل کلیدی در تحقق اهداف پیشگیری وضعی و کاهش وقوع جرم است. به این معنا که دوربین‌های مختلف بسته به نوع کاربرد، مکان و هدف نصب می‌توانند از لحاظ کارایی و اثربخشی پیشگیری تابع سیاست‌ها و روش‌های متفاوتی باشند. نخستین و معمول‌ترین نوع این دوربین‌ها از نوع آشکار بوده و معمولاً در اماکنی نظیر فروشگاه‌ها، مغازه‌ها یا دفاتر اداری نصب می‌شوند تا به همه افراد و مراجعه‌کنندگان اعلام شود که محل مورد نظر تحت نظارت شدید قرار دارد. این نوع نصب، اساس پیشگیری وضعی را بر پایه «آگاهی» از نظارت بنا می‌نهد؛ به این معنا که صرف حضور و نصب دوربین‌ها نمی‌تواند کافی باشد، بلکه اطلاع‌رسانی صریح و مشخص در مورد وجود این تجهیزات لازم است، زیرا پیشگیری موثر هنگامی شکل می‌گیرد که افراد آگاه شوند رفتارهای آنها در معرض نظارت قرار دارد و در نتیجه از انجام اعمال مجرمانه یا رفتاری خارج از چارچوب قانون پرهیز کنندو این آگاهی منجر به ایجاد حس افزایش ریسک برای مجرمین بالقوه می‌شود، زیرا آن‌ها معتقدند که احتمال شناسایی، پیگرد قانونی و دستگیری در صورت انجام جرم بسیار بالاست(عبداله پور، ۱۳۹۴، ۴۴).

دسته دوم این دوربین‌ها به گونه‌ای طراحی و نصب می‌شوند که به آسانی قابل تشخیص و رؤیت نباشند. این نوع کاربرد در مکان‌هایی است که مجرمان بالقوه به دلیل آشنایی فزاینده با روش‌های مقابله با دوربین‌های آشکار، توانایی غیرفعال کردن یا دور زدن این سیستم‌ها را یافته‌اند. نصب دوربین‌های نیمه‌مخفی و در نقاط استراتژیک، سبب می‌شود فرد خاطی نتواند به راحتی مکان دقیق دوربین‌ها را پیش‌بینی کند و این عدم اطمینان موجب افزایش احساس عدم امنیت و تقویت بازدارندگی می‌شود. به عبارتی، این نوع نظارت سبب می‌شود که جرم‌ورزی با فرض وجود نظارت دائمی و گسترده مواجه باشد و بنابراین افراد ریسک ارتکاب جرم را بسیار پرهزینه تشخیص دهند و از آن صرف‌نظر نمایند.

نوع سوم از دوربین‌های الکترونیکی که در رشته جرم‌شناسی پیشگیری وضعی از اهمیت خاصی برخوردارند، دوربین‌های کاملاً مخفی و غیرقابل رویت هستند. این دسته ـ که غالباً با ابعادی کوچک و در نقاط نامشهود نصب می‌شوند ـ پاسخی به چالش‌های پیشین است. مجرمان حرفه‌ای که با فناوری‌های نظارت آشکار و نیمه‌مخفی آشنا شده و راه‌های خنثی‌سازی آنها را یافته‌اند، با

این روش جدید مواجه بوده و نمی‌توانند به سادگی آنها را شناسایی یا مخدوش کنند. از این نظر، دوربین‌های مخفی قادرند نقاط کور نظارتی را از میان بردار

ارده و امکان ثبت دقیق رفتارهای مجرمانه را در شرایطی فراهم آورند که مرتکبین احساس امنیت کاذب کرده و بدون نگرانی از دید نظارتی اقدام به ارتکاب جرم می‌نمایند. این دوربین‌ها با پنهان ماندن از دید متخلفان، موجب افزایش احتمال شناسایی و ضبط شواهد تخلفات شده و بنابراین به شکل مؤثری در فرآیند کشف جرم و پیگیری قانونی آن نقش ایفا می‌کنند. از منظر جرم‌شناسی، چنین رویکردی به‌خصوص در پیشگیری وضعی جرم، افزایش هزینه احتمالی ارتکاب جرم را برای فرد خاطی به همراه دارد و انگیزه او را برای انجام رفتارهای مجرمانه کاهش می‌دهد.

با این حال، پژوهش‌های جرم‌شناسی تأکید دارند که صرف نصب دوربین‌های مداربسته، علیرغم نوع و تکنولوژی به کار رفته، نمی‌تواند تضمینی برای کاهش میزان جرم و تخلف باشد؛ بلکه کیفیت و دقت اجرا و بهره‌برداری از این فناوری‌ها اهمیت بسزایی دارد. عواملی همچون انتخاب مکان استراتژیک نصب دوربین، تعیین زاویه مناسب برای پوشش دید محیط، درجه کیفیت تصویر و تجهیزات ضبط، شرایط نگهداری و نظارت مستمر بر عملکرد دستگاه‌ها، نحوه واکنش سریع و مقتضی به اطلاعات ثبت‌شده و تناسب این اقدامات با ماهیت و نوع جرایم محتمل در آن فضا، همگی تأثیرگذار بر کارایی این سامانه‌ها هستند (Piza and eth, 2019, 137). به عنوان مثال، نصب دوربینی که دید محدود یا زاویه‌ای نامناسب دارد، نمی‌تواند به طور مؤثر رفتار مجرمانه را رصد کند و در پی آن از اثر بازدارندگی و کشف جرم کاسته خواهد شد. همچنین، نقاط کور در پوشش دوربین‌ها می‌توانند فضای مناسبی برای فعالیت مجرمان فراهم آورد.

از سوی دیگر، رویکردهای جدید جرم‌شناسی بر ضرورت ایجاد چارچوب‌های قانونی و اخلاقی به منظور حفظ تعادل میان کارکردهای نظارتی و تضمین حقوق شهروندان تأکید دارند. نصب و بهره‌برداری از دوربین‌های مداربسته می‌بایست با رعایت حقوق افراد، به ویژه حق حریم خصوصی، توأم باشد، چرا که احساس نظارت گسترده و غیرشفاف ممکن است منجر به کاهش اعتماد عمومی، ایجاد استرس اجتماعی و بعضاً مقاومت و فرار از قانون گردد. به همین جهت، قانون‌گذاری دقیق و شفاف در زمینه نظارت الکترونیکی، به همراه اطلاع‌رسانی و آموزش عمومی در خصوص اهداف و دامنه کاربرد این فناوری‌ها، از جمله پیش‌نیازهای موفقیت در استقرار این سامانه‌ها به شمار می‌رود.

