سیاست جنایی تقنینی ایران در قبال جرایم مرتبط با اینترنت اشیاء در پرتو اسناد بین‌المللی

سیده مهشید میری بالاجورشری
گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران.
s.miribalajorshari@iau.ac.ir

امیررضا محمودی(نویسنده مسئول)
گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران.
dr.mahmoudi@iau.ac.ir

بابک پورقهرمانی
گروه حقوق کیفری و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.
pourghahramani@iau.ac.ir

چکیده

امروزه گسترش اینترنت اشیاء و نقش فزاینده آن در حوزه‌های مختلف، زمینه‌ساز شکل‌گیری طیفی از جرایم نوپدید شده است که قواعد سنتی حقوق کیفری توان پاسخ‌گویی کامل به آن‌ها را ندارد. در ایران نیز قانون‌گذار عمدتاً بر رفتارهای انسانی در جرایم سایبری تمرکز دارد و جرایم ناشی از عملکرد خودکار یا نقص سامانه‌های متصل، فاقد چارچوب روشن در حوزه تعیین فاعل، سوءنیت و مسئولیت کیفری هستند. هدف این پژوهش تبیین سیاست جنایی تقنینی ایران در قبال جرایم مرتبط با اینترنت اشیاء در پرتو اسناد بین‌المللی می‌باشد. نوع تحقیق در پژوهش حاضر نظری و روش آن توصیفی- تحلیلی است. یافته‌ها نشان می‌دهد که اگرچه قوانین ایران بخش‌هایی از جرایم اینترنت اشیاء، به‌ویژه حملات مستقیم به سامانه‌ها یا استفاده از دستگاه‌های متصل به‌عنوان ابزار ارتکاب جرم را پوشش می‌دهد، اما در مواجهه با جرایم ناشی از تصمیم‌گیری خودکار سامانه‌ها با خلأهای جدی در جرم‌انگاری اختصاصی، تعیین مسئولیت کیفری و احراز عنصر معنوی مواجه است. اسناد ملی همچون مصوبه الزامات اینترنت اشیاء و دستورالعمل خودروهای متصل نیز با وجود کارکرد پیشگیرانه، فاقد ضمانت اجرای کیفری هستند. از این‌رو سیاست جنایی تقنینی ایران برای مواجهه مؤثر با این دسته از جرایم نیازمند بازنگری ساختاری و به‌روزرسانی قواعد سنتی و همسوسازی با اسناد و استانداردهای بین‌المللی است تا تقویت حمایت کیفری در حوزه اینترنت اشیاء، اعتماد عمومی به فناوری‌های نوظهور و امنیت کاربران افزایش یابد.

واژگان کلیدی: سیاست جنایی تقنینی، اینترنت اشیاء، جرایم مرتبط با اینترنت اشیاء، مسئولیت کیفری، اسناد بین‌المللی.

مقدمه

تحولات گسترده در فناوری‌های دیجیتال، به‌ویژه گسترش اینترنت اشیاء، الگوهای سنتی ارتباط، خدمات و فعالیت‌های روزمره را متحول ساخته است. اینترنت اشیاء مفهومی ناظر بر شبکه‌ای از اشیاء و تجهیزات فیزیکی است که با بهره‌گیری از حسگرها، نرم‌افزارها و بسترهای ارتباطی، قادر به تولید، جمع‌آوری، تبادل و پردازش داده‌اند و می‌توانند با حداقل مداخله انسانی یا به‌صورت خودکار واکنش نشان دهند. در این ساختار، اشیایی مانند خودروهای متصل، تجهیزات پزشکی هوشمند، لوازم خانگی، سامانه‌های صنعتی و ابزارهای پوشیدنی، از حالت ابزارهای صرفاً منفعل خارج شده و به اجزایی داده‌محور و تصمیم‌پذیر تبدیل می‌شوند. بنابراین، ویژگی اساسی اینترنت اشیاء تنها اتصال اشیاء به شبکه نیست، بلکه پیوند مستمر میان جهان فیزیکی و فضای دیجیتال و امکان ایجاد آثار واقعی بر مبنای پردازش خودکار داده‌هاست؛ ویژگی‌ای که در کنار مزایای گسترده، مسائل نوینی را در زمینه امنیت، حریم خصوصی و مسئولیت کیفری ایجاد می‌کند. در واقع اینترنت اشیاء با ایجاد بستر ارتباطی میان اشیای فیزیکی و مجازی، امکان جمع‌آوری و تحلیل خودکار داده‌ها را فراهم کرده و به یکی از زیرساخت‌های حیاتی در حوزه‌هایی همچون سلامت، حمل‌ونقل، صنعت، انرژی، امنیت و خدمات شهری تبدیل شده است. در کنار این ظرفیت‌ها، ظهور جرایم نوپدیدی که بر بستر دستگاه‌ها و سامانه‌های متصل ارتکاب می‌یابند یا از این ابزارها به‌عنوان وسیله ارتکاب جرم استفاده می‌کنند و یا توسط عملکرد خودکار سامانه‌های متصل به وقوع می‌پیوندند، چالش‌های عمیقی برای سیاست جنایی کشورها ایجاد کرده است. ویژگی‌هایی نظیر ماهیت فناورانه، قابلیت خودکار و خودمختار عمل کردن دستگاه‌ها و فرامرزی بودن بسیاری از این جرایم موجب می‌شود که قواعد و سازوکارهای سنتی تقنینی حقوق کیفری پاسخگوی مقتضیات این جرایم نباشند. اهمیت این موضوع از چند منظر قابل تبیین است: نخست آنکه اینترنت اشیاء به سرعت در حال تبدیل شدن به زیرساخت حیاتی در حوزه‌های حساس همچون سلامت، حمل‌ونقل و امنیت عمومی است و آسیب‌پذیری آن تهدیدی جدی برای جان و مال شهروندان محسوب می‌شود. دوم آنکه جرایم مرتبط با اینترنت اشیاء، به‌ویژه جرایم ناشی از عملکرد خودکار، با قواعد سنتی حقوق کیفری، که مبتنی بر رفتار انسان و قصد مجرمانه است، سازگاری کامل ندارد. سوم آنکه در فقدان چارچوب تقنینی مناسب، تعیین فاعل جرم، احراز عنصر معنوی، تعیین حدود مسئولیت کیفری و نیز واکنش کیفری متناسب با این پدیده‌ها با ابهام جدی مواجه است. در عین حال، ضرورت انجام این تحقیق زمانی آشکارتر می‌شود که پیامدهای ادامه وضعیت موجود در نظر گرفته شود. عدم توجه به این موضوع به معنای استمرار خلأهای تقنینی در این راستا خواهد بود؛ وضعیتی که نه‌تنها موجب آشفتگی حقوقی و سردرگمی مراجع رسیدگی می‌شود، بلکه می‌تواند بستر سوءاستفاده‌های مجرمانه را گسترش دهد. ابهام در انتساب مسئولیت کیفری در جرایم مرتبط با اینترنت اشیاء، فضای حقوقی نامطمئنی برای تولیدکنندگان، توسعه‌دهندگان و کاربران این فناوری‌ها ایجاد می‌کند. هدف اصلی پژوهش، تحلیل وضعیت موجود سیاست جنایی تقنینی ایران در قبال جرایم مرتبط با اینترنت اشیاء و شناسایی خلأها و چالش‌های تقنینی موجود است. جرایم مرتبط با اینترنت اشیاء از پدیده‌های نوظهور در عرصه حقوق کیفری محسوب می‌شوند که در ایران کمتر به‌صورت منسجم و نظام‌مند مورد مطالعه قرار گرفته‌اند. مطالعات موجود عمدتاً ناظر بر جنبه‌های فنی و امنیتی این فناوری بوده و ابعاد تقنینی سیاست‌گذاری جنایی آن مغفول مانده است. نوآوری این پژوهش در آن است که با تمرکز بر سیاست جنایی تقنینی ایران در قبال این جرایم و بررسی اسناد بین‌المللی به شناسایی خلأها و چالش‌های موجود می‌پردازد. این پژوهش ابتدا به تبیین چارچوب مفهومی اینترنت اشیاء و طبقه‌بندی جرایم مرتبط با آن می‌پردازد و سپس سیاست جنایی پیشگیرانه و تقنینی ایران را در در حوزه جرایم مرتبط با اینترنت اشیاء بررسی می‌کند و چالش‌ها و خلأهای تقنینی و محدودیت‌های حقوق کیفری ایران در

مواجهه با جرایم مرتبط با اینترنت اشیاء را مورد تحلیل قرار می‌دهد و همچنین به بررسی اسناد بین‌المللی مرتبط با اینترنت اشیاء می‌پردازد.

پیشینه پژوهش

حسین‌زاده و رضایی (۱۴۰۲) در مقاله‌ای با عنوان «امنیت سایبری در حوزه اینترنت اشیاء» که در فصلنامه آرمان پردازش منتشر شده است، با تمرکز بر ابعاد فناورانه و امنیتی اینترنت اشیاء، به بررسی این موضوع پرداخته‌اند که با افزایش روزافزون دستگاه‌های متصل به اینترنت، موضوع امنیت سایبری به یکی از اصلی‌ترین چالش‌ها و دغدغه‌های جامعه جهانی بدل شده است. یافته‌های مقاله بیانگر آن است که امنیت سایبری یک فرآیند مستمر و پویاست که نیازمند رویکردی چندلایه، تحلیل‌محور و پیشگیرانه است. همچنین تأکید می‌شود که ضعف در پیاده‌سازی این تدابیر می‌تواند تبعات و خسارت‌های گسترده‌ای را نیز به دنبال داشته باشد.

دیلمی معزی و همکاران (۱۴۰۱) در مقاله‌ای با عنوان «ارزیابی سیاست جنایی تقنینی ایران و اتحادیه اروپا در قبال جرایم رایانه‌ای» که در فصلنامه تحقیقات حقوقی بین‌المللی منتشر شده است، با رویکرد تطبیقی و تحلیلی، به بررسی نحوه مواجهه ایران و اتحادیه اروپا با جرایم رایانه‌ای پرداخته‌اند و تلاش می‌کنند تا تصویری جامع از سیاست‌های تقنینی دو نظام حقوقی ارائه دهند. این مقاله از نظر علمی دارای نقاط قوتی چون استفاده از منابع معتبر، تحلیل تطبیقی جامع و شناسایی دقیق کاستی‌های سیاست جنایی ایران است. اما نقاط ضعف آن تمرکز صرف بر جرایم رایانه‌ای در معنای سنتی (مانند هک و جاسوسی رایانه‌ای) است و به حوزه‌های نوین‌تر مانند جرایم ناشی از اینترنت اشیاء و چالش‌های خاص آن ورود نکرده است.

