فصلنامه علمی راهبرد سیاسی
انتشارات دانشگاه راهبردی

مدیریت مخاطرات حریم خصوصی و امنیت در اینترنت اشیاء تحت چارچوب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا

سیده مهشید میری بالاجورشری[1]، امیررضا محمودی[2]، بابک پورقهرمانی[3]

دوره ۱۰، شماره ۱، پیاپی ۳۶
بهار ۱۴۰۵

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۴/۱۲/۰۴
تاریخ پذیرش:
۱۴۰۵/۰۳/۱۷
صص: ۲۴۳-۲۱۷

شاپا چاپی: ۴۵۶۵-۲۵۸۸
الکترونیکی: ۰۳۸۱-۲۷۱۷

چکیده

گسترش شتابان فناوری اینترنت اشیاء به‌عنوان یکی از مهم‌ترین جلوه‌های تحول دیجیتال، موجب افزایش بی‌سابقه جمع‌آوری، پردازش و تبادل داده‌های شخصی در مقیاسی گسترده شده است. ویژگی‌هایی نظیر اتصال دائمی اشیاء، پردازش خودکار و تحلیل کلان‌داده چالش‌های بنیادینی را در حوزه حریم خصوصی پدید آورده است. هدف اصلی این پژوهش، تبیین مخاطرات حریم خصوصی در بستر اینترنت اشیاء و ارزیابی نحوه مدیریت این مخاطرات در چارچوب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا است. نوع تحقیق در این پژوهش نظری می‌باشد که با رویکردی توصیفی-تحلیلی و با بهره‌گیری از منابع کتابخانه‌ای به بررسی چالش‌هایی چون ردیابی مکانی، قابلیت انتساب و شناسایی مجدد داده‌ها و نقض امنیت اطلاعات در اینترنت اشیاء پرداخته است. یافته‌های تحقیق نشان می‌دهد که ماهیت داده‌محور اینترنت اشیاء، بدون ادغام الزامات حمایتی در مرحله طراحی، می‌تواند به نقض گسترده حقوق بنیادین اشخاص منجر شود. در مقابل، چارچوب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا با نهادینه‌سازی اصولی چون شفافیت، پاسخگویی، حداقل‌گرایی در جمع‌آوری داده و حفاظت از داده از طریق طراحی و به‌صورت پیش‌فرض، رویکردی پیشگیرانه و ساختاری برای مدیریت مخاطرات ارائه می‌دهد. برقراری توازن میان نوآوری فناورانه و صیانت از حقوق بنیادین اشخاص، تنها در پرتو رویکردی پیش‌دستانه و حقوق‌محور در حکمرانی داده‌ها امکان‌پذیر خواهد بود.

کلیدواژه‌ها: اینترنت اشیاء، حریم خصوصی، حمایت از داده‌های شخصی، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، حریم خصوصی در طراحی.

۱. گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران.
۲. گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران. (نویسنده مسئول) dr.mahmoudi@iau.ac.ir
۳. گروه حقوق کیفری و جرمشناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران.

مقدمه

تحولات شتابان فناوری اطلاعات و ارتباطات در دهه‌های اخیر، ساختارهای سنتی تعاملات انسانی، اقتصادی و حقوقی را به‌طور بنیادین دگرگون کرده است. در این میان، اینترنت اشیاء[1] به‌عنوان یکی از مهم‌ترین جلوه‌های تحول دیجیتال، نقش تعیین‌کننده‌ای در شکل‌گیری جامعه داده‌محور ایفا می‌کند. اینترنت اشیاء با اتصال اشیاء فیزیکی به شبکه‌های ارتباطی و امکان جمع‌آوری، پردازش و تبادل خودکار داده‌ها، بستری نوین برای ارائه خدمات هوشمند، مدیریت منابع و بهبود کیفیت زندگی فراهم ساخته است. با این حال، همین ویژگی‌ها موجب شده است که اینترنت اشیاء به یکی از چالش‌برانگیزترین حوزه‌ها از منظر حقوق حریم خصوصی و حمایت از داده‌های شخصی تبدیل شود. تعریف اینترنت اشیاء به دلیل پیچیدگی فنی و تنوع کاربردهای آن، امری چالش‌برانگیز است. به‌طور کلی، اینترنت اشیاء به شبکه‌ای از اشیاء فیزیکی اطلاق می‌شود که از طریق حسگرها، ریزتراشه‌ها و سامانه‌های ارتباطی به یکدیگر متصل شده و قادرند داده‌ها را بدون مداخله مستقیم انسان تولید و منتقل کنند. کاربردهای این فناوری در حوزه‌هایی نظیر سلامت، حمل‌ونقل، انرژی، مدیریت شهری و... مزایای قابل توجهی به همراه داشته است. (ITU-T Y2026: 2012) تجمیع داده‌های تولیدشده توسط اشیاء مختلف و تحلیل آن‌ها در قالب سامانه‌های هوشمند می‌توانند حاوی اطلاعات حساس درباره عادات رفتاری، سبک زندگی، موقعیت مکانی و حتی وضعیت سلامت افراد باشند. چنین قابلیتی، به‌ویژه زمانی که بدون آگاهی یا کنترل مؤثر اشخاص صورت گیرد، امکان نظارت گسترده و مداوم بر زندگی خصوصی افراد را فراهم می‌کند و حق بر حریم خصوصی را به‌طور جدی در معرض تهدید قرار می‌دهد. از این منظر، اینترنت اشیاء نه‌تنها یک پدیده فناورانه، بلکه موضوعی بنیادین در تقاطع فناوری و حقوق محسوب می‌شود. از این‌رو، گسترش اینترنت اشیاء مسائل حقوقی متعددی را در حوزه حریم خصوصی و حمایت از داده‌های شخصی مطرح کرده است. پردازش داده‌ها در اینترنت اشیاء غالباً به‌صورت خودکار، گسترده و غیرشفاف انجام می‌شود و کاربران در بسیاری از موارد، آگاهی و کنترل مؤثری بر نحوه جمع‌آوری، تحلیل و اشتراک‌گذاری داده‌های خود ندارند. پدیده‌هایی نظیر شناسایی مستقیم و غیرمستقیم داده‌های شخصی، مکان‌یابی مداوم و تجمیع داده‌ها، امکان نظارت فراگیر بر زندگی خصوصی اشخاص را فراهم می‌سازد و مرز میان استفاده