در نهایت، با توجه به روند توسعه فناوری‌های نوین ارتباطی و دیجیتال، امکان ادغام دوربین‌های مداربسته با دیگر سیستم‌های هوشمند مانند هوش مصنوعی، تحلیل تصویر و داده‌های بزرگ، ظرفیت پیشگیری و کشف جرم را بیش از پیش ارتقاء داده است. این توسعه‌ها می‌تواند باعث افزایش دقت و سرعت در رصد رفتارهای مجرمانه، شناسایی زودهنگام تهدیدها و اجرای سریع اقدامات پیشگیرانه گردد؛ اما در عین حال، چالش‌ها و نگرانی‌های جدیدی در خصوص حفظ حقوق شهروندان و مقابله با سوءاستفاده‌های احتمالی به همراه دارد که نیازمند مطالعه، تحلیل و تنظیم سیاست‌های متعادل و به‌روز در حوزه جرم‌شناسی و حقوق کیفری است. به طور کلی، استفاده هدفمند از دوربین‌های مداربسته در چارچوب الگوهای جرم‌شناختی پیشگیری وضعی، با در نظر گرفتن مولفه‌های فنی، انسانی، اجتماعی و قانونی، می‌تواند به عنوان یکی از ابزارهای مؤثر در کاهش جرم و ارتقای امنیت اجتماعی در ایران قلمداد شود و نقشی اساسی در بهبود کیفیت زندگی شهروندان و افزایش حس امنیت ایفا کند.

۲-۱-۲- نظارت الکترونیکی با استفاده از دستبندهای الکترونیکی

جرم و نقض هنجارها پدیده‌ای ناخوشایند و تهدیدکننده‌ای است که امنیت و آرامش زندگی انسان‌ها را به خطر می‌اندازد. از این رو، بشر در طول تاریخ همواره تلاش کرده است تا آن را کنترل کرده و مقابله‌ای مؤثر با آن داشته باشد و در دوره‌های مختلف، شیوه‌های متنوعی را برای این منظور به کار گرفته است. امروزه با پیشرفت فناوری‌های نوین، روش‌های مقابله و پاسخ به مجرمین به طور چشمگیری تغییر یافته است و بهره‌گیری از این فناوری‌ها می‌تواند تأثیر مثبتی بر نظام حقوق کیفری داشته باشد. به ویژه استفاده از آنها در پیشگیری وضعی جرم، امری ضروری و اجتناب‌ناپذیر است؛ زیرا بزهکاران همواره در حال تغییر و نوآوری در روش‌های ارتکاب جرم خود هستند و دانش پیشگیری وضعی باید چند قدم جلوتر حرکت کند تا بتواند قبل از وقوع جرم، احتمال بروز آن را شناسایی کرده و راهکارهای جلوگیری از آن را پیش‌بینی نماید. دستبند الکترونیکی به عنوان یک فناوری نوین، نقش برجسته و مؤثری در حقوق کیفری و پیشگیری وضعی در روند دادرسی الکترونیکی ایفا می‌کند. در قوانین ایران، زندان و حبس به عنوان مجازات در نظر گرفته شده و مجرمین بسته به نوع جرم ممکن است به این مجازات محکوم شوند؛ ولی امروزه یک مشکل اساسی در این زمینه وجود دارد: زندان علاوه بر اینکه جنبه‌های تنبیهی و تربیتی دارد، متأسفانه به مکانی تبدیل شده است که مجرمین در آن تجربیات و دانش مجرمانه خود را تبادل می‌کنند و به نوعی آموزشگاه مجرمان حرفه‌ای تبدیل می‌شود. همچنین، هزینه‌های بالای نگهداری زندانیان بار سنگینی بر دوش دولت‌ها تحمیل می‌کند. از این رو، استفاده از دستبندهای الکترونیکی می‌تواند جایگزینی مناسب برای زندان باشد که ضمن کاهش هزینه‌ها، ویژگی‌های پیشگیرانه جرم را نیز داراست. بنابراین، تمرکز اصلی این پژوهش بر جنبه پیشگیرانه استفاده از این دستبندها است.

شایان ذکر است که در برخی منابع، واژه‌های «دستبند الکترونیکی» و «نظارت الکترونیکی» به جای یکدیگر به کار رفته‌اند، اما در این تحقیق، دستبند الکترونیکی برای پیشگیری از وقوع جرم در دادرسی الکترونیکی به کار می‌رود، در حالی که مفهوم نظارت الکترونیکی وسیع‌تر است و علاوه بر دستبند، شامل فناوری‌هایی مانند دوربین‌های مداربسته نیز می‌شود. البته یکی از نقدهای این نوع نظارت الکترونیکی، نقض حریم خصوصی افراد در دوران اصلاح و درمان آنهاست.

تعریف دقیق دستبند الکترونیکی، تحت مراقبت الکترونیکی قرار دادن فرد در محل سکونت است، بدین معنا که فرد در محدوده و مکان‌های خاصی به نوعی بازداشت خانگی الکترونیکی در می‌آید و این وضعیت از طریق فناوری الکترونیکی پایش می‌شود (جاویدزاده و میره‌ای، ۱۳۸۳، ۱۹٤).

دستبند الکترونیکی دستگاهی است که به مچ دست یا پای فرد بسته می‌شود و از طریق سیستم موقعیت‌یاب جهانی(GPS) ، در هر لحظه مکان و موقعیت فرد را ردیابی می‌کند و تحت کنترل قرار می‌دهد (احسان‌پور، ۱۳۸۷، ۸۹).

مفهوم نظارت الکترونیکی مجرمان نخستین بار توسط دکتر روبرت شوایترگیل در دهه ۱۹۹۰ میلادی مطرح شد و پس از حدود ۲۰ سال این مفهوم عملاً اجرا گردید. اولین تجربه استفاده عملی از نظارت الکترونیکی به سال ۱۹۸۵ بازمی‌گردد (احسان‌پور، ۱۳۸٦). گفته می‌شود این ایده الهام گرفته از داستان کارتونی «مرد عنکبوتی» بوده است، جایی که در نیومکزیکو قاضی مقرر می‌کند وسیله‌ای الکترونیکی به پای مجرمی بسته شود تا رفت و آمدهای او تحت نظارت قرار گیرد (تدین، ۱۳۸۸، ۵۹).

در کانادا، ابتدا در استان کلمبیا بریتانیایی استفاده از نظارت الکترونیکی آغاز شد. هدف از این اقدام، جایگزینی مجازات کم‌هزینه به جای حبس برای مجرمان بود. از سال ۱۹۹۲، این روش در سراسر کانادا، به جز مناطق کم‌جمعیت، به اجرا درآمد. در همان

سال، به طور متوسط روزانه حدود صد مجرم در برنامه نظارت الکترونیکی شرکت داشتند. گزارش‌های اولیه نشان می‌دهد که این روش نسبت به حبس بسیار مقرون‌به‌صرفه بوده و امتیازات متعددی برای مجرمان فراهم می‌کند.

مطالعات انجام‌شده درباره مزایای نظارت الکترونیکی، علاوه بر صرفه‌جویی اقتصادی در هزینه‌های زندان، نشان می‌دهند که اکثر مجرمان حفظ ارتباط با خانواده را مهم‌ترین مزیت این سیستم می‌دانند. اما دیدگاه‌ها درباره حفظ شغل متفاوت است و نظرات در استان‌های مختلف کانادا متنوع بوده است؛ برخی این مزیت را مثبت ارزیابی کرده و برخی کمتر اهمیت داده‌اند. همچنین گروهی معتقدند استفاده از این دستبندها به حریم خصوصی افراد خدشه وارد می‌کند. از لحاظ جلوگیری از بازگشت به جرم نیز، طرفداران نظارت الکترونیکی این روش را مؤثرتر از زندان قلمداد می‌کنند

یکی از استدلال‌های مکمل در حمایت از نظارت الکترونیکی این است که در مواردی که مجرم به مجازات زندان کوتاه‌مدت محکوم شده، اعتماد عمومی به اجرای عدالت کاهش می‌یابد، چرا که مجرم اغلب با آزادی مشروط زودتر از موعد آزاد می‌شود. اما در نظارت الکترونیکی، مدت زمان نظارت مشخص بوده و فرد فقط برای اهدافی مانند کار یا درمان می‌تواند خارج شود.