رلف و رومانا وبر[1] (۱۳۹۹) در کتابی با عنوان «چشم انداز حقوقی اینترنت اشیا» که توسط فاطمه اقدسی ترجمه شده است، توضیح می‌دهند که اینترنت اشیا یک فناوری فراملی و پیچیده است که از یک‌سو فرصت‌های گسترده‌ای برای رفاه بشر، بهداشت، امنیت غذایی و کاهش شکاف دیجیتال فراهم می‌کند و از سوی دیگر، تهدیدات و آسیب‌پذیری‌های قابل توجهی در حوزه‌های حریم خصوصی، امنیت داده‌ها و مسئولیت حقوقی به همراه دارد. نویسندگان تأکید می‌کنند که نقض امنیت داده‌ها در فضای اینترنت اشیا یک خطر جدی است و باید چارچوب‌های حقوقی روشنی برای حفاظت از داده‌ها، مسئولیت‌پذیری در قبال نقض‌ها و جبران خسارت قربانیان پیش‌بینی شود.

فابیانو[2] (۲۰۱۷) در مقاله‌ای با عنوان «اینترنت اشیاء و مسائل حقوقی مربوط به قانون حمایت از داده‌ها بر اساس مقررات عمومی جدید حفاظت از داده‌های اروپا» به بررسی ابعاد حقوقی اینترنت اشیاء در پرتو مقررات عمومی حفاظت از داده‌های اتحادیه اروپا پرداخته است. نتایج حاصل از این مقاله نشان می‌دهد که اینترنت اشیاء می‌تواند به‌طور ذاتی خطرات گسترده‌ای برای حریم خصوصی ایجاد کند و تنها از طریق به‌کارگیری الزامات سخت‌گیرانه مقررات عمومی اروپا و طراحی سامانه‌ها با رویکرد حفاظت داده‌ها از ابتدا می‌توان این خطرات را کاهش داد. تفاوت اساسی این مقاله با تحقیق حاضر در آن است که مقاله یاد شده بر ابعاد حریم خصوصی و انطباق با مقررات عمومی حفاظت از داده‌های اتحادیه اروپا متمرکز است، در حالی‌که مقاله حاضر با تأکید بر سیاست جنایی ایران به بررسی واکنش‌های تقنینی کشور در قبال جرایم مرتبط با اینترنت اشیاء و مقایسه آن با اسناد بین‌المللی می‌پردازد.

---

[1] Rolf and Romana Weber
[2]. Fabiano

۱. چارچوب مفهومی اینترنت اشیاء

برای واژه اینترنت اشیاء[3] تعاریف مختلفی وجود دارد. کوین اشتون[4] در سال ۱۹۹۹ میلادی برای نخستین بار واژه اینترنت اشیاء را به کار برد تا مفهومی نوین در پیوند میان فضای مجازی و جهان فیزیکی را تبیین نماید. وی این اصطلاح را برای توصیف سامانه‌ای مطرح ساخت که با استفاده از حسگرها، امکان برقراری ارتباط مستقیم میان اشیاء و شبکه اینترنت را فراهم می‌سازد. در چشم‌انداز ترسیم شده توسط او، اشیای بی‌جان واجد هویتی دیجیتال خواهند بود و از این طریق، قابلیت سازمان‌دهی، شناسایی و مدیریت توسط رایانه‌ها را پیدا می‌کنند. (بختیاری، ۱۴۰۱: ۵۸)

براساس تعریف اتحادیه بین المللی مخابرات[5]، اینترنت اشیاء زیر ساختی برای راه اندازی یک شبکه جهانی پویا همراه با قابلیت خود پیکربندی می‌باشد و مبتنی بر پروتکل‌های ارتباطی استاندارد و سازگار با سایر بخش‌های شبکه است. در این زیرساخت، اشیاء فیزیکی و مجازی دارای هویت مستقل، ویژگی‌های فیزیکی مشخص و شخصیت مجازی بوده و از طریق واسط‌های هوشمند، با شبکه اطلاعاتی یکپارچه شده‌اند. به عبارت دیگر اینترنت اشیاء زیرساختی جهانی برای جامعه اطلاعاتی است که با بهره‌گیری از تعامل و ارتباط میان اشیاء فیزیکی و مجازی، امکان ارائه خدمات نوین و پیشرفته را فراهم می‌سازد. (ITU-T Y2060, 2012) از سوی دیگر، سازمان همکاری و توسعه اقتصادی در تعریفی، اینترنت اشیاء را مجموعه‌ای از دستگاه‌ها و اشیائی معرفی می‌کند که وضعیت یا حالت آن‌ها می‌تواند از طریق شبکه اینترنت، با یا بدون دخالت مستقیم انسان، تغییر کند. (OECD, 2023: 12) این تعریف بر جنبه کارکردی اینترنت اشیاء تمرکز دارد و نشان می‌دهد که هدف اصلی آن، هوشمندسازی اشیای روزمره و یکپارچه‌سازی آن‌ها در بستر داده محور جهانی است. عناصر تشکیل دهنده اینترنت اشیاء عبارت است از: شیء فیزیکی، کنترل کننده‌ها، حسگرها، عملگرها[6] و اینترنت که در کنار هم نوعی هوشمندی سایبری را برای اشیاء فیزیکی به ارمغان می‌آورند. (کیان‌خواه و کریمی قهرودی، ۱۳۹۴: ۸۷)

اینترنت اشیا در زندگی روزمره به طیفی گسترده از اشیای متصل به اینترنت، از لوازم خانگی و خودروها گرفته تا تجهیزات پزشکی و... اشاره دارد که این اشیاء به حسگرها و قابلیت‌های پردازشی مجهز هستند و از طریق اتصال به شبکه می‌توانند داده‌های خود را به‌صورت مستمر تولید، جمع‌آوری و با یکدیگر مبادله کنند. داده‌های به‌دست‌آمده بدون دخالت انسان یا با حداقل مداخله انسانی پردازش و تحلیل می‌شوند و نتیجه این فرایند، ارائه خدمات متنوع و ارزش افزوده‌ای است که برای کاربران از افراد گرفته تا شرکت‌ها و جامعه سودمند خواهد بود. (ITU-T Y2060, 2012) اینترنت اشیاء که با ایجاد شبکه‌ای از اشیای فیزیکی و مجازی که از طریق حسگرها، قابلیت‌های پردازشی و اتصال به اینترنت به یکدیگر مرتبط می‌شوند، بستر ارائه خدمات هوشمند در ابعاد گوناگون زندگی فردی و اجتماعی را فراهم ساخته است. اما همین قابلیت گسترده در جمع‌آوری، پردازش و تبادل داده‌ها، زمینه‌ای تازه برای ارتکاب جرایم و سوءاستفاده‌های نوین ایجاد می‌کند که تحت عنوان جرایم مرتبط با اینترنت اشیاء شناخته می‌شوند.

۲. جرایم مرتبط با اینترنت اشیاء

جرایم مرتبط با اینترنت اشیاء عبارت‌اند از هرگونه رفتار مجرمانه‌ای که یا بر بستر دستگاه‌ها و شبکه‌های اینترنت اشیاء ارتکاب می‌یابد، یا با بهره‌گیری از این دستگاه‌ها به‌عنوان ابزار تحقق می‌یابد و یا به‌صورت خودکار و مستقل توسط عملکرد سامانه‌های اینترنت اشیاء واقع می‌شود، به‌گونه‌ای که نتیجه آن نقض حقوق کیفری یا تهدید امنیت عمومی باشد. بدین‌ترتیب، جرایم اینترنت اشیاء در مرز میان جرایم سایبری کلاسیک و جرایم فیزیکی قرار می‌گیرند و اقتضای آن دارند که سیاست جنایی نوینی متناسب با

[3] Internet of Things
[4] Kevin Ashton
[5] International Telecommunication Union (ITU)
[6] Controller, Sensors, Actuators

ماهیت فناورانه، فرامرزی و خودکار این جرایم طراحی و اجرا شود. (ENISA, 2020) جرایم مرتبط با اینترنت اشیاء با توجه به ماهیت و شیوه ارتکاب، در سه دسته اصلی قابل طبقه‌بندی‌اند:

دسته نخست جرایمی هستند که به‌طور مستقیم خود دستگاه‌ها و شبکه‌های متصل را هدف قرار می‌دهند؛ شامل جرایمی نظیر نفوذ غیرمجاز، نصب بدافزار، تخریب یا از کار انداختن سامانه‌ها و حملات بات‌نت است که اساساً متوجه امنیت و کارکرد اینترنت اشیاء می‌باشد. در نظام حقوقی ایران، غالباً مواد قانون جرایم رایانه‌ای مصوب ۱۳۸۸ ظرفیت انطباق با این دسته از جرایم را دارد.

دسته دوم، جرایمی هستند که در آن‌ها دستگاه‌های اینترنت اشیاء به‌عنوان ابزار ارتکاب جرم به‌کار گرفته می‌شوند؛ در این دسته، بزهکار از قابلیت‌های دستگاه‌های متصل برای ارتکاب جرم بهره‌برداری می‌کند؛ مانند سرقت داده‌های پزشکی، جاسوسی تصویری و صوتی از طریق دوربین‌ها و میکروفون‌های هوشمند، کلاهبرداری مبتنی بر دستکاری داده‌های حسگر، اخاذی با تهدید به انتشار تصاویر خصوصی و مواردی از این قبیل. در ایران، مقررات قانون جرایم رایانه‌ای ۱۳۸۸ و قانون مجازات اسلامی ۱۳۹۲ قابلیت پوشش این دسته را نیز دارند.

اما دسته سوم، جرایمی را دربرمی‌گیرد که از نقص فنی، خطای طراحی یا تصمیم‌گیری خودکار سامانه‌های متصل به اینترنت اشیاء ناشی می‌شوند و بدون دخالت مستقیم و آنی انسان، به تحقق نتایج مجرمانه‌ای نظیر صدمه به جان اشخاص، آسیب به اموال یا نقض حریم خصوصی می‌انجامند. وجه تمایز اساسی این دسته از جرایم آن است که کنش مادی زیان‌بار مستقیماً توسط دستگاه یا سامانه خودمختار انجام می‌شود، نه توسط عامل انسانی به‌صورت مستقیم. این ویژگی، ماهیت خاصی به جرایم مرتبط با اینترنت اشیاء می‌بخشد؛ چراکه در بسیاری از نظام‌های حقوقی، عنصر مادی جرم به‌طور سنتی در پیوند با رفتار انسانی تعریف شده است، حال آنکه در اینجا سامانه هوشمند می‌تواند منشأ فعل زیان‌بار قرار گیرد. (Hashmi et al. 2025: 291) برای مثال، در حوزه حمل‌ونقل هوشمند، خودروهای خودران یا پهپادهای هوشمند ممکن است به‌دلیل نقص الگوریتمی، ضعف امنیتی یا خطای نرم‌افزاری، موجب تصادفات رانندگی مرگ‌بار یا ورود غیرمجاز به حریم‌های هوایی حساس شوند. اختلال در سیستم ترمز یا فرمان یک خودروی متصل می‌تواند خسارات گسترده‌ای به جان و مال افراد وارد سازد، یا نقص در الگوریتم پردازش تصویر سبب عدم تشخیص عابر پیاده و بروز صدمات جبران‌ناپذیر شود. همچنین پهپادهای هوشمندی که برای خدمات پستی یا نقشه‌برداری به کار می‌روند، در صورت خطای برنامه‌ریزی مسیر ممکن است سقوط کرده و به اشخاص یا اموال آسیب برسانند. (Beck, 2016: 139) در سامانه‌های حمل‌ونقل دریایی و ریلی هوشمند نیز، خطا در سیستم‌های ناوبری یا سیگنالینگ می‌تواند منجر به برخورد وسایل نقلیه، آلودگی محیط زیست دریایی یا صدمات گسترده انسانی شود. (ENISA, 2020) افزون بر این، در حوزه نظامی و امنیتی، عملکرد نادرست سامانه‌های تسلیحاتی خودکار یا پهپادهای نظامی، در نتیجه خطای الگوریتمی یا نقص ارتباطی، ممکن است به شناسایی اشتباه اهداف و تحقق نتایجی نظیر قتل غیرعمد یا حتی نقض قواعد حقوق بشردوستانه بین‌المللی بینجامد. (ICRC, 2021)