[1] Internet of Things (IoT)

مشروع از داده‌ها و نقض حریم خصوصی را به‌شدت تضعیف می‌کند. این وضعیت، نه‌تنها حقوق بنیادین اشخاص را در معرض تهدید قرار می‌دهد، بلکه اعتماد عمومی به فناوری‌های نوین را نیز با چالش مواجه می‌سازد. افزون بر این، ساختار چندلایه و پیچیده زنجیره بازیگران در اینترنت اشیاء، از جمله تولیدکنندگان سخت‌افزار، توسعه‌دهندگان نرم‌افزار، ارائه‌دهندگان خدمات ابری و تحلیل‌گران داده، تعیین مسئولیت حقوقی در صورت نقض داده‌ها را با دشواری‌های مضاعف مواجه ساخته است. اتحادیه اروپا با تصویب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا[1] گامی مهم در جهت نهادینه‌سازی یک چارچوب جامع و یکپارچه برای حمایت از داده‌های شخصی برداشته است. این مقرره با رویکردی فراملی و مبتنی بر اصولی همچون شفافیت، پاسخگویی، حداقل‌گرایی در جمع‌آوری داده، مشروعیت پردازش، ارزیابی اثرات حفاظت از داده و رویکرد حفاظت از داده از طریق طراحی و به‌صورت پیش‌فرض، تلاش کرده است پاسخ‌هایی ساختاری و پیشگیرانه به مخاطرات عصر داده ارائه دهد. با توجه به ماهیت داده‌محور اینترنت اشیاء، این چارچوب حقوقی می‌تواند معیاری مهم برای ارزیابی مشروعیت و کفایت سازوکارهای حمایتی در این حوزه تلقی شود.

با وجود پژوهش‌های پراکنده درباره حریم خصوصی در فناوری‌های نوین یا تحلیل کلی مقررات عمومی حفاظت از داده‌ها، بررسی منسجم و متمرکز میان ویژگی‌های خاص اینترنت اشیاء با الزامات و سازوکارهای پیش‌بینی‌شده در این مقرره، همچنان نیازمند تحلیل عمیق حقوقی است. خلأ اصلی در ادبیات موجود، فقدان واکاوی نظام‌مند چالش‌های خاص اینترنت اشیاء، از جمله ردیابی مکانی، انتساب داده‌ها، نقض امنیت و پیچیدگی تعیین نقش کنترل‌کننده و پردازشگر، در پرتو اصول و نهادهای حقوقی مقرر در مقررات عمومی حفاظت از داده‌های اتحادیه اروپا است. بر این اساس، هدف اصلی این پژوهش، تبیین چالش‌های بنیادین حریم خصوصی در بستر اینترنت اشیاء و ارزیابی نحوه مدیریت و تنظیم این چالش‌ها در چارچوب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا می‌باشد. پرسش محوری مقاله آن است که چارچوب حقوقی مقررات عمومی حفاظت از داده‌های اتحادیه اروپا چگونه و تا چه میزان قادر است مخاطرات خاص اینترنت اشیاء را پوشش داده و حمایت مؤثری از حریم خصوصی اشخاص فراهم آورد؟ در پاسخ به این پرسش، فرضیه پژوهش بر این مبنا استوار است که هرچند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا با اتخاذ رویکردی پیشگیرانه و ساختاری،

[1] General Data Protection Regulation (GDPR)

ابزارهای مناسبی برای مدیریت ریسک‌های اینترنت اشیاء فراهم کرده است، تحقق عملی حمایت مؤثر از حریم خصوصی در این حوزه، مستلزم ادغام واقعی الزامات حقوقی در معماری فنی سامانه‌ها، شناسایی دقیق نقش بازیگران و تقویت سازوکارهای پاسخگویی می‌باشد.