در مرحله تعقیب، دستبندهای الکترونیکی برای نظارت بر متهمانی که در انتظار رسیدگی قضایی هستند، استفاده می‌شوند. با وجود این، جمع‌آوری داده‌های مکانی و فعالیت فرد می‌تواند تهدیدی جدی برای حریم خصوصی محسوب شود؛ به ویژه در شرایطی که متهم هنوز به عنوان مجرم قانونی شناخته نشده است. به همین دلیل، استفاده از فناوری‌های رمزنگاری و محدودسازی دسترسی به اطلاعات تنها برای مأموران تحقیقاتی مجاز، امری ضروری است. علاوه بر این، اطلاع‌رسانی به متهم و وکیل وی درباره نوع داده‌های جمع‌آوری شده و هدف از نظارت، همراه با آموزش مأموران تحقیقاتی در زمینه مسئولیت‌های قانونی و اخلاقی، از مهم‌ترین راهکارهای اجتماعی برای کاهش ریسک نقض حریم خصوصی محسوب می‌شود.

در مرحله رسیدگی، داده‌های جمع‌آوری شده توسط دستبندهای الکترونیکی ممکن است در جلسات دادرسی مورد استفاده قرار گیرند. انتشار غیرمجاز این اطلاعات می‌تواند بر استقلال دادرسی و امنیت روانی متهم تأثیر منفی بگذارد. بنابراین، ضروری است دسترسی به داده‌ها محدود به قاضی و نمایندگان قانونی باشد و امکان مشاهده زنده موقعیت متهم تنها در محیط‌های امن فراهم شود. ثبت و نظارت مستمر بر دسترسی‌ها، به‌ویژه از طریق سیستم‌های Audit Log، می‌تواند از سوءاستفاده احتمالی جلوگیری کند. از بعد اجتماعی، آموزش قضات و وکلا درباره استفاده مسئولانه از اطلاعات و اطلاع‌رسانی به عموم درباره حقوق متهمان و محدودیت‌های نظارت، زمینه را برای رعایت حریم خصوصی فراهم می‌کند.

در مرحله اجرای حکم، داده‌های موقعیت متهم تحت نظارت دستبندهای الکترونیکی در فرآیند اجرای حکم و پایش رفتار او مورد استفاده قرار می‌گیرند. در این مرحله نیز خطر سوءاستفاده از داده‌ها یا دسترسی غیرمجاز توسط نهادهای غیرمرتبط وجود دارد. استفاده از رمزنگاری داده‌ها، محدود کردن دسترسی‌ها و طراحی سیستم‌هایی که امکان حذف خودکار داده‌های غیرضروری پس از پایان دوره نظارت را دارند، از مهم‌ترین راهکارهای وضعی به شمار می‌رود. از منظر اجتماعی، آموزش مأموران اجرای حکم درباره اهمیت حفاظت از حریم خصوصی و فراهم کردن امکان شکایت متهمان در صورت نقض قوانین، به ارتقای اعتماد عمومی و رعایت حقوق شهروندی کمک می‌کند.

۳-تدابیر پیشگیرانه اجتماعی

"پیشگیری اجتماعی" به تدابیر و شیوه‌های آموزشی، فرهنگی، اقتصادی و اجتماعی اشاره دارد که توسط دولت و نهادهای غیر دولتی برای سالم‌سازی محیط اجتماعی و فیزیکی به‌منظور حذف یا کاهش عوامل اجتماعی بروز جرم اتخاذ می‌شود. تعاریف مختلفی برای پیشگیری اجتماعی وجود دارد که از میان آنها می‌توان به این تعریف اشاره کرد: پیشگیری اجتماعی از جرم، مجموعه‌ای از اقدامات و تدابیر است که هدف آن کاهش یا حذف عوامل اجتماعی، اقتصادی و محیطی مؤثر بر جرم است. این تدابیر پیش از آن‌که به مرحله مداخله پس از وقوع آسیب برسند، می‌کوشند شرایط بروز نقض حریم خصوصی را در سطح اجتماعی کاهش دهند.

بدون شک، پیشگیری اجتماعی با نقش جامعه در بروز جرم ارتباط دارد. جامعه به عنوان یک واژه، دو مفهوم متفاوت دارد: یکی به معنای محیط فیزیکی (مانند خیابان‌ها و ساختمان‌ها) و دیگری به عنوان محیط انسانی اطراف فرد. کارکرد اول جامعه به عنوان پیشگیری محیطی و کارکرد دوم به عنوان پیشگیری اجتماعی شناخته می‌شود. جامعه می‌تواند همزمان نقش‌های حمایتی و بازدارنده در برابر جرم داشته باشد . به همین دلیل، تدابیر پیشگیری اجتماعی باید از دو رویکرد اصلی بهره‌مند شوند. رویکرد اول، غیرفعال کردن مکانیسم‌های اجتماعی جرم (رویکرد سلبی) و رویکرد دوم، فعال ساختن جامعه و مکانیسم‌های اجتماعی به منظور پیشگیری از جرم (رویکرد ایجابی) است. نکته مهم این است که این دو رویکرد می‌توانند به طور همزمان به اجرا درآیند.

افرادی که در مناطق با نرخ جرم بالا زندگی یا کار می‌کنند، ممکن است به دلیل تأثیرات اجتماعی و اقتصادی ناشی از جرم و احساس بیزاری و ناامیدی ناشی از آن، از برخی از فرصت‌های طبیعی زندگی محروم شوند از سوی دیگر، انحرافات اجتماعی و بزهکاری جزئی اصلی از جوامع بشری است و نمی‌توان جامعه‌ای را تصور کرد که در آن آثاری از کج‌روی و جرم وجود نداشته باشد. بنابراین، ضروری است که در جهت مقابله با بی‌نظمی و انحرافات اجتماعی اقداماتی انجام دهیم. در گذشته، این مسائل معمولاً با مجازات‌های سخت و سنگین بزهکاران حل و فصل می‌شد. اما واقعیت این است که این مجازات‌ها در طول تاریخ نتوانسته‌اند از بروز جرم جلوگیری کنند و جوامع را از مخمصه مجرمین و جنایات دور نگه‌دارند.