در حوزه بهداشت و درمان نیز، نقص در ربات‌های جراحی یا تجهیزات پزشکی هوشمند، مانند پمپ‌های انسولین، ضربان‌سازهای قلب یا سامانه‌های پایش از راه دور، می‌تواند جان بیماران را به‌طور جدی به خطر اندازد. حتی در فقدان حمله سایبری، نقص فنی یا تنظیمات پیش‌فرض ناایمن ممکن است به افشای داده‌های حساس پزشکی منجر شود، یا دستگاه‌های تنظیم خودکار دوز دارو، در اثر خطای نرم‌افزاری، میزان نامناسبی از دارو را تزریق کرده و موجب مرگ یا آسیب شدید شوند. (Ahmed et al., 2024: 11) همچنین ابزارهای پوشیدنی سلامت، نظیر دستبندها و ساعت‌های هوشمند، در صورت ارسال خودکار داده‌های حساس سلامت یا موقعیت مکانی به سرورهای ناامن، می‌توانند مصداق نقض حریم خصوصی کیفری تلقی شوند.

۳. سیاست جنایی تقنینی ایران در حوزه پیشگیری از جرایم مرتبط با اینترنت اشیاء

در ایران، در حوزه اینترنت اشیاء تاکنون دو سند تدوین شده است: نخست مصوبه الزامات اینترنت اشیاء در چارچوب شبکه ملی اطلاعات (۱۳۹۷) و دوم دستورالعمل توسعه و بهره‌برداری از خودروهای متصل (۱۴۰۰) که در ادامه مورد بررسی قرار می‌گیرند.

۳-۱. مصوبه الزامات اینترنت اشیاء در چارچوب شبکه ملی اطلاعات

مصوبه «الزامات حاکم بر اینترنت اشیاء در شبکه ملی اطلاعات» مصوب ۱۳۹۷ را می‌توان از نخستین اسناد راهبردی ایران دانست که به‌طور مشخص برخی ابعاد حقوقی، فنی و مدیریتی اینترنت اشیاء را مورد توجه قرار داده است. (زیبنده و عطاردی، ۱۴۰۱: ۴۷۵) این مصوبه با تأکید بر شناسنامه‌دار شدن موجودیت‌ها و بازیگران، میزبانی خدمات در محدوده امکان اعمال حاکمیت جمهوری اسلامی ایران، حمایت از کلان‌داده‌های حاصل از اینترنت اشیاء و بومی‌سازی اجزای زیست‌بوم این فناوری، درصدد ایجاد چارچوبی کلان برای حکمرانی اینترنت اشیاء است. بااین‌حال، تحلیل این مصوبه از منظر سیاست جنایی مستلزم تفکیک میان «پیشگیری از جرم به معنای خاص»، «پیشگیری از مخاطرات و آسیب‌های فناورانه» و «تدابیر ناظر بر نظارت، کشف و تعقیب جرم» است؛ زیرا هر الزام ایمنی، مدیریتی یا امنیتی را نمی‌توان بدون احراز نحوه تأثیر آن بر علل یا فرصت‌های ارتکاب جرم، مصداق پیشگیری جرم‌شناختی تلقی کرد.

از میان مقررات این مصوبه، بند ۵ ماده ۲، که مقرر می‌دارد تمام موجودیت‌های زنجیره خدمات (اعم از کاربران، اشیاء و ارائه‌دهندگان خدمات)، با رعایت حریم خصوصی کاربران و امنیت عمومی قابل شناسایی و احراز هویت باشند، را می‌توان واجد نوعی ظرفیت پیشگیرانه وضعی دانست. احراز هویت پیشینی موجودیت‌ها می‌تواند از ناشناس‌ماندن مطلق کاربران و بهره‌برداران جلوگیری کرده و خطر ادراک‌شده شناسایی مرتکب را افزایش دهد. از این جهت، چنانچه این الزام از طریق سازوکارهای فنی روشن، متناسب و همراه با تضمین‌های حمایت از حریم خصوصی اجرا شود، ممکن است فرصت سوءاستفاده ناشناس از دستگاه‌ها و شبکه‌های اینترنت اشیاء را محدود کند. با این‌حال، قابلیت ردیابی و شناسایی، افزون بر اثر احتمالی پیشگیرانه، دارای کارکرد کشفی و اثباتی نیز هست؛ زیرا پس از وقوع جرم می‌تواند شناسایی عامل انسانی، منشأ ارتباطات و مسیر تبادل داده را تسهیل نماید.

بند ۷ ماده ۲ این مصوبه نیز مقرر می‌کند که اصول ایمنی کاربران در اتصال به شبکه اینترنت اشیاء، به‌منظور تضمین امنیت و سلامت فردی و عمومی از جنبه‌های جسمی، روانی، اقتصادی، امنیتی، اجتماعی، فرهنگی و زیست‌محیطی لحاظ شود. ماهیت این بند بیش از هر چیز ایمنی‌محور و ناظر بر مدیریت پیشینی مخاطرات فناوری است. همچنین بند ۶ ماده ۲ و پاورقی آن که توجه به آموزش، پژوهش و آگاهی‌بخشی عمومی درباره آثار اجتماعی و روانی فناوری‌های اینترنت اشیاء دارد، می‌تواند از مصادیق پیشگیری اجتماعی تلقی گردد. این بند بیانگر آن است که آگاهی و فرهنگ استفاده صحیح از فناوری در کاهش آسیب‌های ناشی از اینترنت اشیاء نقشی حیاتی دارد. درواقع آموزش کاربران و خانواده‌ها می‌تواند از وقوع رفتارهای خطرناک یا مجرمانه در این بستر جلوگیری کند.

علاوه بر آن، بند ۴ ماده ۳ ناظر بر میزبانی خدمات اینترنت اشیاء در محدوده‌ای که امکان اعمال حاکمیت جمهوری اسلامی ایران وجود داشته باشد، اساساً حکمی در زمینه حکمرانی داده، صلاحیت و کنترل زیرساخت‌هاست. میزبانی داخلی داده‌ها ممکن است

دسترسی نهادهای صلاحیت‌دار، نظارت قانونی، واکنش به رخدادهای امنیتی و جمع‌آوری ادله دیجیتال را تسهیل کند؛ اما به‌خودی‌خود موجب کاهش آسیب‌پذیری فنی سامانه‌ها یا جلوگیری از وقوع جرم نمی‌شود. میزان امنیت یک سامانه بیش از محل جغرافیایی میزبانی، به معماری امنیتی، نحوه مدیریت دسترسی، رمزنگاری، به‌روزرسانی، نظارت مستمر و رعایت استانداردهای فنی وابسته است. ازاین‌رو، این بند را باید عمدتاً در زمره تدابیر حاکمیتی و تسهیل‌کننده نظارت و اجرای قانون قرار داد و تنها در صورت همراهی آن با الزامات امنیتی مشخص، برای آن آثار پیشگیرانه غیرمستقیم قائل شد.

بند ۵ ماده ۳ نیز کلان‌داده‌های تجمیع شده از کاربران را به‌مثابه دارایی ملی تلقی کرده و آن‌ها را مشمول الزامات حمایت از داده می‌داند. صرف شناسایی داده‌ها به‌عنوان دارایی ملی، بدون تعیین اصول پردازش، حدود دسترسی، تکالیف امنیتی، ضمانت اجراهای نقض داده و حقوق اشخاص موضوع داده، برای پیشگیری از جرایم مرتبط با داده کافی نیست. با این‌حال، این حکم از آن جهت که مبنایی برای وضع مقررات حمایتی و امنیتی آینده فراهم می‌کند، می‌تواند دارای ظرفیت تقنینی و پیشگیرانه باشد. تحقق این ظرفیت منوط به تدوین قواعد الزام‌آور درباره جمع‌آوری، پردازش، نگهداری، انتقال و افشای داده‌های حاصل از دستگاه‌های متصل است.

بر این اساس، مصوبه الزامات حاکم بر اینترنت اشیاء را نمی‌توان به‌طور کلی و بدون تفکیک مفاد آن، سندی جامع در زمینه پیشگیری وضعی یا اجتماعی از جرایم اینترنت اشیاء دانست. این مصوبه بیش از آنکه متضمن یک الگوی منسجم پیشگیری از جرم باشد، سندی تنظیم‌گرانه، ایمنی‌محور و حاکمیتی است که برخی احکام آن، به‌ویژه الزام به شناسایی و احراز هویت موجودیت‌ها، می‌توانند ظرفیت پیشگیرانه داشته باشند و برخی دیگر صرفاً زمینه فنی، حقوقی یا نهادی لازم برای اقدامات پیشگیرانه آینده را فراهم می‌کنند. در عین حال، مصوبه در زمینه جرم‌انگاری رفتارهای پرخطر، تعیین مسئولیت کیفری تولیدکنندگان، طراحان، عرضه‌کنندگان، اپراتورها و کاربران، گزارش‌دهی اجباری رخدادهای امنیتی، حفظ و پردازش ادله دیجیتال، تعیین استانداردهای امنیتی لازم‌الاجرا و همکاری قضایی فرامرزی فاقد مقررات روشن است. همچنین برای نقض الزامات کلی آن ضمانت اجراهای کیفری یا اداری مشخصی پیش‌بینی نشده است. در نتیجه، این سند را می‌توان بخشی از سیاست تنظیمی و غیرکیفری ایران با جهت‌گیری کلی ایمنی و کاهش مخاطرات دانست، اما نمی‌توان آن را جایگزین یک سیاست جنایی تقنینی منسجم و مبتنی بر تعریف دقیق پیشگیری از جرم قلمداد کرد.

۳-۲. دستورالعمل توسعه و بهره‌برداری از خودروهای متصل

دستورالعمل «به‌کارگیری خدمات شبکه‌های ارتباطی برای کمک به توسعه صنعت خودروهای متصل» مصوب ۱۴۰۰، یکی از اسناد تنظیم‌گرانه ایران درباره یکی از مهم‌ترین مصادیق اینترنت اشیاء یعنی خودروهای متصل است. این دستورالعمل با تعریف ارکان زیست‌بوم خودروهای متصل (کارور، جعبه ارتباطی، خودروی متصل، فروشنده و سامانه‌های دادگان) و تعیین مجموعه‌ای از الزامات فنی و قراردادی، تلاش دارد چارچوبی برای بهره‌برداری ایمن و نظام‌مند از داده‌های تولیدشده در صنعت خودروهای هوشمند فراهم آورد. با این‌حال، تحلیل آن از منظر سیاست جنایی مستلزم تفکیک میان تدابیر پیشگیرانه، اهداف کلی سند و سازوکارهای مربوط به نظارت و کشف جرم است.