در این پژوهش ابتدا کاربست‌های نوین اینترنت اشیاء و پیامدهای فناورانه و حقوقی آن مورد بررسی قرار گرفته و سپس چالش‌های بنیادین حریم خصوصی در بستر اینترنت اشیاء مطالعه می‌شود و پس از آن مسئولیت ناشی از نقض امنیت داده‌ها در اینترنت اشیاء در اتحادیه اروپا مورد تحلیل قرار گرفته و در نهایت مدیریت مخاطرات حریم خصوصی و امنیت در اینترنت اشیاء تحت چارچوب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا بررسی می‌شود.

۱. کاربست‌های نوین اینترنت اشیاء و چالش‌های آن

اکوسیستم اینترنت اشیاء به‌عنوان یکی از جلوه‌های بارز تحول دیجیتال، بستر مناسبی برای توسعه گسترده کاربردهای فناورانه در حوزه‌های مختلف اقتصادی، اجتماعی و خدمات عمومی فراهم کرده است. اتصال اشیاء فیزیکی به شبکه‌های ارتباطی و امکان تبادل داده به‌صورت خودکار، موجب شکل‌گیری نسلی جدید از سامانه‌ها شده است که از آن‌ها با عنوان سامانه‌های هوشمند یاد می‌شود. در سال‌های اخیر، مفاهیمی نظیر شهر هوشمند، شبکه هوشمند انرژی، خودروی هوشمند و خانه هوشمند به‌عنوان مهم‌ترین مصادیق کاربردی اینترنت اشیاء مطرح شده‌اند و نقش فزاینده‌ای در مدیریت منابع، بهبود کیفیت زندگی و افزایش بهره‌وری ایفا می‌کنند. در این سامانه‌ها، اشیاء مجهز به حسگرها، تراشه‌ها و نرم‌افزارهای پردازش داده، قادرند اطلاعات محیطی، رفتاری یا عملکردی را جمع‌آوری کرده و از طریق زیرساخت‌های ارتباطی به سایر اشیاء، سامانه‌های مرکزی یا کاربران نهایی منتقل کنند. ویژگی اصلی این فناوری، تعامل خودکار میان اشیاء بدون مداخله مستقیم انسان و پردازش داده‌ها در زمان واقعی است؛ امری که موجب افزایش سرعت تصمیم‌گیری و کاهش هزینه‌های عملیاتی می‌شود. با این حال، همین ویژگی، پیامدهای حقوقی و امنیتی قابل توجهی نیز به همراه دارد که نمی‌توان از آن‌ها غفلت کرد. (Babalola, 2021: 311-313)

در حوزه خانه‌های هوشمند، که یکی از رایج‌ترین و ملموس‌ترین کاربردهای اینترنت اشیاء به شمار می‌رود، مجموعه‌ای از تجهیزات و وسایل خانگی نظیر سیستم‌های روشنایی، گرمایش و سرمایش،

یخچال‌ها، دوربین‌های امنیتی و دستیارهای صوتی به یکدیگر و به شبکه اینترنت متصل می‌شوند. این تجهیزات با استفاده از داده‌های دریافتی از حسگرها، قادرند به‌صورت خودکار عملکرد خود را تنظیم کرده و اطلاعات مربوط به وضعیت مصرف انرژی، زمان استفاده یا حتی الگوهای رفتاری ساکنان را ثبت و ارسال کنند. در حوزه شبکه‌های هوشمند انرژی نیز، کنتورهای هوشمند نقش کلیدی ایفا می‌کنند. این ابزارها اطلاعات دقیقی درباره میزان و الگوی مصرف انرژی خانوارها را به‌صورت مستمر به سامانه‌های مرکزی ارائه‌دهندگان خدمات منتقل می‌کنند. این داده‌ها می‌توانند برای بهینه‌سازی توزیع انرژی، کاهش تلفات و تنظیم تعرفه‌ها مورد استفاده قرار گیرند و از این حیث، مزایای قابل توجهی برای شرکت‌های خدمات‌رسان و مصرف‌کنندگان به همراه دارند. با این حال، داده‌های مصرف انرژی به‌طور غیرمستقیم می‌توانند بازتاب‌دهنده الگوهای زندگی، ساعات حضور یا عدم حضور افراد در منزل و حتی برخی ویژگی‌های رفتاری آنان باشند که این امر، اهمیت حمایت حقوقی از این داده‌ها را دوچندان می‌سازد. از منظر فنی، توسعه کاربردهای اینترنت اشیاء مستلزم طراحی و پیاده‌سازی سازوکارهای امنیتی پیشرفته به‌منظور جلوگیری از دستکاری، نفوذ یا دسترسی غیرمجاز به داده‌ها است. با پیچیده‌تر شدن سامانه‌ها و افزایش تعداد اشیاء متصل، سطح حملات سایبری نیز گسترش یافته و اینترنت اشیاء به یکی از اهداف جذاب برای مهاجمان تبدیل شده است. آسیب‌پذیری‌های نرم‌افزاری، ضعف در رمزنگاری ارتباطات یا فقدان به‌روزرسانی‌های امنیتی می‌تواند منجر به رهگیری داده‌ها یا کنترل غیرمجاز تجهیزات شود. (معینی‌فر، وحیدزاده، ۱٤۰۱: ٦۹-۷۰)