برآورد هزینه‌های ناشی از اجرای مجازات و اقدام‌های تربیتی و تأمینی، به همراه هزینه‌های مربوط به جرایم برای بزهکار، بزه‌دیده و جامعه، رقم بالایی را نشان می‌دهد. اگر مدیران کشور به این سطح از درک برسند که به جای انتظار برای وقوع جرم و تعقیب مرتکب، خود را وقف پیشگیری از جرم کنند و با صرف هزینه‌های ذکر شده، به رفع نیازها و کمبودهای جامعه بپردازند، می‌توانند از گسترش کمی و کیفی جرایم در جامعه جلوگیری کرده و بزهکاری را کنترل نمایند. بنابراین، با بهره‌گیری از الگوهای پیشگیری از جرم، می‌توان علاوه بر جلوگیری از جرایم جدید که با ورود فناوری و صنعتی شدن جوامع به وجود آمده‌اند، از تأثیر ابزارها و تکنولوژی‌های مدرن استفاده کرد. این امر از طریق الگوهای پیشگیری وضعی که بر وضعیت‌های خاص تأکید دارد، و پیشگیری اجتماعی که شامل تدابیر پیشگیرانه در محیط‌های اجتماعی است که در فرآیند جامعه‌پذیری فرد نقش ایفا می‌کنند، امکان‌پذیر است. علاوه بر این، با افزایش ریسک و کنترل مناطق پرخطر و استفاده از رسانه‌های گروهی و اجتماعی، همچنین در زمینه دادرسی الکترونیکی، می‌توان جوامع را آگاه کرده و با آموزش و اطلاعات‌رسانی به مردم، به پیشگیری از ارتکاب جرایم کمک کرد. از این رو، فناوری‌های نوین می‌توانند در کنار حقوق کیفری و نظام قضایی قرار گرفته

و در الگوهای پیشگیری وضعی و اجتماعی مورد استفاده قرار گیرند. با استفاده صحیح از این فناوری‌ها، می‌توان زمینه‌های ارتکاب جرایم را کاهش داد و گامی مؤثر در جهت پیشگیری از جنایات سنتی و نوین برداشت.

در مرحله تعقیب، تدابیر پیشگیرانه اجتماعی می‌توانند شامل آموزش مأموران تحقیقاتی و کارکنان قضایی درباره حقوق دیجیتال متهمان و محدودیت‌های قانونی در جمع‌آوری و استفاده از داده‌ها باشند. همچنین، اطلاع‌رسانی به متهمان و وکلا درباره نحوه نظارت الکترونیکی و حقوق مربوطه، به ایجاد شفافیت کمک می‌کند و امکان اعتراض قانونی به نقض حریم خصوصی را فراهم می‌سازد. ایجاد فرهنگ پاسخگویی و احترام به حریم خصوصی در سطح دستگاه قضایی، از ارتکاب تخلفات پیشگیری می‌کند و اعتماد عمومی را تقویت می‌نماید.

در مرحله دادرسی، آموزش قضات و وکلا درباره محدودیت‌های قانونی استفاده از داده‌های دیجیتال و پیامدهای افشای غیرمجاز، به عنوان یک تدبیر پیشگیرانه اجتماعی حیاتی است. اطلاع‌رسانی به شهروندان و طرفین پرونده درباره حقوق آنان در محیط دادرسی الکترونیکی و نحوه حفاظت از اطلاعات شخصی، علاوه بر اثر بازدارنده، حس امنیت و شفافیت را افزایش می‌دهد. همچنین، تدوین پروتکل‌های اخلاقی و راهنماهای عملی برای استفاده از اطلاعات جمع‌آوری شده، به کاهش خطر نقض حریم خصوصی کمک می‌کند و رفتارهای حرفه‌ای قضات و وکلا را هدایت می‌نماید. همچنین ایجاد سیستم‌های ثبت و گزارش‌گیری (Audit Log) که هر دسترسی یا تغییر در داده‌ها را مستند می‌کند، می‌تواند علاوه بر بعد وضعی، از نظر اجتماعی نیز با افزایش شفافیت و پاسخگویی، زمینه را برای رعایت حریم خصوصی فراهم کند. فرهنگ‌سازی در میان قضات و وکلا درباره رعایت قوانین حریم خصوصی و آگاهی‌بخشی به طرفین پرونده در مورد حقوق خود، ضمانت اجتماعی این راهکار را تقویت می‌کند.

در مرحله اجرای حکم، تدابیر اجتماعی شامل آموزش مأموران اجرای حکم و کارکنان نهادهای مرتبط به اهمیت حریم خصوصی، ایجاد سازوکارهای شکایت و پیگیری تخلفات و اطلاع‌رسانی عمومی درباره حقوق شهروندان در این مرحله است. فرهنگ‌سازی در سطح جامعه درباره احترام به داده‌های شخصی و خطرات سوءاستفاده از اطلاعات، علاوه بر اثر آموزشی، نقش پیشگیرانه کیفری نیز دارد. این اقدامات موجب می‌شوند که متهمان و شهروندان نسبت به حقوق خود آگاه شوند و از سویی، مأموران و کارکنان دستگاه قضایی نیز نسبت به مسئولیت‌های قانونی و اخلاقی خود پایبند بمانند.

افزون بر راهکارهای مذکور، تدابیر دیگری نیز به طور کلی در راستای پیشگیری از نقض حریم خصوصی در تمام مراحل دادرسی و نه یک مرحله خاص، در ادامه مورد اشاره و بررسی قرار می گیرد.

۱-۳- آموزش و ارتقاء سواد دیجیتال

نخستین گام در این مسیر، آموزش و ارتقاء سواد دیجیتال و حقوقی در میان شهروندان و کاربران دستگاه قضایی است. فقدان آگاهی نسبت به حقوق داده‌های شخصی و نحوه استفاده از آن‌ها در سامانه‌های دادرسی، اغلب سبب می‌شود افراد نتوانند از خود در برابر نقض‌های احتمالی دفاع کنند. آموزش‌های رسمی در دانشگاه‌ها، دوره‌های ضمن خدمت برای کارکنان قضایی، و حتی کمپین‌های عمومی اطلاع‌رسانی، نقش اساسی در پیشگیری دارند.

سواد دیجیتال در این زمینه، صرفاً محدود به مهارت‌های فنی همچون استفاده از رایانه یا اینترنت نیست، بلکه شامل آگاهی نسبت به خطرات سایبری، روش‌های حفظ امنیت داده‌ها، نحوه شناسایی آسیب‌پذیری‌های حریم خصوصی، و همچنین آشنایی

با حقوق قانونی مربوط به داده‌های شخصی است. بسیاری از شهروندان به دلیل ناآشنایی با مفاهیمی چون رضایت آگاهانه (Informed Consent)، رمزگذاری داده‌ها، یا سیاست‌های حریم خصوصی (Privacy Policies)، قادر به تشخیص نقض‌ها یا پیگیری حقوق خود در مواجهه با آن‌ها نیستند.

نمونه‌های موفق جهانی مانند برنامه‌های آگاهی‌بخشی در اتحادیه اروپا در قالب کمپین‌های GDPR، یا اقدامات آموزشی وزارت دادگستری فرانسه برای ارتقاء سواد داده‌ای قضات، نشان می‌دهد که آموزش، نه تنها از آسیب‌های احتمالی می‌کاهد، بلکه موجب افزایش اعتماد عمومی به سیستم عدالت دیجیتال نیز می‌شود. در نهایت، باید توجه داشت که آموزش و ارتقاء سواد دیجیتال امری مستمر، تدریجی و تعاملی است. طراحی برنامه‌های آموزشی باید متناسب با تحولات فناوری و نیازهای مخاطبان به‌روزرسانی شود و از رویکردهای مشارکت‌محور، تعاملی و حتی بازی‌محور (gamification) بهره بگیرد تا بیشترین اثربخشی را داشته باشد. این مسیر، زمینه‌ساز فرهنگ‌سازی فراگیر در زمینه احترام به حریم خصوصی و گامی بنیادین در مسیر پیشگیری اجتماعی از نقض آن خواهد بود(Barth S, De Jong, 2017, 1038).