برخی الزامات بند ۳ این دستورالعمل را می‌توان واجد ظرفیت پیشگیرانه وضعی دانست؛ زیرا اجرای آن‌ها ممکن است آسیب‌پذیری سامانه‌ها، امکان دسترسی غیرمجاز یا فرصت سوءاستفاده از داده‌های خودرو را کاهش دهد. بند ۳ـ۲ کارورها را مکلف می‌کند برای

هر قرارداد، سامانه اختصاصی فیزیکی یا منطقی ایجاد و نظام دسترسی مربوط به آن را به‌صورت مستقل تعریف کنند. این تفکیک می‌تواند دسترسی غیرمجاز و سرایت رخدادهای امنیتی میان سامانه‌ها را محدود سازد.

همچنین مطابق بندهای ۳ـ۴ـ۱ و ۳ـ۴ـ۲، کارورها موظف‌اند فناوری‌ها و سازوکارهای مربوط به حریم خصوصی و امنیت سایبری را درباره سیم‌کارت‌های مورد استفاده در خدمات خودروهای متصل اعمال کنند. این مقررات می‌توانند از طریق کاهش آسیب‌پذیری سامانه‌ها و دشوار کردن دسترسی غیرمجاز، واجد کارکرد پیشگیرانه باشند؛ هرچند دستورالعمل درباره موضوعاتی مانند رمزنگاری، احراز هویت، ثبت وقایع، به‌روزرسانی امنیتی و مدیریت آسیب‌پذیری‌ها معیار مشخصی ارائه نکرده است.

بند ۳ـ۵ نیز حق بهره‌برداری پردازش داده‌ها را تابع قرارداد با فروشنده و رضایت مالک خودرو قرار می‌دهد. این الزام می‌تواند پردازش داده‌های خودرو بدون مبنای قراردادی یا رضایت مالک را محدود کند و از این جهت واجد کارکرد حمایت از حریم خصوصی و کاهش خطر بهره‌برداری غیرمجاز از داده‌ها می‌باشد. همچنین بند ۳ـ۷ـ۱ ارائه داده‌های خام ثبت شده در سامانه به طرف‌های ثالث را ممنوع نموده و مقرر می‌کند که اطلاعات پس از پردازش و در قالب بسته استنتاجی ارائه شوند. این ممنوعیت می‌تواند احتمال بهره‌برداری مجرمانه از داده‌های خام را کاهش دهد. بند ۳ـ۷ـ۲ نیز ارائه اطلاعات انبوه را منوط به گمنام‌سازی کرده است. گمنام‌سازی، در صورتی که به‌صورت مؤثر و غیرقابل بازگشت انجام شود، می‌تواند خطر افشای هویت و نقض حریم خصوصی را کاهش دهد. با این‌حال، معیارهای فنی گمنام‌سازی و ضمانت اجرای نقض این الزامات مشخص نشده است.

در مقابل، بندهای ۳ـ۶ و ۳ـ۸ عمدتاً دارای کارکرد نظارتی و کشف جرم هستند. مطابق بند ۳ـ۶، مشخصات خودرو و سیم‌کارت باید به فرماندهی انتظامی ارائه و سیم‌کارت جعبه ارتباطی به کد ملی منتسب شود. این سازوکار ممکن است با افزایش احتمال شناسایی، اثر بازدارنده غیرمستقیم داشته باشد، اما کارکرد اصلی آن تسهیل ردیابی و شناسایی است. البته انتساب سیم‌کارت به مالک لزوماً به معنای انتساب رفتار به مرتکب واقعی نیست؛ زیرا ممکن است استفاده‌کننده خودرو شخص دیگری باشد.

بند ۳ـ۸ نیز کارورها را موظف کرده است نیازهای داده‌ای مربوط به امنیت ملی و مدیریت جرایم و تخلفات را در اختیار متقاضیان حاکمیتی قرار دهند. این بند زیرساخت دسترسی نهادهای حاکمیتی به داده‌ها را برای شناسایی، تحلیل، مدیریت و پیگیری جرایم و تخلفات فراهم می‌کند.

برخی اهداف بند ۲ این دستورالعمل نیز ظرفیت بالقوه پیشگیرانه دارند. برای مثال، بند ۲ـ۸ به سلامت رانندگی و تشخیص جرایم و تخلفات و بند ۲ـ۹ به ترویج فرهنگ و هنجارهای مطلوب ترافیکی اشاره می‌کند. تشخیص جرم و تخلف اصولاً در قلمرو کشف و نظارت قرار دارد. ترویج فرهنگ ترافیکی نیز تنها در صورتی مصداق پیشگیری اجتماعی است که در قالب برنامه‌های آموزشی و اصلاح رفتار مشخص اجرا شود.

در کنار ظرفیت‌های یادشده، دستورالعمل با کاستی‌هایی مواجه است. نخست، چارچوب مشخصی برای تعیین مسئولیت تولیدکننده خودرو، سازنده جعبه ارتباطی، فروشنده خدمات، کارور، توسعه‌دهنده نرم‌افزار و کاربر در صورت نقص فنی، ضعف امنیتی یا پردازش غیرمجاز داده‌ها ارائه نمی‌کند. دوم، هرچند بند ۳ـ۴ـ۳ به نگهداری داده‌ها و بند ۳ـ۴ـ۴ به دسترسی در شکایات و ارجاعات قضایی اشاره دارد، لکن مقررات جامعی درباره تمامیت ادله دیجیتال، زنجیره حفاظتی، مدت نگهداری، ثبت دسترسی‌ها و قابلیت استناد قضایی پیش‌بینی نشده است. سوم، دستورالعمل تکلیف مشخصی برای گزارش‌دهی رخدادهای امنیتی، افشای آسیب‌پذیری‌ها و اطلاع‌رسانی به کاربران تعیین نکرده و ضمانت اجرای روشنی برای نقض الزامات امنیتی و حریم خصوصی ندارد.

در مجموع، دستورالعمل خودروهای متصل را باید سندی تنظیم‌گرانه با برخی ظرفیت‌های پیشگیرانه دانست. این دستورالعمل اگرچه گامی مثبت در تنظیم زیست‌بوم خودروهای متصل است، اما برای پیوند منسجم با سیاست جنایی تقنینی، نیازمند تکمیل از طریق قوانین بالادستی، استانداردهای امنیتی الزام‌آور، نظام روشن مسئولیت و ضمانت اجراهای متناسب است.

۴. چالش‌های سیاست جنایی تقنینی ایران در قبال جرایم مرتبط با اینترنت اشیاء

در ایران جرایمی که از تصمیم‌گیری خودکار سامانه‌های متصل ناشی می‌شوند و بدون دخالت مستقیم انسان، منجر به تحقق نتایج مجرمانه‌ای می‌گردند، یعنی دسته سوم از جرایم مرتبط با اینترنت اشیاء، با چالش‌ها و خلأهای بسیاری مواجه می‌باشند که در ادامه مورد بررسی قرار خواهند گرفت.

۴-۱. چالش شناسایی فاعل جرم و انتساب مسئولیت کیفری

نخستین چالش بنیادین در این حوزه، مسأله شناسایی فاعل جرم است. در نظام حقوق کیفری ایران، عنصر مادی جرم به رفتار انسانی گره خورده است و در نتیجه دستگاه یا سامانه خودکار نمی‌تواند به‌عنوان فاعل جرم شناخته شود. این در حالی است که در عمل، رفتار زیان‌بار مستقیماً توسط سامانه هوشمند واقع می‌شود. بدین ترتیب، سیاست جنایی ایران در تعیین فاعل و مسئول اصلی چنین جرایمی با چالش جدی مواجه است. در واقع یکی از اساسی‌ترین ابهامات در حوزه جرایم مرتبط با اینترنت اشیاء، تعیین مسئولیت کیفری در مواردی است که رفتار زیان‌بار مستقیماً توسط دستگاه واقع می‌شود و عامل انسانی در لحظه وقوع جرم مداخله‌ای ندارد که در این خصوص مسئولیت کیفری میان سازنده، برنامه‌نویس، کاربر یا حتی نهاد ناظر محل مناقشه خواهد بود.

استدلال می‌شود که اگر نقص در طراحی یا ضعف امنیتی دستگاه موجب ارتکاب جرم شده، سازنده یا برنامه‌نویس باید مسئول شناخته شود. در حقوق ایران چنین مسئولیتی در سطح کیفری به‌صراحت پیش‌بینی نشده است و بیشتر در چارچوب مسئولیت مدنی قابل طرح است. از سوی دیگر برخی نظریات عرضه‌کننده یا توزیع‌کننده را به دلیل عدم رعایت استانداردهای ایمنی مسئول می‌دانند. در ایران با اینکه قانون حمایت از حقوق مصرف‌کنندگان ۱۳۸۸ مقرر کرده است که تولیدکننده یا عرضه‌کننده در صورت معیوب بودن کالا و ورود خسارت به مصرف‌کننده، علاوه بر جبران خسارت، به جزای نقدی محکوم خواهد شد، اما این ضمانت اجرا صرفا محدود به روابط مصرف‌کننده و عرضه‌کننده می‌باشد و پاسخگوی تمامی مصادیق این دسته از جرایم اینترنت اشیاء، خصوصاً در مواردی که اشخاص ثالث غیرمصرف‌کننده متضرر می‌شوند، نیست.