گزارش‌های متعددی از رهگیری ارتباطات تجهیزات هوشمند، از جمله یخچال‌ها یا سیستم‌های خانگی، منتشر شده است که نشان می‌دهد از طریق تحلیل میزان تبادل داده، می‌توان به اطلاعاتی درباره حضور یا عدم حضور ساکنان در منزل، الگوی مصرف یا حتی وضعیت سلامت آنان دست یافت. افشای چنین اطلاعاتی نه‌تنها می‌تواند نقض آشکار حریم خصوصی افراد محسوب شود، بلکه می‌تواند زمینه‌ساز ارتکاب جرایم مختلفی نظیر سرقت، سوءاستفاده از داده‌های سلامت یا نظارت غیرقانونی بر اشخاص باشد. در نتیجه، توسعه کاربردهای اینترنت اشیاء صرفاً یک مسئله فنی یا اقتصادی نیست، بلکه پدیده‌ای چندبعدی است که مستلزم توجه هم‌زمان به ابعاد حقوقی، امنیتی و اخلاقی است. عدم پیش‌بینی الزامات حقوقی در مرحله طراحی و بهره‌برداری از این سامانه‌ها می‌تواند پیامدهای جدی برای حقوق بنیادین اشخاص، به‌ویژه حق بر حریم خصوصی و حمایت از داده‌های

شخصی، به همراه داشته باشد. از این‌رو، رویکردی جامع و پیشگیرانه در توسعه و تنظیم کاربردهای اینترنت اشیاء ضروری است تا ضمن بهره‌مندی از مزایای فناورانه آن، از بروز مخاطرات حقوقی و اجتماعی جلوگیری شود. (ساکت، ۱۳۹۸: ۲۹)

با وجود ظرفیت‌ها و مزایای گسترده اینترنت اشیاء در بهبود کارایی سامانه‌ها و ارتقای کیفیت زندگی، این فناوری نوظهور به دلیل ماهیت فنی و شیوه‌های پردازش داده‌های آن، با مخاطرات جدی در حوزه حریم خصوصی و امنیت اطلاعات مواجه است. اینترنت اشیاء مبتنی بر جمع‌آوری، پردازش و تبادل مستمر داده‌ها در مقیاسی وسیع است؛ داده‌هایی که در بسیاری از موارد، به‌طور مستقیم یا غیرمستقیم به اشخاص حقیقی قابل انتساب بوده و در نتیجه، مشمول قواعد و اصول حقوقی مربوط به حمایت از داده‌های شخصی می‌شوند. گستردگی دامنه داده‌های گردآوری‌شده، عدم شفافیت در نحوه پردازش آن‌ها و پیچیدگی زنجیره بازیگران دخیل در اکوسیستم اینترنت اشیاء، زمینه‌ساز بروز چالش‌های اساسی برای تضمین حریم خصوصی افراد است. (Pettorru, et al. 2024: 16-17) در ادامه به برخی از چالش‌های حریم خصوصی در بستر اینترنت پرداخته می‌شود.