۲-۳- ایجاد شفافیت و اعتماد در نهادهای قضایی دیجیتال

ایجاد شفافیت در عملکرد نهادهای قضایی دیجیتال، عامل مؤثری در جلب اعتماد عمومی و کاهش نگرانی‌های اجتماعی نسبت به نقض حریم خصوصی است. وقتی افراد بدانند چه داده‌هایی، چگونه و به چه منظور جمع‌آوری می‌شود و دسترسی به آن‌ها تحت چه ضوابطی صورت می‌گیرد، مشارکت فعال‌تری در فرآیندهای دادرسی خواهند داشت. تنظیم سیاست‌های حریم خصوصی شفاف، انتشار منشور حقوق دیجیتال و پاسخ‌گویی در برابر خطاهای سیستمی، بخشی از این فرایند اعتمادسازی محسوب می‌شود.

شفافیت در فرآیند جمع‌آوری، ذخیره‌سازی و استفاده از داده‌های شخصی باید در مرکز طراحی زیرساخت‌های دادرسی الکترونیکی قرار گیرد. کاربران و اصحاب دعوا باید بدانند چه اطلاعاتی از آن‌ها ثبت می‌شود، در چه بازه‌ای نگهداری می‌شود، چه نهادهایی به آن دسترسی دارند و هدف از استفاده از این اطلاعات چیست(Solove DJ, Schwartz, 2020, 34) نهادهای قضایی باید سازوکارهایی برای رضایت آگاهانه فراهم آورند؛ بدین معنا که کاربران قبل از ثبت اطلاعات خود در سامانه‌ها، فرصت مطالعه، درک و تأیید استفاده از داده‌هایشان را داشته باشند. تجربه‌ی اتحادیه اروپا در الزامی کردن این اصل تحت مقررات عمومی حفاظت از داده‌ها (GDPR)، الگویی مؤثر برای دیگر کشورها محسوب می‌شود (Voigt P, Von dem, 2017, 64). ایجاد کانال‌های ارتباطی شفاف با کاربران برای پاسخ به سؤالات، دریافت شکایات و اطلاع‌رسانی در مورد حقوق دیجیتال، موجب بهبود رابطه میان نهاد قضایی و شهروندان می‌شود. در برخی کشورها، راه‌اندازی «دفاتر راهنمای حریم خصوصی» در ساختمان‌های دادگستری یا در بستر دیجیتال، برای پاسخ‌گویی به ابهامات کاربران، از جمله اقدامات مؤثر در جهت تقویت شفافیت نهادی بوده است.

به طور کلی، شفافیت و اعتماد نه صرفاً مفاهیم اخلاقی، بلکه پیش‌شرط‌های عملکرد مؤثر، پایدار و مشروع در نظام قضایی دیجیتال هستند. سرمایه‌گذاری بر روی این اصول، نه‌تنها از نقض‌های احتمالی حریم خصوصی جلوگیری می‌کند، بلکه اعتماد بلندمدت کاربران به عدالت الکترونیکی را تضمین خواهد نمود.

۳-۳- مشارکت عمومی در طراحی و نظارت بر فناوری‌های دادرسی

مشارکت عمومی در طراحی و نظارت بر فناوری‌های مورد استفاده در فرآیند دادرسی، یکی دیگر از محورهای مهم پیشگیری اجتماعی است. فناوری بدون نظارت اجتماعی، می‌تواند به ابزاری برای سلطه اطلاعاتی بدل شود. از این رو، درگیر کردن نهادهای مدنی، متخصصان حقوقی، فعالان حوزه فناوری و حتی نمایندگان اقشار آسیب‌پذیر در ارزیابی، طراحی و بازنگری سامانه‌های دادرسی الکترونیکی، امری ضروری است. چنین مشارکتی نه‌تنها موجب افزایش مشروعیت فناوری‌های مورد استفاده می‌شود، بلکه احتمال وقوع نقض‌های سیستماتیک را نیز کاهش می‌دهد.

یکی از مهم‌ترین گام‌ها در این راستا، درگیر کردن گروه‌های مختلف جامعه در فرآیند طراحی و توسعه سیستم‌های دادرسی دیجیتال است. به‌ویژه، مشارکت افرادی که به‌طور مستقیم تحت تأثیر این فناوری‌ها قرار دارند (مانند متهمان، وکلا، قضات، و حتی افراد آسیب‌پذیر)، موجب می‌شود که طراحی‌ها به‌طور دقیق‌تر و منصفانه‌تری انجام شوند. این مشارکت می‌تواند از طریق برگزاری جلسات مشورتی، کارگروه‌های بررسی و آزمایش پروتوتایپ‌ها صورت گیرد(O'Hara K, Shadbolt, 2019, 45) .

از سوی دیگر، رسانه‌ها و نهادهای نظارتی مستقل، نقش کلیدی در افشا، هشدار و پیگیری موارد نقض حریم خصوصی ایفا می‌کنند. حمایت قانونی از روزنامه‌نگاری تحقیقی در حوزه عدالت دیجیتال و ایجاد نهادهای مستقل برای پایش عملکرد قضایی در فضای دیجیتال (نظیر شوراهای حریم خصوصی یا کارگروه‌های حقوق داده‌ها) از جمله اقدامات ضروری برای تضمین نظارت عمومی مؤثر هستند. در نهایت، مشارکت عمومی و نظارت مستقل، تضمینی برای پاسخ‌گویی در سیستم‌های دادرسی الکترونیکی است. این مشارکت می‌تواند مانع از سوءاستفاده از فناوری‌ها و تهدیدات امنیتی احتمالی شود و به شکل‌گیری نظام قضائی دیجیتال شفاف‌تر، عادلانه‌تر و قابل اعتمادتر منتهی گردد.