در حقوق ایران، به دلیل فقدان چارچوب قانونی ویژه، غالباً مسئولیت به کاربر یا مالک دستگاه منتقل می‌شود، که این رویکرد نه‌تنها با عدالت کیفری تعارض دارد، بلکه می‌تواند اعتماد عمومی به فناوری‌های نوین را تضعیف کند. در نظام‌های حقوقی‌ای مانند آلمان و اتریش که از یک نظام جامع مسئولیت مبتنی بر ریسک در خصوص وسایل نقلیه موتوری حمایت می‌کنند، اگر خطای نرم‌افزاری در یک خودرو خودران منجر به وقوع تصادف شود، این وضعیت به منزله نقص در کیفیت وسیله نقلیه تلقی می‌گردد؛ زیرا مطابق قواعد مسئولیت محصول، تولیدکننده مسئول آسیب‌هایی است که بر اثر نقص یا عیب محصول به افراد وارد می‌شود. در واقع فرد زیان‌دیده همواره امکان طرح دعوا علیه دارنده وسیله نقلیه را دارد و دارنده یا مالک وسیله نقلیه که بر پایه قواعد سنتی مسئول شناخته می‌شود، همواره حق رجوع و طرح دعوا علیه تولیدکننده را خواهد داشت. (لوسه و همکاران، ۱۴۰۲: ۱۱۱)

برخی حقوقدانان حوزه حقوق خصوصی و حقوق بیمه درباره مسئله صدمات ایجاد شده توسط ربات ها بحث‌هایی را مطرح کرده‌اند. این حقوقدانان پیشنهاد کردند که عامل هوشمند خودش باید در قبال صدماتش مسئول باشد (بر اساس سیستم مسئولیت مطلق). برخی از حقوقدانان نیز پیشنهاد دادند یک صندوق خصوصی یا سیستم بیمه برای جبران خسارت کسانی ایجاد شود که در اثر عملکرد ربات‌ها به آن‌ها صدمه وارد می‌شود. (Gless, 2016: 414) برخی نیز معتقدند که در جرایم ارتکابی توسط دستگاه‌های متصل به اینترنت مثل خودروهای خودران، کاربر خودرو که هیچ نقشی در کنترل خودرو ندارد، اصولاً مسئولیتی هم در خصوص صدمات ایجاد شده توسط آن ندارد و مسئولیت بر تولیدکننده بار می‌شود، مگر اینکه در رابطه با نتیجه عملکرد خودروی خودران مرتکب تقصیری شده باشد که در این صورت کاربر خودران مبتنی بر تسبیب دارای مسئولیت است. (برزگر و الهام، ۱۳۹۹: ۲۲۶) در ایران مسئولیت کیفری مربوط به جرایم ارتکابی توسط اینترنت اشیاء هنوز به طور مشخص تعریف نشده است و قوانین موجود عمدتاً بر اساس مسئولیت فردی و تقصیر بنا شده‌اند. از این رو فقدان قوانین اختصاصی در این حوزه باعث ایجاد خلا قانونی شده است.

۴-۲. چالش احراز عنصر معنوی در جرایم ناشی از سامانه‌های اینترنت اشیاء

چالش مهم دیگر، ناظر بر احراز عنصر معنوی است. حقوق کیفری متعارف بر پایه قصد مجرمانه یا تقصیر انسانی استوار است، اما در مواردی مانند خطای الگوریتم خودرو خودران یا نقص نرم‌افزاری ربات جراحی، اساساً قصد یا سوءنیت انسانی در لحظه وقوع حادثه وجود ندارد. (هالوی، ۱۳۹۸: ۱۳۳) انتساب سوءنیت به طراح یا تولیدکننده نیز دشوار است، زیرا غالباً نقص ناشی از پیچیدگی فناوری و خطای پیش‌بینی‌ناپذیر سامانه است. در چنین شرایطی، مقررات فعلی ایران عموماً این وقایع را در زمره جرایم غیرعمدی قرار می‌دهد، اما این رویکرد پاسخ‌گوی ماهیت خاص جرایم ناشی از عملکرد خودکار سامانه‌های هوشمند نیست.

۴-۳. چالش ماهیت فراملی جرایم مرتبط با اینترنت اشیاء و ضعف همکاری بین‌المللی

ماهیت فراملی بسیاری از جرایم مرتبط با اینترنت اشیاء یکی دیگر از چالش‌هایی است که در این راستا باید به آن اشاره نمود. بسیاری از جرایم مرتبط با اینترنت اشیاء به دلیل ماهیت شبکه‌ای و جهانی فناوری، ابعادی فرامرزی دارند (مثل نقص یک دستگاه به‌روزرسانی‌شده از سرور خارجی) در حالی که ایران هنوز چارچوب حقوقی مشخصی برای همکاری‌های بین‌المللی در این حوزه ندارد، اما اسناد بین‌المللی نظیر کنوانسیون بوداپست، دستورالعمل امنیت شبکه و اطلاعات اتحادیه اروپا و توصیه‌های آژانس امنیت سایبری اروپا و... چارچوب‌های مشخصی برای پیشگیری، جرم‌انگاری و همکاری‌های بین‌المللی ارائه کرده‌اند، سیاست جنایی ایران فاقد همسویی نظام‌مند با این اسناد است. این خلأ در همکاری بین‌المللی و در واقع عدم هماهنگی با اسناد بین‌المللی، تعقیب کیفری و جبران خسارت در مواردی که عناصر فرامرزی دخیل هستند را با دشوارهای جدی مواجه می‌سازد.

۴-۴. چالش محدودیت و ناکارآمدی قوانین موجود در پوشش جرایم مرتبط با اینترنت اشیاء

دامنه قوانین موجود در ایران در این راستا بسیار محدود است. قانون جرایم رایانه‌ای مصوب ۱۳۸۸ اساساً بر رفتارهای انسانی نظیر نفوذ، تخریب و شنود و... متمرکز است و هیچ اشاره‌ای به مسئولیت ناشی از نقص یا تصمیم‌گیری خودکار دستگاه‌های متصل ندارد. در زمینه مسئولیت کیفری اشخاص حقوقی نیز ماده ۱۹ قانون جرایم رایانه‌ای (ماده ۷۴۷ قانون مجازات اسلامی) مقرر می‌دارد

هرگاه جرم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، در مواردی مانند ارتکاب یا صدور دستور جرم از سوی مدیر، ارتکاب جرم توسط کارمند با اطلاع مدیر یا در اثر عدم نظارت وی و یا اختصاص تمام یا بخشی از فعالیت شخص حقوقی به جرم رایانه‌ای، شخص حقوقی دارای مسئولیت کیفری خواهد بود. با این‌حال، قلمرو این مسئولیت محدود است و در مواردی که نتیجه زیان‌بار صرفاً از نقص طراحی، آسیب‌پذیری امنیتی، خطای نرم‌افزاری یا تصمیم‌گیری خودکار دستگاه ناشی شده و رفتار مجرمانه شخص حقیقی معینی قابل احراز نباشد، این ماده پاسخ روشنی ارائه نمی‌کند.

در قانون مجازات اسلامی مصوب ۱۳۹۲ نیز بند «پ» ماده ۲۹۱، که جنایت ناشی از تقصیر مرتکب را شبه‌عمدی می‌داند، ممکن است در مواردی قابل اعمال باشد که نتیجه زیان‌بار سامانه بر اساس قواعد عمومی سببیت به تقصیر شخص معینی، مانند تولیدکننده، طراح، برنامه‌نویس، اپراتور یا کاربر، منتسب شود. با این‌حال، این ماده درباره معیار تشخیص تقصیر فنی، نحوه انتساب رفتار خودکار دستگاه و چگونگی توزیع مسئولیت میان بازیگران متعدد زیست‌بوم اینترنت اشیاء حکم مشخصی ارائه نمی‌کند. در واقع مواد قانون مجازات اسلامی ناظر به رفتارهای انسانی است و برای پوشش جرایم پیچیده‌ای که توسط دستگاه‌های متصل به اینترنت واقع می‌شود، کارآمد نمی‌باشد.

قانون حمایت از حقوق مصرف‌کنندگان مصوب ۱۳۸۸ نیز (مواد ۱۸ و ۱۹) برای تولیدکنندگان و عرضه‌کنندگان کالاهای معیوب در صورت ورود خسارت به مصرف‌کننده، صرفاً جزای نقدی و جبران خسارت را مقرر کرده است. قانون تجارت الکترونیک مصوب ۱۳۸۲ نیز در باب چهارم صرفا به جرایمی مانند کلاهبرداری کامپیوتری، جعل کامپیوتری، نقض حفاظت از داده پیام در بستر مبادلات الکترونیکی پرداخته است که این مقررات عمدتاً رفتار انسانی را هدف گرفته‌اند و نه عملکرد خودکار دستگاه‌های متصل. ماده ۷۸ این قانون، مسئولیت مدنی مؤسسات را در قبال خسارات ناشی از نقص سیستم‌ها پذیرفته است. در واقع این ماده مسئولیت ناشی از نقص یا ضعف سیستم‌های خودکار را به رسمیت می‌شناسد اما ضمانت اجرای آن صرفاً مدنی و جبران خسارت است و هیچ جنبه کیفری برای چنین وضعیتی پیش‌بینی نشده است و از حیث سیاست جنایی کیفری ساکت است. هیچ‌یک از این قوانین جرم‌انگاری صریح یا مسئولیت کیفری ویژه‌ای برای جرایم ناشی از عملکرد خودکار دستگاه‌های اینترنت اشیاء پیش‌بینی نکرده‌اند. بنابراین، حقوق کیفری ایران همچنان با خلأ جدی در این حوزه روبه‌روست و در عمل ناچار است از قواعد عمومی مسئولیت مدنی یا جرایم غیرعمدی بهره گیرد؛ امری که نه با ماهیت فناورانه و فرامرزی این جرایم سازگار است و نه می‌تواند عدالت کیفری و بازدارندگی لازم را تأمین کند. (میرلوحی، ۱۴۰۵: ۱۹۲)

به‌طور کلی، سیاست جنایی تقنینی ایران در قبال جرایم مرتبط با اینترنت اشیاء بیش از آنکه بر پایه یک رویکرد جامع و آینده‌نگر باشد، بر قوانین سنتی و پراکنده متکی بوده و فاقد انسجام، جامعیت و نگاه آینده‌نگر است. این سیاست تنها بخشی از مصادیق جرایم دسته اول (یعنی حملات مستقیم به دستگاه‌ها و شبکه‌ها) و تا حدی جرایم دسته دوم (استفاده از دستگاه‌ها به‌عنوان ابزار ارتکاب جرم) را پوشش می‌دهد و در قبال جرایم دسته سوم، یعنی جرایمی که از تصمیم‌گیری خودکار سامانه‌ها ناشی می‌شوند، با خلأ جدی مواجه است. در واقع این چالش‌ها ضرورت بازاندیشی در اصول سنتی حقوق کیفری ایران و همگرایی با استانداردهای بین‌المللی را بیش از پیش آشکار می‌سازد. بنابراین، اصلاح قوانین موجود و تدوین سیاست جنایی نوین که همسو با اسناد و استانداردهای بین‌المللی باشد، ضرورتی اجتناب‌ناپذیر است.

۵. اسناد و استانداردهای بین‌المللی در سیاست‌گذاری تقنینی اینترنت اشیاء

تحولات شتابان فناوری و گسترش اینترنت اشیاء موجب شده است که نظام‌های حقوقی مختلف برای مقابله با تهدیدات ناشی از این فناوری، مجموعه‌ای از اسناد، مقررات و استانداردهای بین‌المللی را تدوین و اجرا کنند که تحلیل تطبیقی اسناد بین‌المللی می‌تواند مسیر اصلاح و تقویت سیاست جنایی تقنینی ایران را روشن سازد. در عرصه بین‌المللی، طیف متنوعی از اسناد و مقررات در حوزه جرایم سایبری و به‌طور خاص امنیت و مسئولیت در حوزه اینترنت اشیاء شکل گرفته است. (عابدیان و احمدی، ۱۳۹۱: ۱۲۸-۱۲۹) برخی از این اسناد ماهیت الزام‌آور دارند و صرفاً پس از الحاق رسمی کشورها تعهدآور می‌شوند، در حالی که گروه دیگری از اسناد در قالب اسناد حقوقی نرم و توصیه‌نامه‌های بین‌المللی به‌طور مستقیم الزام‌آور نیستند، اما عملاً نقش الگویی و اثرگذاری قابل توجه بر سیاست‌گذاری‌های داخلی ایفا می‌کنند.