۱-۱. چالش‌های حقوقی ناشی از ردیابی مکانی در اینترنت اشیاء

یکی از مهم‌ترین و در عین حال حساس‌ترین مخاطرات حریم خصوصی در بستر اینترنت اشیاء، ردیابی مکانی می‌باشد؛ چراکه داده‌های مکانی به‌طور مستقیم با آزادی‌های فردی، حریم خصوصی و امنیت اشخاص در ارتباط است. در اکوسیستم اینترنت اشیاء، تعیین موقعیت مکانی افراد نه‌تنها از طریق سامانه‌های سنتی مکان‌یابی، بلکه از طریق طیف گسترده‌ای از ابزارها و تجهیزات متصل به اینترنت امکان‌پذیر شده است. گوشی‌های هوشمند، ساعت‌ها و دست‌بندهای هوشمند، وسایل نقلیه متصل، تجهیزات خانگی و حتی زیرساخت‌های شهری، به‌طور مستمر داده‌هایی را تولید می‌کنند که قابلیت تحلیل مکانی و زمانی دارند و در مجموع، تصویری دقیق از تحرکات و الگوهای رفتاری افراد ارائه می‌دهند. گسترش استفاده از گوشی‌های هوشمند نقش تعیین‌کننده‌ای در تشدید پدیده ردیابی مکانی داشته است. این دستگاه‌ها، به‌عنوان یکی از اجزای اصلی اینترنت اشیاء، به حسگرهای متعددی نظیر جی پی اس[1] وای‌فای، بلوتوث و شتاب‌سنج مجهز هستند که امکان تعیین موقعیت مکانی با دقت بالا را فراهم می‌سازند. در صورتی که کاربر خدمات مکان‌یابی را غیرفعال نکرده باشد یا از پیامدهای فعال

[1] Global Positioning System (GPS)

بودن این خدمات آگاهی کافی نداشته باشد، داده‌های دقیق مکانی وی به‌صورت مستمر ثبت و منتقل می‌شود. چنین وضعیتی، به‌ویژه زمانی که بدون رضایت آگاهانه و کنترل مؤثر شخص صورت گیرد، مصداق بارز نقض حریم خصوصی تلقی می‌شود. (Oktay, et al. 2024: 9)

اهمیت داده‌های مکانی از آن جهت است که این داده‌ها، برخلاف بسیاری از انواع داده‌های شخصی، به‌تنهایی نیز می‌توانند اطلاعات حساسی درباره زندگی افراد آشکار سازند. الگوهای رفت‌وآمد روزانه، مکان‌های سکونت، محل کار، مراکز درمانی، اماکن مذهبی یا سیاسی و حتی روابط اجتماعی افراد، همگی از طریق تحلیل داده‌های مکانی قابل شناسایی هستند. بدین ترتیب، داده‌های مکانی علاوه بر موقعیت مکانی شخص، تصویری جامع از سبک زندگی، باورها و ترجیحات وی ترسیم می‌کنند. از منظر حقوقی، چنین داده‌هایی در زمره حساس‌ترین داده‌های شخصی قرار می‌گیرند و مستلزم بالاترین سطح حمایت قانونی هستند. در اکوسیستم اینترنت اشیاء، داده‌های مکانی به‌طور مستمر و در مقیاسی گسترده تولید می‌شوند و این داده‌ها اغلب با سایر داده‌های رفتاری یا فنی ترکیب می‌گردند. گوشی‌های هوشمند و سایر دستگاه‌های متحرک، هر روزه حجم عظیمی از داده‌های مکانی را تولید می‌کنند که می‌تواند به‌راحتی مورد پردازش، ذخیره‌سازی و تحلیل قرار گیرد. در صورت فقدان چارچوب‌های حقوقی شفاف و تدابیر امنیتی مناسب، این داده‌ها ممکن است به‌صورت غیرقانونی مورد استفاده قرار گیرند یا به دست اشخاص ثالثی بیفتند که اهدافی خارج از اراده و منافع کاربران را دنبال می‌کنند. از منظر حقوقی، چالش اصلی مکان‌یابی در اینترنت اشیاء به مسئله رضایت آگاهانه و کنترل مؤثر کاربر بر داده‌های مکانی بازمی‌گردد. بسیاری از کاربران از دامنه واقعی پردازش داده‌های مکانی خود، اشخاصی که به این داده‌ها دسترسی دارند و اهدافی که برای آن‌ها مورد استفاده قرار می‌گیرد، آگاهی کافی ندارند. حتی در مواردی که رضایت اولیه اخذ می‌شود، این رضایت غالباً کلی، مبهم و غیرقابل تفکیک است و امکان انتخاب آگاهانه و محدودسازی پردازش داده‌ها را برای کاربر فراهم نمی‌سازد. در نتیجه، اصل خودمختاری اطلاعاتی افراد که یکی از مبانی حقوق حریم خصوصی محسوب می‌شود، تضعیف می‌گردد. (Pettorru, et al. 2024: 16-17)

علاوه بر این، مکان‌یابی مداوم می‌تواند زمینه‌ساز نظارت فراگیر و کنترل غیرموجه بر اشخاص شود. تحلیل داده‌های مکانی در کنار سایر داده‌های تولیدشده توسط اشیاء متصل، امکان پایش دائمی رفتار افراد را فراهم می‌کند و مرز میان نظارت مشروع و نقض آزادی‌های فردی را به‌شدت مخدوش می‌سازد.