٤-۳-افزایش اعتماد عمومی

در حال حاضر، افرادی وجود دارند که به دلایل مختلف مانند سن بالا، بی‌سوادی، بیماری، و عدم آشنایی با فناوری‌های الکترونیکی قادر به دسترسی به این سامانه‌ها نیستند. اجباری شدن استفاده از این روش می‌تواند حقوق این افراد را تضییع کند. همچنین، سرعت پایین اینترنت و مشکلات سیاسی که منجر به محدودیت در باند اینترنت می‌شود، می‌تواند ارتباط متهمان و مالکان حقوق و اصحاب دعوی را دچار اختلال کند. استفاده از دادرسی الکترونیکی نیازمند زیرساخت‌های مناسب برای اجرای مؤثر آن است و بدون این بسترها، صحبت درباره دادرسی الکترونیکی بی‌معنا خواهد بود. افراد متخصص در این حوزه با چالش‌های متعددی مواجه هستند و افرادی که بی‌سوادند عملاً نمی‌توانند به صورت آنلاین شرکت کنند و مجبورند در مکان‌هایی ارتباط برقرار کنند که امنیت داده‌های شخصی و اطلاعات دادرسی آنچنان تأمین نمی‌شود. مراجعه به دفاتر خدماتی غیرمجاز منجر به نظارت افراد غیر مسئول بر حریم خصوصی می‌شود. علاوه بر این، وجود نیروهای اطلاعاتی، نظامی و پلیس فتا که بدون مجوز قضایی به لحاظ امنیتی مکالمات و اطلاعات افراد را مورد استراق سمع قرار می‌دهند، می‌تواند باعث تضعیف اعتماد عمومی به فرآیند دادرسی الکترونیکی شود. بنابراین، بسترهای لازم برای توسعه دولت الکترونیک و دادرسی الکترونیکی تنها در صورت افزایش اعتماد عمومی به شبکه‌ها و سامانه‌های دولتی و قضایی فراهم می‌شود، اعتمادی که وقتی حاصل می‌گردد که دولت به قوانین خود پایبند باشد و به درستی آن‌ها را اجرا کند. زمانی که بحث‌های امنیتی مطرح می‌شود، حتی قوانین نیز ممکن است تحت تأثیر قرار بگیرند زیرا ممکن است مجریان قانون به قوانین مورد اجرا اعتقادی نداشته باشند. در چنین فضایی

که به دلیل تحریم‌ها و رقابت‌های نظامی و تهدیدات دشمنان، امنیت در معرض خطر است، صحبت از حفظ حریم خصوصی افراد و اجرای دادرسی الکترونیکی به یک افسانه تبدیل می‌شود. هرچند دادرسی الکترونیکی امروزه از طریق برخی سامانه‌های قضایی در حال شکل‌گیری است و مردم نیز از آن استفاده می‌کنند، ولی باید توجه داشت که مسأله اعتماد با جبر و ضرورت تفاوت دارد. وقتی قانون دادرسی الکترونیکی به یک اخبار عادی تبدیل شود، به این معنی است که به جز ثبت اطلاعات و شکایت‌ها از طریق سامانه‌های الکترونیکی، گزینه‌های دیگری وجود ندارد. در این صورت، مردم ناگزیر اطلاعات خود را در اختیار افرادی قرار می‌دهند که در دفاتر این سامانه‌ها فعالیت می‌کنند و درز اطلاعات به بیرون بسیار آسان و ممکن است.

بنابراین، اعتماد افرادی که از این طریق با دولت الکترونیک یا دادگاه الکترونیکی مرتبط می‌شوند، به خطر می‌افتد و حریم خصوصی آن‌ها به راحتی نقض می‌شود. به نظر می‌رسد که بهتر است در کنار آموزش عمومی برای استفاده از سامانه‌های دادرسی الکترونیکی، کنترل این سامانه‌ها به طور کامل در دست خود افراد باشد. آن‌ها باید برای احقاق حقوق خود از وکلای معتبر و قابل اعتماد استفاده کنند و اگر وکیل غیرمجاز را به دادگاه معرفی کنند، باید تحت پیگرد قضائی قرار گیرند. همچنین، ورود به سامانه‌های دادرسی الکترونیکی باید بر اساس اطلاعات و رموزی باشد که خود افراد تعیین می‌کنند، و دسترسی به این اطلاعات شخصی باید کاملاً در اختیار خود افراد قرار گیرد. در چنین شرایطی، میزان جرایم مربوط به سرقت اطلاعات و استفاده از داده‌ها محدود خواهد شد و حریم شخصی افراد بهتر محافظت می‌شود لازم به ذکر است که استفاده از این روش مستلزم رعایت قوانین موجود در تشکیل و اصول حاکم بر دادرسی است و در برخی موارد، نیاز به اصلاح قوانین برای تطابق شرایط استفاده از دادرسی الکترونیکی با شرایط فعلی وجود دارد(رحمتی، ۱۴۰۲، ۱۲۵-۱۲۳).

نتیجه‌گیری

فرآیند دادرسی از حوزه‌هایی است که به‌دلیل ماهیتش می‌تواند حریم خصوصی افراد را با چالش‌هایی مواجه کند. این چالش‌ها به‌ویژه در دادرسی‌های الکترونیکی، که کانون تبادل اطلاعات و داده‌های الکترونیکی محسوب می‌شود، بارز است زیرا دسترسی مقامات قضائی به داده‌ها و حریم خصوصی افراد در این نوع دادرسی‌ها بیشتر از روش‌های سنتی است. به همین دلیل، ضرورت تعیین دقیق مفهوم حریم خصوصی و حدود قانونی و حقوقی آن در دادرسی‌های الکترونیکی اجتناب‌ناپذیر است. این امر در نخستین قدم مستلزم تعریف واضح مفهوم حریم خصوصی افراد است تا از سوءتفسیر و برداشت‌های نادرست مقامات قضائی محافظت شود. بر اساس قانون مجازات اسلامی، حریم خصوصی شامل انواع رفتارها و ویژگی‌های شخصی هر فرد می‌باشد.

علاوه بر این، نبود یک سیاست کیفری جامع می‌تواند ناشی از نقص‌ها و ضعف‌های قوانین اساسی و عادی در این زمینه باشد. به عنوان نمونه، در قانون اساسی ایران اصول مشخصی برای حمایت از حریم خصوصی وجود ندارد. اگر حریم خصوصی را به حوزه‌های مختلفی مانند حریم خلوت و تنهایی، حریم مکانی، حریم اطلاعات، حریم ارتباطات و حریم جسمانی تقسیم کنیم، متوجه می‌شویم که حق داشتن حریم خصوصی به‌عنوان یک حق اساسی در قانون اساسی ایران شناسایی و حمایت نشده است و مصادیق آن نه به‌طور صریح و نه به‌طور ضمنی مشخص گردیده است. همچنین، استثنائاتی مانند عدم اخلال به مبانی اسلامی و عدم تضییع حقوق دیگران، به موجب قوانین و امنیت ملی، در صورت فقدان حدود مشخص می‌تواند باعث نقض حریم خصوصی افراد شود.

نظام حقوقی ایران به‌جز کمبودهای قانونی در عرصه حمایت از حریم خصوصی، همچنین از لحاظ رویه قضایی نیز ناتوان و ناکارآمد است. تدوین قانونی جامع که شامل سیاست کیفری مؤثری به‌منظور حمایت از حریم خصوصی باشد و ایجاد رویه قضایی غنی توسط قضات در صدور احکام مربوط به حریم خصوصی، از الزامات اولیه محسوب می‌شود تا نواقص موجود در حقوق موضوعه در این حوزه اصلاح گردد.