۵-۱. کنوانسیون بوداپست درباره جرایم سایبری

یکی از مهم‌ترین اسناد بین‌المللی در این حوزه، کنوانسیون بوداپست درباره جرایم سایبری[7] ۲۰۰۱ و پروتکل الحاقی آن در سال ۲۰۰۳ است که بنیان همکاری فرامرزی در تحقیقات جنایی، استرداد مجرمان، دسترسی به ادله دیجیتال و جرم‌انگاری رفتارهای اساسی سایبری را فراهم کرده است. (پورقهرمانی و کتانچی، ۱۳۹۸: ۳۱) اگرچه این سند مستقیماً به اینترنت اشیاء نپرداخته، اما رفتارهای مجرمانه‌ای که در بستر اینترنت اشیاء رخ می‌دهد، از جمله دسترسی غیرمجاز، شنود، تخریب داده‌ها و حمله به سامانه‌های کنترل، در چارچوب آن قابل پیگیری است. ایران با وجود تأثیرپذیری غیرمستقیم قانون جرایم رایانه‌ای از این کنوانسیون، هنوز فاقد سازوکارهای کارآمدی برای همکاری‌های فرامرزی، استرداد مجرمان و جمع‌آوری ادله دیجیتال پیچیده مربوط به سامانه‌های متصل است و این امر یکی از موانع مهم در پیگیری جرایم فرامرزی اینترنت اشیاء به شمار می‌آید. (دیلمی معزی و همکاران، ۱۴۰۰: ۱۱۴) همسویی با این سند می‌تواند ظرفیت حقوقی ایران را برای مقابله با حملات فرامرزی به زیرساخت‌ها و دستگاه‌های متصل تقویت کند.

۵-۲. قانون تاب‌آوری سایبری اتحادیه اروپا

قانون تاب‌آوری سایبری اتحادیه اروپا مصوب[8] ۲۰۲۴ مقرره‌ای جامع در سطح اتحادیه اروپا است که الزامات امنیتی برای تمامی محصولات دارای مؤلفه دیجیتال، از جمله دستگاه‌های اینترنت اشیاء، را تعیین می‌کند. این مقرره تکالیفی همچون طراحی امن، مدیریت ریسک سایبری در چرخه عمر محصول، ارائه به‌روزرسانی‌های امنیتی در دوره پشتیبانی، سازوکار گزارش‌دهی آسیب‌پذیری‌ها و الزامات ارزیابی تطابق و نظارت بر بازار را برای تولیدکنندگان پیش‌بینی کرده است. هدف اصلی آن کاهش آسیب‌پذیری‌های ذاتی محصولات متصل و پیشگیری از بهره‌برداری‌های مجرمانه، به‌ویژه در حوزه اینترنت اشیاء، است که به دلیل پیوند مستقیم با زندگی روزمره شهروندان و زیرساخت‌های حیاتی، اهمیت ویژه‌ای دارد. (Cyber Resilience Act, 2024) اگرچه این مقرره برای ایران الزام‌آور حقوقی نیست، اما هر تولیدکننده یا صادرکننده ایرانی که قصد ورود به بازار اروپا را داشته باشد، ناگزیر به رعایت این مقرره خواهد بود. در واقع این مقرره به‌عنوان یک هنجار بین‌المللی می‌تواند به‌طور غیرمستقیم بر ایران اثرگذار باشد؛ چرا که استانداردهای امنیتی مقرر در آن به مرور به معیارهای جهانی تبدیل خواهند شد و فقدان چارچوب مشابه در ایران،

[7] Convention on Cybercrime (Budapest Convention)
[8] Cyber Resilience Act (CRA)

ضمن ایجاد مانع برای تعاملات تجاری، اعتماد به نظام حقوقی داخلی در حوزه امنیت و مسئولیت اینترنت اشیاء را کاهش خواهد داد. بنابراین، این مقرره گرچه در ایران الزام‌آور نیست، اما الگویی مهم برای سیاست‌گذاری تقنینی به شمار می‌آید و می‌تواند مبنای تدوین مقررات ملی در زمینه امنیت و مسئولیت کیفری و مدنی دستگاه‌های اینترنت اشیاء قرار گیرد.

۵-۳. مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا

مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا[9] ۲۰۱۶، سخت‌گیرانه‌ترین چارچوب حقوقی بین‌المللی در زمینه حفاظت از داده‌ها و امنیت سایبری به شمار می‌رود. اگرچه ایران الزام حقوقی به رعایت آن ندارد، اما به‌دلیل اصل صلاحیت فراسرزمینی، هرگونه فعالیت شرکت‌ها و نهادهای ایرانی که متضمن پردازش داده‌های شهروندان اروپایی یا ارائه خدمات به بازار اتحادیه اروپا باشد، در عمل به طور غیرمستقیم تحت شمول الزامات آن قرار می‌گیرد. این مقررات به‌عنوان هنجار جهانی حفاظت از داده، از طریق فشارهای بازار، تعاملات تجاری و الزامات فنی، بر روی فعالیت‌های مرتبط با اینترنت اشیاء در ایران به‌طور غیرمستقیم اثرگذار بوده و در عمل برخی کسب‌وکارها و نهادهای ایرانی برای حضور در بازار بین‌المللی ناگزیر به انطباق نسبی با استانداردهای آن شده‌اند که این موضوع موجب بروز چالش‌های جدی در همکاری‌های بین‌المللی و تعاملات فرامرزی در حوزه اینترنت اشیاء می‌شود. (قناد و شریف، ۱۴۰۰: ۱۹) این وضعیت ضرورت بازنگری و تدوین چارچوبی منسجم و همسو با استانداردهای بین‌المللی را در سیاست جنایی ایران آشکار می‌سازد.

دستورالعمل امنیت شبکه و اطلاعات اتحادیه اروپا[10] ۲۰۱۶ و نسخه بازنگری‌شده آن[11] ۲۰۲۲ چارچوبی جامع برای الزامات امنیت سایبری در خدمات و زیرساخت‌های حیاتی، از جمله اینترنت اشیاء، ارائه می‌دهد. این دستورالعمل نیز برای ایران الزام‌آور نیست، اما استانداردهای مندرج در آن به‌ویژه در حوزه امنیت زیرساخت‌ها و حملات فرامرزی، می‌تواند مورد توجه سیاست‌گذاران امنیت سایبری قرار بگیرد.

۵-۴. توصیه‌نامه‌های اتحادیه بین‌المللی مخابرات

توصیه‌نامه‌های اتحادیه بین‌المللی مخابرات نظیر توصیه‌نامه آی تی یو- تی وای[12] ۲۰۶۰ که تعاریف و چارچوب‌های فنی اینترنت اشیاء را ارائه می‌دهد، برای ایران که عضو اتحادیه بین‌المللی مخابرات است از اهمیت ویژه‌ای برخوردار است. این توصیه‌نامه اصولی را مطرح می‌سازد که جنبه‌ای پیشگیرانه در برابر جرایم مرتبط با این فناوری دارند. این سند با تأکید بر مدیریت هویت و شناسه‌گذاری یکتا برای اشیاء متصل به منظور افزایش قابلیت رهگیری، امنیت در طراحی[13]، رمزنگاری و کنترل دسترسی ایمن برای حفاظت از داده‌ها، رعایت اصول حریم خصوصی و استانداردسازی ارتباطات میان دستگاه‌ها، زمینه کاهش آسیب‌پذیری و سوءاستفاده‌های احتمالی را فراهم می‌کند. هرچند این توصیه‌نامه الزام‌آور حقوقی نیست، اما به‌عنوان مرجع فنی معتبر، مبنای تدوین سیاست‌های ملی در حوزه پیشگیری فناورانه از جرایم اینترنت اشیاء محسوب شده و می‌تواند به عنوان پایه‌ای برای سیاست جنایی پیشگیرانه در ایران برای مقابله با جرایم نوپدید مبتنی بر اینترنت اشیاء مورد استناد قرار گیرد.

---

[9] General Data Protection Regulation (GDPR)
[10] NIS Directive
[11] NIS2 Directive
[12] ITU-T Y.2060
[13] Security by Design

۵-۵. استانداردهای سازمان استانداردسازی بین‌المللی[14] و کمیسیون بین‌المللی الکتروتکنیک[15]

سازمان استانداردسازی بین‌المللی و کمیسیون بین‌المللی الکتروتکنیک با تدوین استانداردهایی چون استاندارد معماری مرجع اینترنت اشیاء[16] ۲۰۲۴، استاندارد راهنمای امنیت سایبری و حریم خصوصی در اینترنت اشیاء[17] ۲۰۲۲ و همچنین استاندارد مدیریت امنیت اطلاعات[18] ۲۰۱۳، چارچوب‌های جهانی برای امنیت و قابلیت اعتماد سامانه‌های اینترنت اشیاء ایجاد کرده‌اند و راهکارهایی مشخص برای طراحی امن، مدیریت ریسک و حفاظت از داده‌ها ارائه می‌کنند که در بسیاری از کشورها مبنای الزامات قانونی قرار گرفته‌اند. این در حالی است که در ایران استانداردهای ملی مشخص و الزام‌آور درباره طراحی و تولید امن تجهیزات اینترنت اشیاء وجود ندارد و همین امر ارزیابی مسئولیت کیفری یا حتی مدنی سازندگان را با دشواری مواجه می‌سازد.

۵-۶. گزارش‌های سازمان همکاری و توسعه اقتصادی

همچنین سازمان همکاری و توسعه اقتصادی در گزارش خود با عنوان سنجش اینترنت اشیاء[19] ۲۰۲۳، به بررسی ابعاد گسترش، کاربرد و چالش‌های اینترنت اشیاء در کشورهای عضو پرداخته و بر ضرورت تدوین چارچوب‌های منسجم برای سنجش، امنیت و حکمرانی داده‌های مرتبط با این فناوری تأکید نموده است. هرچند این سند ماهیت آماری و تحلیلی دارد، اما نتایج آن واجد اهمیت ویژه‌ای برای سیاست‌گذاری جنایی پیشگیرانه است. در این گزارش، از جمله مهم‌ترین چالش‌های شناسایی‌شده، نگرانی نسبت به امنیت سایبری، حفاظت از داده‌ها و نقض حریم خصوصی عنوان شده است که می‌تواند زمینه‌ساز بروز جرایم نوپدید در بستر اینترنت اشیاء گردد. بر همین اساس، سازمان همکاری و توسعه اقتصادی کشورها را به اتخاذ تدابیری از قبیل استانداردسازی الزامات امنیتی برای تولیدکنندگان و ارائه‌دهندگان خدمات، شفافیت در فرایند جمع‌آوری و پردازش داده‌ها، ارتقای سواد دیجیتال کاربران، تقویت نظام‌های پایش و ارزیابی مستمر ریسک‌ها و نیز توسعه همکاری‌های بین‌المللی در زمینه تبادل داده و تجارب امنیتی توصیه می‌کند.