چنین وضعیتی، به‌ویژه در فضاهای شهری هوشمند که زیرساخت‌های مکان‌یابی در مقیاسی وسیع به‌کار گرفته می‌شوند، می‌تواند پیامدهای اجتماعی و حقوقی قابل توجهی به همراه داشته باشد. از حیث امنیتی نیز، افشای داده‌های مکانی می‌تواند تهدیدی جدی برای امنیت شخصی افراد ایجاد کند. دسترسی غیرمجاز به اطلاعات مکانی ممکن است زمینه‌ساز ارتکاب جرایمی نظیر تعقیب، سرقت، خشونت یا سایر اشکال سوءاستفاده شود. در چنین مواردی، مسئولیت حقوقی پردازش‌کنندگان داده و ارائه‌دهندگان خدمات اینترنت اشیاء مطرح می‌شود و ضرورت پیش‌بینی تدابیر پیشگیرانه و حمایتی بیش از پیش آشکار می‌گردد. (Wazirali, 2022: 772)

در مجموع، مکان‌یابی در بستر اینترنت اشیاء یکی از بارزترین مصادیق تعارض میان نوآوری فناورانه و حقوق بنیادین اشخاص است. بهره‌برداری از قابلیت‌های مکان‌یابی، بدون توجه به اصول حمایت از داده‌ها، شفافیت، حداقل‌سازی پردازش و تضمین حقوق کاربران، می‌تواند به نقض گسترده حریم خصوصی و تضعیف اعتماد عمومی نسبت به فناوری‌های نوین منجر شود. از این رو، تنظیم حقوقی مکان‌یابی در اینترنت اشیاء باید به‌عنوان یکی از اولویت‌های اساسی حقوق حریم خصوصی در عصر دیجیتال مورد توجه قرار گیرد.

۱-۲. چالش‌های انتساب داده‌ها در سامانه‌های اینترنت اشیاء

یکی از مهم‌ترین مخاطرات حریم خصوصی در اینترنت اشیاء، شناسایی اطلاعات شخصی و انتساب داده‌ها به اشخاص حقیقی است. انتقال و پردازش داده‌های شخصی زمانی محقق می‌شود که یک شیء فیزیکی یا دیجیتال به یک فرد معین مرتبط گردد؛ ارتباطی که می‌تواند به‌صورت مستقیم یا غیرمستقیم شکل گیرد. در بسیاری از کاربردهای اینترنت اشیاء، این ارتباط به‌گونه‌ای طراحی شده است که حتی بدون آگاهی یا کنترل مؤثر کاربر، امکان شناسایی شخص فراهم شود. در ارتباط مستقیم، شخص حقیقی به‌طور آگاهانه با شیء یا سامانه مرتبط می‌شود و معمولاً رضایت خود را برای پردازش داده‌های شخصی اعلام می‌کند. این وضعیت در مواردی مانند استفاده از دستگاه‌های پوشیدنی سلامت، دستیارهای صوتی یا سامانه‌های هوشمند خانگی که مستلزم ثبت‌نام کاربر و ارائه اطلاعات هویتی است، مشاهده می‌شود. با این حال، حتی در چنین مواردی نیز مسئله آگاهی واقعی و رضایت قابل بحث است؛ چرا که کاربران غالباً بدون درک دقیق دامنه پردازش داده‌ها، مدت نگهداری اطلاعات یا اشخاص ثالثی که به داده‌ها دسترسی دارند، با شرایط استفاده موافقت می‌کنند. از این منظر، رضایت

کاربر ممکن است صرفاً شکلی و فاقد کیفیت حقوقی لازم برای مشروعیت‌بخشی به پردازش داده‌ها باشد. (اقدسی، محقق داماد، ۱٤۰۰: ۵۵-۵٦)