به‌طور خلاصه، می‌توان نتیجه‌گیری کرد که سیاست کیفری ایران در زمینه حفاظت و ممانعت از نقض حریم خصوصی هنوز با استانداردهای مقبول و مورد انتظار فاصله معناداری دارد. خلأهای موجود در سیاست کیفری قانون‌گذار عمدتاً به دو بخش عمده تقسیم می‌شود: نخست، عدم وجود قانونی مستقل و جامع برای حفاظت از حریم خصوصی اطلاعات شهروندان، و قوانین فعلی نیز به‌حدود زیادی محدود به شمار می‌روند. لایحه‌ای که برای حمایت از حریم خصوصی تدوین گردیده، اگرچه می‌تواند به بهبود این خلأها کمک کند، اما همچنان بلاتکلیف مانده است. بررسی وضعیت کشورهای پیشرو در این زمینه نشان می‌دهد که تمامی این کشورها دارای قوانینی مستقل با عنوان «قانون حمایت از داده‌ها» یا «قانون صیانت از حریم خصوصی اطلاعات» هستند که الزامات حفظ حریم خصوصی اطلاعات شهروندان را برای نهادهای مختلف تعیین می‌کند. دومین خلأ کلیدی، عدم ایجاد سازمان یا نهادی مستقل از قوه قضائیه و قوه مجریه برای نظارت و پیگیری موارد نقض حریم خصوصی در فرآیند دادرسی می‌باشد. در حال حاضر، در بسیاری از کشورها، سازمان‌هایی به‌نام «دیده‌بان حریم خصوصی اطلاعات» مسئولیت نظارت بر نهادهای دولتی و غیردولتی در زمینه نقض قوانین حمایت از داده‌ها یا قوانین حفاظت از حریم خصوصی اطلاعات را برعهده دارند و از مراجع رسیدگی به شکایات شهروندان در این حوزه به‌شمار می‌آیند.

نتایج پژوهش حاضر حاکی از آن است که ترکیب پیشگیری وضعی، پیشگیری اجتماعی و ضمانت اجراهای قانونی، رویکردی جامع و مؤثر برای کاهش ریسک نقض حریم خصوصی فراهم می‌آورد. پیشگیری وضعی از طریق ابزارهای نوین فناوری، رمزنگاری داده‌ها، محدودسازی دسترسی‌ها و نظارت قضایی امکان کنترل فنی و عملیاتی داده‌ها را فراهم می‌کند. حفاظت از حریم خصوصی در دادرسی الکترونیکی، مستلزم مداخله همزمان قانون‌گذار، قوه قضاییه و جامعه است. اتخاذ سیاست‌های کیفری منسجم، اعمال ابزارهای فنی و مکانیزم‌های اجتماعی، نه تنها ریسک نقض داده‌ها را کاهش می‌دهد، بلکه اعتماد عمومی به سیستم دادرسی الکترونیکی را افزایش داده و اجرای عدالت را در کوتاه‌ترین زمان ممکن تضمین می‌کند.

پیشنهادات عملی و کاربردی

۱. رمزنگاری پیشرفته داده‌ها: تمام اطلاعات جمع‌آوری شده توسط سیستم‌های دادرسی الکترونیکی، از جمله داده‌های دستبندهای الکترونیکی، باید با الگوریتم‌های رمزنگاری قوی محافظت شوند تا از دسترسی غیرمجاز جلوگیری شود.
۲. نظارت و پایش الکترونیکی امن: استفاده از دستبندهای الکترونیکی باید همراه با پروتکل‌های امنیتی و محدودیت زمانی و مکانی باشد تا از نقض حریم خصوصی جلوگیری شود.
۳. آموزش و فرهنگ‌سازی: آموزش مستمر قضات، وکلا، مأموران تحقیقاتی و اجرای حکم درباره حفظ حریم خصوصی و مسئولیت‌های قانونی و اخلاقی آن‌ها ضروری است.
٤. تدوین قانون مستقل و جامع برای حمایت از حریم خصوصی اطلاعات که الزامات حفاظت از اطلاعات در فرایند دادرسی را مشخص نماید.

۵. ایجاد نهاد نظارتی مستقل مانند دیده‌بان حریم خصوصی اطلاعات که وظیفه پایش و نظارت بر عملکرد دستگاه‌های قضایی و دولتی در حفاظت از داده‌های شخصی را برعهده داشته باشد.

منابع

-فارسی

۱. ابوذری, مهرنوش . (۱٤۰۳). مقابله با بزهکاری در عصر هوش مصنوعی: پیش‌بینی به مثابه پیشگیری.. دوفصلنامه تحقیق و توسعه در حقوق کیفری و جرم شناسی, ۱(۲), doi: 10.22034/jclc.2025.720961

۲. احسان پور، سید رضا. (۱۳۷۸) ، کنترل الکترونیکی متهمین و مجرمین. مجله اصلاح و تربیت، ۷۹ ، ٤٥-٤۰

۳. آشوری ،محمد، میرزایی، اسدالله، (۱۳۹۱)، حقوق کیفری و توسعهٔ اقتصادی ـ صنعتی، آموزه های حقوق کیفری دوره جدید پاییز و زمستان شماره ٤

٤. پوربافرانی, حسن , حیدرپور, حمیدرضا و قاسمی, حوا . (۱٤۰٤). درآمدی بر اصول سیاست‌گذاریِ پیش‌گیرانه از جرم و ارزیابی وضعیت شناسایی آن‌ها در نظام حقوقی ایران. دوفصلنامه تحقیق و توسعه در حقوق کیفری و جرم شناسی, doi: 10.22034/jclc.2025.2052560.1159

۵. تدین, عباس . (۱۳۸۸). احترام به حریم خصوصی اشخاص در مقام تحصیل دلیل در آیین دادرسی کیفری ایران، فرانسه و رویه قضایی دیوان اروپایی حقوق بشر. دوفصلنامهٔ علمی حقوق تطبیقی, ۰(۱٦), ۸۳-۱۰٤

٦. جاویدزاده, حمیدرضا , میره ای, سیدحسن و پیوندی, غلامرضا . (۱۳۸۳). مراقبت الکترونیکی و بررسی اجمالی آن براساس آموزه‌های فقه اسلامی. حقوق اسلامی, ۱(۲), ۱۹۳-۲۲۰.

۷. حیدر نژاد، کیوان و تقی زاده، امیر، (۱٤۰۱)، جرم شناسی و تدابیر پیشگیری از جرم در حقوق کیفری ایران،دومین کنفرانس ملی حقوق، فقه و فرهنگ،شیراز

۸. رحمتی، هاشم، (۱٤۰۲)، پایان نامه کارشناسی ارشد نقض حریم خصوصی در نظام دادرسی الکترونیکی با تکیه بر جلوه ها و راهکارها ، راهنما جمال بیگی، آزاد اسلامی واحد مراغه

۹. رزنبام، دنیس؛ لوریسیو، آرتور؛ داویس، روبرت. (۱۳۷۹). «پیشگیری وضعی از جرم». مجله حقوقی دادگستری. شماره ۳۲، دوره۳، ص۱٤۷-۱۷۲.

۱۰. رییسی دزکی، لیلا، و قاسم زاده لیاسی، فلور. (۱۳۹۹). چالش های نظام حقوقی ایران در نقض داده های شخصی و حریم خصوصی در فضای سایبر. حقوقی دادگستری، ۸٤(۱۱۰)، ۱۲۳-۱٤٦.