این گزارش با رویکردی فناورانه نشان می‌دهد که پیشگیری از تهدیدات و سوءاستفاده‌های ناشی از اینترنت اشیاء، نیازمند ترکیبی از تدابیر فنی، مدیریتی و آموزشی در کنار چارچوب‌های نظارتی و حمایتی است. از این منظر، این گزارش را می‌توان مبنایی برای طراحی سیاست جنایی پیشگیرانه مبتنی بر داده و ریسک‌مدار دانست که هدف آن کاهش آسیب‌پذیری‌های امنیتی و جلوگیری از شکل‌گیری جرایم مرتبط با اینترنت اشیاء در سطح ملی و بین‌المللی است.

مقایسه اسناد بین‌المللی با وضعیت حقوقی ایران نشان می‌دهد که سیاست جنایی تقنینی ایران در سه حوزه اصلی با خلأهای جدی روبه‌رو است. نخست، در حوزه الزامات امنیتی و استانداردهای فنی، ایران فاقد نظام جامع و اجباری مبتنی بر امنیت در طراحی، مدیریت آسیب‌پذیری‌ها و گزارش رخدادهای امنیتی است؛ در حالی که اسناد بین‌المللی بر نقش بنیادین این موارد تأکید دارند. دوم، در حوزه مسئولیت حقوقی و کیفری، الگوی ایران همچنان بر رفتار انسانی تمرکز دارد و برای مدیریت خطرات ناشی از عملکرد خودکار سیستم‌های اینترنت اشیاء چارچوب روشن و مبتنی بر ریسک ارائه نکرده است؛ در مقابل، اتحادیه اروپا مسئولیت

[14] International Organization for Standardization (ISO)
[15] International Electrotechnical Commission (IEC)
[16] ISO/IEC 30141:2024
[17] ISO/IEC 27400:2022
[18] ISO/IEC 27001:2013
[19] Measuring the Internet of Things 2023

تولیدکنندگان و توسعه‌دهندگان را به‌صورت شفاف و قابل اجرا تعریف کرده است. سوم، در حوزه همکاری فرامرزی و حکمرانی دیجیتال، ایران هنوز از سازوکارهای بین‌المللی مؤثر مانند کنوانسیون بوداپست بهره‌مند نشده و این موضوع ظرفیت کشور برای مقابله با جرایم فراملی مرتبط با اینترنت اشیاء را محدود کرده است. بنابراین، استفاده از این اسناد می‌تواند مبنایی مستحکم برای بازنگری و تقویت سیاست جنایی تقنینی ایران باشد. به‌ویژه ایجاد نظام استانداردسازی اجباری، طراحی چارچوب مسئولیت مبتنی بر ریسک، توسعه سازوکارهای گزارش‌دهی امنیتی، و همسویی با اسناد و سازوکارهای بین‌المللی می‌تواند در ارتقای ظرفیت کشور برای مواجهه با جرایم نوپدید اینترنت اشیاء نقش تعیین‌کننده داشته باشد.

نتیجه‌گیری

تحولات بنیادین ناشی از گسترش اینترنت اشیاء، ضمن ایجاد فرصت‌های گسترده برای توسعه اقتصادی، ارتقای کیفیت خدمات و بهبود حکمرانی هوشمند، زمینه بروز طیف متنوعی از جرایم نوپدید را نیز فراهم ساخته است؛ جرایمی که ماهیت آن‌ها با جرایم سایبری سنتی متفاوت بوده و در بسیاری موارد، تصمیم‌گیری یا عملکرد خودکار سامانه‌های هوشمند نقش اصلی را در تحقق رفتار زیان‌بار بر عهده دارد. تحلیل انجام‌شده در این مقاله نشان داد که سیاست جنایی تقنینی ایران، علی‌رغم برخورداری از برخی ظرفیت‌ها در قوانین موجود و اسناد ملی، همچنان فاقد انسجام، جامعیت و کارآمدی لازم برای مواجهه مؤثر با جرایم مرتبط با اینترنت اشیاء است. مطالعه قوانین نشان می‌دهد که مقرراتی مانند قانون جرایم رایانه‌ای، قانون مجازات اسلامی، قانون تجارت الکترونیکی و قانون حمایت از حقوق مصرف‌کنندگان، عمدتاً بر رفتار انسانی مبتنی‌اند و جرایم ناشی از خطای نرم‌افزاری، نقص فنی یا تصمیم‌گیری خودکار سامانه‌ها در این نظام تقنینی فاقد جایگاه مشخص هستند. نبود جرم‌انگاری اختصاصی، عدم تعریف فاعل در جرایم خودکار، دشواری انتساب سوءنیت و فقدان نظام مشخص برای تعیین مسئولیت کیفری تولیدکنندگان، برنامه‌نویسان، عرضه‌کنندگان و کاربران، مهم‌ترین خلأهایی هستند که مواجهه سنتی حقوق کیفری با این جرایم را ناکارآمد می‌سازند. اسناد ملی همچون مصوبه الزامات اینترنت اشیاء و دستورالعمل خودروهای متصل گرچه در حوزه‌های امنیتی، فنی و مدیریتی دارای نقش پیشگیرانه‌اند، اما فاقد ضمانت اجرای کیفری، سازوکارهای تعیین مسئولیت و چارچوب واکنش قضایی هستند. این اسناد بیشتر در زمره سیاست‌های پیشگیرانه غیرکیفری قرار می‌گیرند و نمی‌توانند جای خالی یک سیاست تقنینی منسجم را پر کنند. از سوی دیگر، بررسی اسناد و استانداردهای بین‌المللی نشان می‌دهد که رویکرد جهانی بر طراحی امن، مسئولیت‌پذیری تولیدکننده، حفاظت سخت‌گیرانه از داده‌ها و تاب‌آوری امنیتی در چرخه عمر محصول استوار است؛ در حالی که نظام حقوقی ایران همچنان رویکرد رفتارمحور و سنتی خود را حفظ کرده و به مقررات ویژه برای مواجهه با فناوری‌های خودکار و تصمیم‌گیر وابسته نیست. این مقایسه آشکار می‌سازد که سیاست جنایی ایران در برابر جرایم اینترنت اشیاء بیش از پیش نیازمند بازنگری بنیادین و همسویی با استانداردهای جهانی است، به‌ویژه در حوزه‌هایی که جان و مال شهروندان، امنیت عمومی و اعتماد به فناوری‌های نوین را تحت تأثیر مستقیم قرار می‌دهد. بنابراین، تداوم وضعیت موجود می‌تواند موجب افزایش آسیب‌پذیری نظام حقوقی، گسترش ناامنی دیجیتال، دشواری در انتساب مسئولیت، و سردرگمی مراجع رسیدگی شود. برای رفع این چالش‌ها ضرورت دارد سیاست جنایی تقنینی ایران با توجه به ماهیت فناورانه و ریسک‌محور این پدیده‌ها، از تکیه بر قواعد سنتی فاصله گرفته و چارچوبی جامع، آینده‌نگر و مبتنی بر نظام مسئولیت مشخص و استانداردهای امنیتی نوین طراحی کند.

پیشنهادات:

- تدوین قانون جامع اینترنت اشیاء

با توجه به گسترش روزافزون کاربرد اینترنت اشیاء و ظهور مخاطرات و جرایم نوپدید در این حوزه، سیاست جنایی تقنینی ایران ناگزیر است از چارچوب‌های سنتی فاصله گرفته و رویکردی آینده‌نگر، ریسک‌محور و سازگار با استانداردهای جهانی اتخاذ کند. نخستین گام در این مسیر، تدوین قانونی است که بتواند تعریف دقیق مفاهیم، تعیین قلمرو مسئولیت کیفری سازندگان، برنامه‌نویسان، عرضه‌کنندگان و کاربران، تبیین انواع جرایم اختصاصی این حوزه و طبقه‌بندی آن‌ها، سازوکارهای جمع‌آوری و حفاظت از داده‌ها و چارچوب‌های ویژه برای ادله دیجیتال را دربرگیرد. چنین قانونی باید ضمن توجه به ماهیت چندلایه و پیچیده این فناوری، میان نقش تولیدکننده، ارائه‌دهنده خدمات، کاربر نهایی و نهادهای نظارتی تفکیک روشنی ایجاد کرده و مسئولیت کیفری ناشی از نقص‌های طراحی، ضعف امنیتی یا عرضه محصولات ناایمن را روشن و قابل اجرا سازد.

- طراحی الگوی مسئولیت مبتنی بر ریسک برای دستگاه‌های خودکار

بر اساس این الگو، مسئولیت صرفاً بر رفتار انسانی مبتنی نیست، بلکه نقش سازنده، طراح، اپراتور و سایر بازیگران بر اساس میزان کنترل فنی و امکان پیش‌بینی‌پذیریِ خطرات تعیین می‌شود. در واقع ایران بایستی مسئولیت سازنده را در نقص‌های طراحی و امنیتی تصریح کند، مسئولیت کاربر را تنها در صورت تقصیر واقعی بپذیرد و زمینه رجوع بین بازیگران مختلف را مشخص سازد. به عبارت دیگر سیاست جنایی ایران بایستی به سمت پذیرش مسئولیت مبتنی بر ریسک حرکت کند؛ رویکردی که بر اساس آن، تولیدکنندگان و عرضه‌کنندگان تجهیزات هوشمند ملزم می‌شوند از مرحله طراحی تا پایان چرخه عمر محصول، اصول امنیتی لازم را رعایت کرده و در برابر آسیب‌پذیری‌های ناشی از قصور فنی پاسخ‌گو باشند. این تحول تقنینی باید با جرم‌انگاری رفتارهای پرخطر و تهدیدکننده در حوزه اینترنت اشیاء همراه شود، از جمله تولید یا عرضه تجهیزات فاقد استانداردهای امنیتی، عدم ارائه به‌روزرسانی‌های حیاتی، جمع‌آوری یا افشای غیرقانونی داده‌های تولیدشده توسط دستگاه‌های متصل و نقض الزامات امنیتی در بخش‌هایی که جان، مال یا حریم خصوصی شهروندان را در معرض خطر قرار می‌دهد. در این چارچوب مسئولیت کیفری باید برای مواردی پیش‌بینی شود که نقض آشکار الزامات ایمنی یا تقصیر فاحش موجب بروز تهدیدات جدی شده باشد.

- تصویب قانون جامع حمایت از داده‌های شخصی

در کنار این اقدامات، تصویب قانون جامع حمایت از داده‌های شخصی ضرورتی اجتناب‌ناپذیر است. داده‌هایی که از طریق اینترنت اشیاء تولید و پردازش می‌شوند از حساسیت ویژه‌ای برخوردارند و فقدان قانون جامع موجب شده بخش مهمی از حریم خصوصی کاربران در معرض آسیب و سوءاستفاده قرار گیرد. چنین قانونی باید اصول امنیت در پردازش داده، شفافیت، محدودیت هدف، رضایت آگاهانه، نگهداری امن اطلاعات و مسئولیت‌پذیری پردازش‌گران را به‌صورت الزام‌آور و همراه با ضمانت اجراهای کیفری و اداری پیش‌بینی کند.