در مقابل، در ارتباط غیرمستقیم، انتساب داده‌ها به اشخاص حقیقی بدون اطلاع یا رضایت مستقیم آن‌ها صورت می‌گیرد. این وضعیت به‌ویژه در مواردی رخ می‌دهد که اشیاء دارای شناسه‌های فنی نظیر سامانه‌های امواج رادیویی،[1] شناسه‌های شبکه یا تراشه‌های هوشمند هستند و در فرآیندهای روزمره نظیر خرید کالا، استفاده از خدمات حمل‌ونقل یا بهره‌برداری از زیرساخت‌های عمومی مورد استفاده قرار می‌گیرند. پیچیدگی این مسئله زمانی افزایش می‌یابد که داده‌های حاصل از اشیاء متعدد با یکدیگر تجمیع شوند. در چنین شرایطی، حتی اگر داده‌های مربوط به یک شیء به‌تنهایی حاوی اطلاعات هویتی نباشد، اتصال آن به داده‌های سایر اشیاء مرتبط با یک شخص مشخص، امکان شناسایی وی را فراهم می‌کند. به‌عنوان مثال، ممکن است اطلاعات دریافتی از یک شیء منفرد فاقد نشانه‌های مستقیم هویتی باشد، اما هنگامی که مشخص شود این شیء با مجموعه‌ای از اشیاء دیگر مرتبط است که به یک فرد معین تعلق دارند، داده‌های آن نیز به‌طور غیرمستقیم قابل انتساب به همان شخص خواهد بود. این فرایند که در ادبیات حقوق داده از آن به‌عنوان قابلیت شناسایی مجدد یاد می‌شود، یکی از چالش‌های اساسی حمایت از حریم خصوصی در محیط‌های داده‌محور محسوب می‌گردد. از منظر حقوقی، چنین وضعیتی موجب تضعیف اصل کنترل فرد بر داده‌های شخصی خود می‌شود؛ اصلی که در نظام‌های حقوقی معاصر، به‌ویژه در حقوق اتحادیه اروپا، به‌عنوان یکی از ارکان بنیادین حمایت از داده‌ها شناخته می‌شود. زمانی که اشخاص قادر به شناسایی، مدیریت یا محدودسازی پردازش داده‌های منتسب به خود نباشند، حق بر حریم خصوصی آنان به‌طور جدی در معرض نقض قرار می‌گیرد. افزون بر این، امکان شناسایی غیرمستقیم اشخاص از طریق اینترنت اشیاء، زمینه را برای نظارت گسترده، تحلیل رفتارها و حتی سوءاستفاده‌های مجرمانه فراهم می‌سازد. (احمدوند، جهانشاهی، ۱٤۰۲: ٦۹-۷۰)

در نتیجه، شناسایی اطلاعات شخصی در بستر اینترنت اشیاء صرفاً یک مسئله فنی نیست، بلکه چالشی بنیادین در تقاطع فناوری و حقوق به‌شمار می‌رود که مستلزم بازاندیشی در مفاهیمی چون رضایت، شفافیت، حداقل‌سازی داده‌ها و مسئولیت پردازش‌کنندگان است. عدم توجه به این چالش

[1] Radio Frequency Identification (RFID)

می‌تواند منجر به تضعیف اعتماد عمومی به فناوری‌های نوین و نقض گسترده حقوق بنیادین اشخاص در جامعه اطلاعاتی شود.

۲. بررسی مسئولیت ناشی از نقض امنیت داده‌ها در اینترنت اشیاء در اتحادیه اروپا

یکی از مهم‌ترین پیامدهای حقوقی توسعه اینترنت اشیاء، شکل‌گیری نظام مسئولیت ناشی از نقض داده‌های شخصی و از دست رفتن اطلاعات است. ماهیت اینترنت اشیاء به‌گونه‌ای است که پردازش داده‌ها در آن به‌صورت گسترده، مستمر و غالباً غیرمتمرکز انجام می‌شود و همین امر، خطر نقض امنیت داده‌ها را به‌طور قابل توجهی افزایش می‌دهد. در چنین شرایطی، فقدان تدابیر فنی و سازمانی مناسب می‌تواند منجر به افشای داده‌های شخصی، دسترسی غیرمجاز، از بین رفتن اطلاعات یا تغییر غیرقانونی آن‌ها شود؛ امری که به‌طور مستقیم مسئولیت حقوقی پردازش‌کنندگان داده و ارائه‌دهندگان خدمات اینترنت اشیاء را به دنبال دارد. (آقایی طوق، ناصر، ۱۳۹۹: ٤٨-٤٩)

در نظام حقوقی اتحادیه اروپا، مجموعه‌ای از مقررات داخلی و فراملی برای مقابله با نقض داده‌های شخصی و تضمین امنیت اطلاعات پیش‌بینی شده است. پیش از تصویب مقررات عمومی حمایت از داده‌ها، دستورالعمل 2002/58/EC در مورد پردازش داده‌های شخصی و حفاظت از حریم خصوصی در حوزه ارتباطات الکترونیکی، ارائه‌دهندگان خدمات را مکلف می‌کرد در صورت وجود خطر خاص برای امنیت شبکه، مشترکان را از این خطر و راهکارهای ممکن برای کاهش آن آگاه سازند. این الزام، بیانگر شناسایی اصل تعهد به اطلاع‌رسانی به‌عنوان یکی از عناصر اساسی مسئولیت در حوزه امنیت داده‌ها است؛ اصلی که بعدها در مقررات جدید حمایت از داده‌ها به‌صورت گسترده‌تری توسعه یافت. (Fabiano, 2017: 208)

اتحادیه اروپا همواره برای تدوین مقرراتی در حمایت از حریم خصوصی افراد کوشیده است و مقرراتی را به نام مقررات عمومی حفاظت از داده اتحادیه اروپا معروف به سند جی دی پی آر به تصویب رساند که در حقیقت جایگزینی برای قانون حفاظت از داده اتحادیه اروپا[1] است. با لازم‌الاجرا شدن مقررات عمومی حفاظت از داده‌های اتحادیه اروپا از ۲۵ می سال ۲۰۱۸، نظام حقوقی حمایت از داده‌ها وارد مرحله‌ای جدید و منسجم‌تر شد. جی دی پی آر مجموعه مقرراتی است که در مورد حفاظت از داده و محرمانگی همه اشخاص و خروج داده در اتحادیه اروپا و منطقه اقتصادی اروپا وضع شده است.