۱۱. عبداله پور، اسماعیل، (۱۳۹٤)، پایان نامه کارشناسی ارشد، بررسی نظارت الکترونیکی و پیامدهای اجرایی آن در سیستم حقوقی ایران، استاد راهنما: ابوذر سالاری فر، دانشگاه آزاد اسلامی واحد بندرعباس - دانشکده حقوق

۱۲. عشق پور منصور اکبرپور نعمت اله ۱۳۹۵ جایگاه دادرسی الکترونیک در حقوق ایران فصلنامه مطالعات علوم اجتماعی دوره ۲، شماره ۱۳ پاییز

۱۳. فرهادی آلاشتی، زهرا، (۱۳۹۵)، پیشگیری وضعی از جرایم سایبری، تهران، نشرمیزان.

۱٤. موذن زادگان, حسنعلی و روستا, نرجس . (۱۳۹٦). دادرسی الکترونیکی در رویارویی با جرایم رایانه‌ای: چالش‌ها و بایسته‌ها. مجله حقوقی دادگستری, ۸۱(۱۰۰), ۱۹۵-۱٦۹.

-انگلیسی

15. Back, S., & LaPrade, J. (2020). Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. International Journal of Cybersecurity Intelligence & Cybercrime, 3(2), 25-47.

16. Barth S, De Jong MDT. (2017) The Privacy Paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior. Telematics and Informatics;34 (7):1038–1050.

17. Newman, G., & Clarke, R. V. (2016). Rational choice and situational crime prevention: Theoretical foundations. Routledge.

18. O'Hara K, Shadbolt N. (2019) Trust, Transparency, and the Role of Technology in Governance. The Journal of Technology in Society ;12(1):43–57
19. Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. Criminology & public policy, 18(1), 135-159.
20. Solove DJ, Schwartz PM (2020). Information Privacy Law. 6th ed. Aspen Publishers.
21. Voigt P, Von dem Bussche A. (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.

References

1) Abdollahpour, E. (2015). Master's thesis: Electronic monitoring and its executive consequences in the Iranian legal system (Advisor: A. Salarifar). Islamic Azad University, Bandar Abbas Branch.
2) Abouzari, M. (2025). Dealing with Crime in the Age of Artificial Intelligence: Prediction as Prevention. Research and development in criminal law and criminology, 1(2) .doi: 10.22034/jclc.2025.720961
3) Ashouri, M., & Mirzaei, A. (2012). Criminal law and economic–industrial development: Lessons from modern criminal law doctrines. New Era Criminal Law Teachings, 4, Autumn & Winter.
4) Back, S., & LaPrade, J. (2020). Cyber-situational crime prevention and the breadth of cybercrimes among higher education institutions. International Journal of Cybersecurity Intelligence & Cybercrime, 3(2), 25-47.
5) Barth S, De Jong MDT.) 2017) The Privacy Paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior. Telematics and Informatics;34 (7):1038–1050.
6) Eshghpour, M. A. N. (2016). The place of electronic procedure in Iranian law. Journal of Social Sciences Studies, 2(13), Autumn.
7) Farhadi Alashti, Z. (2016). Situational prevention of cybercrimes. Tehran: Mizan Publishing.
8) Heydarnejad, K., & Taghizadeh, A. (2022). Criminology and preventive measures in Iranian criminal law. 2nd National Conference on Law, Jurisprudence and Culture, Shiraz.
9) Javidzadeh, H. R., Mireh, S. H., & Peyvandi, Gh. (2004). Electronic surveillance and its review in the light of Islamic jurisprudence. Islamic Law Review, 1(2), 193-220.
10) Moazzanzadegan, H., & Rousta, N. (2017). Electronic proceedings confronting cybercrimes: Challenges and necessities. Judiciary Law Review, 81(100), 169-195
11) Newman, G., & Clarke, R. V. (2016). Rational choice and situational crime prevention: Theoretical foundations. Routledge.
12) O'Hara K, Shadbolt N. (2019) Trust, Transparency, and the Role of Technology in Governance. The Journal of Technology in Society ;12(1):43–57
13) Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2019). CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. Criminology & public policy, 18(1), 135-159.
14) Pour, S. R. (1999). Electronic monitoring of defendants and offenders. Journal of Correction and Rehabilitation, 79, 40-45.
15) Pourbafrani, H. , heydarpour, H. and Ghasemi, H. (2025). An Introduction to the Principles of Crime Prevention Policymaking and Sssessment of the Situation of Those Recognition in Iranian Legal System.). Research and development in criminal law and criminology, doi: 10.22034/jclc.2025.2052560.1159
16) Rahmati, H. (2023). Master's thesis: Violation of privacy in electronic criminal procedure with emphasis on manifestations and solutions (Advisor: J. Beigi). Islamic Azad University, Maragheh Branch.
17) Reisi Dezaki, L., & Ghasemzadeh Liasi, F. (2020). Challenges of Iranian legal system in violation of personal data and privacy in cyberspace. Judiciary Law Review, 84(110), 123-146.
18) Rosenbaum, D., Luricio, A., & Davis, R. (2000). Situational crime prevention. Judiciary Law Review, 3(32), 147-172.
19) Solove DJ, Schwartz PM (2020). Information Privacy Law. 6th ed. Aspen Publishers.
20) Tadayyon, A. (2009). Respect for individuals' privacy in the collection of evidence in criminal procedure of Iran and France, and in the case law of the European Court of Human Rights. Comparative Law Journal, 16, 83-104.
21) Voigt P, Von dem Bussche A. (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.

Prevention of Privacy Violations in Electronic Litigation Processes

Abstract

Background and Objective: Electronic litigation, as an innovative process, has significantly reduced many challenges in the judicial procedure and plays a key role in achieving the primary objective of criminal law: ensuring justice and legal accountability in the shortest possible time. This type of litigation, by minimizing temporal and spatial constraints, reducing judicial system costs, increasing the speed of case handling, improving information management, and enhancing judicial and administrative security, has brought substantial benefits to the legal system.

Despite these advantages, one of the major challenges of electronic litigation is the violation of individuals' privacy. Digital technologies, by providing extensive tools for data collection and processing, create new threats to the security of personal and professional information and underscore the urgent need for privacy protection. The present study, while examining the manifestations of privacy violations in the electronic litigation system, analyzes preventive measures against these threats across three key stages of litigation: investigation, trial, and enforcement, aiming to propose a comprehensive framework to enhance the efficiency and security of electronic litigation.

Research Method: This study employs a descriptive-analytical approach to examine various aspects of privacy protection in electronic litigation. It identifies situational, social, and legislative preventive measures and analyzes mechanisms to improve performance and strengthen public trust in the judicial system.

Findings and Results: The findings indicate that privacy in the digital space holds the same legal and ethical significance as privacy in the physical world, and safeguarding personal and professional documents and information is essential. Regarding situational prevention, electronic monitoring and judicial oversight using advanced tools are among the most effective strategies. Social prevention includes enhancing digital literacy, promoting transparency, increasing public trust, and encouraging citizen participation in oversight. From a legislative perspective, enacting an independent and effective law to protect privacy is of critical importance.

Establishing a secure and transparent electronic litigation system requires coordinated collaboration between judicial authorities and civil society, and preventive measures across the legislative, situational, and social domains must be implemented simultaneously to mitigate privacy threats and maintain public trust in the electronic judicial system.

Keywords: Privacy, Electronic Litigation, Judicial System, Prevention.