- الزام تولیدکنندگان به رعایت استانداردهای امنیتی بین‌المللی

لازم است استانداردهای امنیتی بین‌المللی، به‌ویژه استانداردهای سازمان استانداردسازی بین‌المللی و کمیسیون بین‌المللی الکتروتکنیک و توصیه‌نامه‌های اتحادیه بین المللی مخابرات، در سطح ملی به استانداردهای اجباری تبدیل شده و نظام «ارزیابی و تأیید امنیت محصول» برای دستگاه‌های متصل ایجاد شود. این اقدام زمینه نظارت پیشینی بر امنیت محصولات و امکان انتساب مسئولیت کیفری را فراهم می‌آورد.

- ایجاد سازوکار ملی گزارش‌دهی حوادث و جرایم اینترنت اشیاء

ایجاد یک سازوکار ملی برای گزارش‌دهی حوادث امنیتی مرتبط با اینترنت اشیاء ضروری است؛ سازوکاری مشابه مدل‌های پیشرفته نظیر دستورالعمل امنیت شبکه و اطلاعات اتحادیه اروپا[20] که وظیفه جمع‌آوری، تحلیل، هشداردهی و هماهنگی واکنش به رخدادهای امنیتی را بر عهده دارد. درواقع بایستی با الهام از این استانداردهای NIS2، سازوکار گزارش‌دهی اجباری رخدادها و ظرفیت فورنزیک تخصصی ایجاد شود تا امکان واکنش سریع، مدیریت بحران و جمع‌آوری ادله دیجیتال فراهم گردد.

- تقویت همکاری‌های فرامرزی

ارتقای همکاری‌های فرامرزی و الحاق به اسناد بین‌المللی مرتبط با جرایم سایبری و ادله دیجیتال، به‌ویژه در حوزه‌هایی که ماهیت فراملی دارند، برای کارآمدی سیاست جنایی ایران ضرورت دارد. همچنین آموزش تخصصی قضات، ضابطان، کارشناسان رسمی و نیروهای پلیس در حوزه فناوری‌های هوشمند و ادله دیجیتال مرتبط با دستگاه‌های متصل اینترنت اشیاء، بخشی حیاتی از اجرای صحیح قوانین آینده خواهد بود. در مجموع، تلفیق قانون‌گذاری پیشرفته، استانداردسازی فنی، همکاری بین‌نهادی و حمایت از داده‌ها می‌تواند زمینه شکل‌گیری نظامی کارآمد و روزآمد برای مواجهه با چالش‌های اینترنت اشیاء در حقوق ایران را فراهم آورد.

در نهایت، با توجه به ماهیت فرامرزی فناوری‌های متصل، همگرایی با سازوکارهای بین‌المللی، همکاری قضایی و فنی و انعقاد توافق‌نامه‌های تخصصی برای تبادل ادله دیجیتال، شرط ضروری کارآمدی واکنش ملی در حوزه اینترنت اشیاء است. برآیند این راهکارها نشان می‌دهد که سیاست جنایی تقنینی کارآمد در برابر تهدیدات اینترنت اشیاء تنها زمانی محقق می‌شود که حقوق ایران از رویکرد مبتنی بر رفتار فردی فاصله گرفته و به الگوی جامع، پیشگیرانه، ریسک‌محور و مبتنی بر مسئولیت‌پذیری ساختاری نزدیک شود. چنین الگویی می‌تواند نه‌تنها خلأهای موجود را برطرف کند، بلکه امنیت دیجیتال، اعتماد عمومی و امکان توسعه پایدار فناوری‌های نوپدید در کشور را نیز تقویت نماید. سیاست جنایی تقنینی ایران برای مواجهه با جرایم اینترنت اشیاء نیازمند تحول ساختاری و رویکرد نوین است؛ تحولاتی که در سه سطح قانون‌گذاری، استانداردسازی و همکاری نهادی تحقق می‌یابد. تنها با چنین رویکردی می‌توان امنیت کاربران، اعتماد عمومی، توسعه فناوری و عدالت کیفری را در عصر اینترنت اشیاء تضمین کرد.

منابع

الف)منابع فارسی

۱. بختیاری، ایرج. (۱۴۰۱). تحلیلی بر کاربرد اینترنت اشیاء در شبکه پدافند هوایی از منظر آسیب‌ها و تهدیدها، فصلنامه علوم و فنون نظامی، ۱۸(۶۱)، ۵۵-۸۲.

https://doi.org/10.22034/qjmst.2022.545564.1639

۲. برزگر، محمدرضا، الهام، غلامحسین. (۱۳۹۹). مسئولیت کیفری کاربر خودروی خودران در قبال صدمات وارده توسط آن، فصلنامه پژوهش حقوق کیفری، ۸(۳۰)، ۲۰۱-۲۲۹.

https://doi.org/10.22054/jclr.2020.39009.1838

۳. پورقهرمانی، بابک، الناز، کتانچی (۱۳۹۸). سیاست‌های نمادین معاهده جرایم سایبری شورای اروپا، فصلنامه مطالعات بین‌المللی، ۱۶(۶۲)، ۳۱-۴۷.

https://doi.org/10.22034/isj.2019.99238

۴. حسین‌زاده، مرضیه، رضایی، علیرضا. (۱۴۰۲). امنیت سایبری در حوزه اینترنت اشیاء، فصلنامه آرمان پردازش، ۴(۱)، ۱-۹.

[20] NIS2 Directive

https://doi.org/10.22034/apj.2023.706757

۵. دیلمی معزی، نوید، اسماعیلی، مهدی، حاجی تبار فیروزجائی، حسن. (۱۴۰۱). ارزیابی سیاست جنایی تقنینی ایران و اتحادیه اروپا در قبال جرایم رایانه‌ای، فصلنامه تحقیقات حقوقی بین‌المللی، ۱۵(۵۶)، ۱۰۵-۱۲۷.

https://doi.org/10.30495/alr.2022.1949604.2258

۶. زیبنده، حسین، عطاردی، محمدرضا. (۱۴۰۱). مطالعه تطبیقی خط‌مشی‌های توسعه اینترنت اشیاء (مقایسه تجارب اتحادیه اروپا، آمریکا و چین). فصلنامه دانش سیاسی، ۱۸(۲)، ۴۵۵-۴۸۴.

https://doi.org/10.30497/pkn.2022.239263.2734

۷. عابدیان، میرحسین، احمدی، منا. (۱۳۹۱). مفهوم حقوق نرم و مزایای آن در نظام حقوق تجارت بین الملل، فصلنامه تحقیقات حقوقی، ۱۵(۶۰)، ۱۱۹-۱۷۱.

https://lawresearchmagazine.sbu.ac.ir/article_56484.html

۸. قناد، فاطمه، شریف، الهام. (۱۴۰۰). مطالعه اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، دوفصلنامه حقوق فناوری‌های نوین، ۲(۴)، ۱-۲۲.

https://doi.org/10.22133/clj.2021.244608.1020

۹. لوسه، سباستین، شولتسه، راینر، اشتاودنمایر، دیرک. (۱۴۰۲). مسئولیت هوش مصنوعی و اینترنت اشیا، ترجمه: فاطمه نجیب‌زاده، تهران: انتشارات جنگل.

۱۰. میرلوحی، سید علی. (۱۴۰۵). چالش اثبات رکن روانی در جرایم ارتکابی توسط هوش مصنوعی و راهکار گذار به مسئولیت مبتنی بر ریسک در فقه و حقوق کیفری، فصلنامه پژوهش‌های حقوق جزا و جرمشناسی، ۱۴(۲۸)، ۱۷۱-۱۹۶.

https://jclc.sdil.ac.ir/article_231652.html

۱۱. وبر، رلف اچ، وبر، رومانا. (۱۳۹۹). چشم انداز حقوقی اینترنت اشیا، ترجمه: فاطمه اقدسی، تهران: انتشارات نوین آیین.

۱۲. هالوی، گابریل. (۱۳۹۸). مسئولیت کیفری ربات‌ها: هوش مصنوعی در قلمرو حقوق کیفری، ترجمه: فرهاد شاهیده و طاهره قوانلو، تهران: انتشارات میزان.

ب) منابع خارجی

1. Ahmed, A. A., Farhan, K., Jabbar, W. A., Al-Othmani, A., & Abdulrahman, A. G. (2024). IoT Forensics: Current Perspectives and Future Directions. Sensors, 24(10), 1-16. https://doi.org/10.3390/s24165210
2. Beck, S. (2016). Intelligent agents and criminal law: Negligence, diffusion of liability and electronic personhood. Robotics and Autonomous Systems, 86, 138–143. https://doi.org/10.1016/j.robot.2016.08.028
3. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). ETS No.185. Strasbourg: Council of Europe.
4. Council of Europe. (2003). Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems. ETS No.189. Strasbourg: Council of Europe.
5. European Parliament & Council of the European Union. (2016). NIS Directive. Official Journal of the European Union, L 194, 1–30.

6. European Parliament & Council of the European Union. (2022). NIS2 Directive. Official Journal of the European Union, L 333, 80–152.
7. European Parliament & Council of the European Union. (2024). Cyber Resilience Act. Official Journal of the European Union, L 2847.
8. European Union Agency for Cybersecurity (ENISA). (2020). Guidelines for Securing the Internet of Things (IoT).
9. European Union. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Brussels: EU.
10. Fabiano, N. (2017). Internet of Things and the legal issues related to the data protection law according to the new European General Data Protection Regulation. Athens Journal of Law, 3(3), 201–214. https://doi.org/10.30958/ajl.3-3-2
11. Gless, S., Silverman, E. & Weigend, T. (2016). If Robots cause harm, who is to blame? Self-driving Cars and Criminal Liability. New Criminal Law Review Journal, 19(3), 412-436. https://doi.org/10.1525/nclr.2016.19.3.412
12. Hashmi, M. A. I., Butt, M. Jawad, M. Sultan, S. (2025). Criminal liability in the age of autonomous systems: Rethinking mens rea and actus reus. The Critical Review of Social Sciences Studies, 3(3), 290-303. https://doi.org/10.59075/szbtkr93
13. International Committee of the Red Cross. (2021). ICRC position on autonomous weapon systems (position paper). Geneva: ICRC.
14. International Organization for Standardization & International Electrotechnical Commission. (2013). ISO/IEC 27001:2013, Information technology, Security techniques, Information security management systems, Requirements. Geneva: ISO/IEC.
15. International Organization for Standardization & International Electrotechnical Commission. (2024). ISO/IEC 30141:2024, Internet of Things (IoT), Reference architecture. Geneva: ISO/IEC.
16. International Organization for Standardization. (2025). ISO 10218-1:2025, Robotics –Safety requirements, Part 1: Industrial robots, Geneva: ISO.
17. International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC). (2022). ISO/IEC 27400:2022, Cybersecurity, IoT security and privacy Guidelines. Geneva: ISO/IEC.
18. International Telecommunication Union (ITU). (2012). Recommendation ITU-T Y.2060: Overview of the Internet of Things. Geneva: ITU.
19. Organization for Economic Co-operation and Development (OECD). (2023). Measuring the Internet of Things. OECD Publishing, Paris.
20. Organization for Economic Co-operation and Development (OECD). (2015). Digital security risk management for economic and social prosperity: OECD Recommendation and Companion Document. Paris: OECD Publishing.