[1] Data Protection Directive, EC/95/46

این مقرره در ۱۱ فصل و ۹۹ ماده برای حفظ محرمانگی، اعطای کنترل داده ها به شهروندان و ساکنان این منطقه و یکسان سازی مقررات تنظیم شده است و شامل احکام و الزاماتی مرتبط با پردازش اطلاعات شخصی قابل تشخیص در اتحادیه اروپا در خصوص همه کسب و کارهایی که با این منطقه اقتصادی مراوده کاری دارند، صرف نظر از مکان استقرارشان می‌شود. بدین ترتیب فرایندهای کسب و کارهایی که اطلاعات شخصی را اداره می‌کنند، باید مبتنی بر حفاظت اطلاعات از طریق طراحی و به طور پیش فرض باشد؛ یعنی اطلاعات شخصی باید به گونه‌ای ذخیره شود که حداکثر محرمانگی به طور پیش فرض در نظر گرفته شود به نحوی که داده‌ها به هیچ وجه بدون رضایت صریح افراد در دسترس عمومی قرار نگیرد. (قناد، شریف، ۱٤۰۰: ٦-۷) این مقررات، با رویکردی یکپارچه، مسئولیت‌های مشخصی را برای کنترل‌کنندگان و پردازش‌کنندگان داده‌ها پیش‌بینی کرده و نقض داده‌های شخصی را به‌عنوان یکی از مهم‌ترین مخاطرات حقوق بنیادین اشخاص مورد توجه قرار داده است. مطابق ماده ۳۳ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، در صورت وقوع نقض داده‌های شخصی، مسئول پردازش داده‌ها موظف است بدون تأخیر غیرموجه و حداکثر ظرف ۷۲ ساعت پس از آگاهی از وقوع نقض، موضوع را به مرجع نظارتی صالح گزارش دهد. این الزام، نه‌تنها جنبه شکلی دارد، بلکه بیانگر اصل پاسخ‌گویی و شفافیت در قبال پردازش داده‌ها است. (GDPR, 2016)

علاوه بر تعهد به اعلام نقض داده‌ها، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا دامنه مسئولیت را به مرحله پیشینی پردازش داده‌ها نیز گسترش داده است. بر این اساس، در مواردی که نوع پردازش داده‌ها، به‌ویژه در فناوری‌های نوظهوری مانند اینترنت اشیاء، با خطرات بالا برای حقوق و آزادی‌های اشخاص همراه باشد، انجام ارزیابی اثرات حفاظت از داده‌ها[1] پیش از آغاز پردازش الزامی است. این سازوکار، با هدف شناسایی و کاهش ریسک‌های احتمالی، پردازش‌کنندگان داده را ملزم می‌کند پیش از بهره‌برداری از سامانه‌های داده‌محور، پیامدهای حقوقی و امنیتی فعالیت‌های خود را مورد بررسی قرار دهند. عدم انجام ارزیابی تأثیر حفاظت از داده‌ها در موارد الزامی، می‌تواند به‌عنوان تخلف مستقل تلقی شده و مبنای مسئولیت اداری قرار گیرد.

از نوآوری‌های مهم مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، می‌توان به نهادینه‌سازی مفاهیمی نظیر مسئول حفاظت از داده‌ها و اصل حمایت از داده‌ها از بدو طراحی و به‌صورت پیش‌فرض

[1] Data Protection Impact Assessment (DPIA)

اشاره کرد. این مفاهیم، بیانگر تغییر رویکرد قانون‌گذار از واکنش پسینی به نقض داده‌ها، به پیشگیری فعالانه از وقوع آن‌ها است. در چارچوب اینترنت اشیاء، این رویکرد اهمیت دوچندانی می‌یابد؛ زیرا معماری فنی این سامانه‌ها، در صورت طراحی نامناسب، می‌تواند به‌صورت ساختاری زمینه‌ساز نقض داده‌ها باشد. از این رو، مسئولیت پردازش‌کنندگان صرفاً به جبران خسارت پس از وقوع نقض محدود نمی‌شود، بلکه شامل تعهد به پیش‌بینی و کاهش ریسک‌ها در مرحله طراحی و اجرا نیز می‌گردد. (لطیف‌زاده، قبولی درافشان، محسنی، عابدی، ۱۴۰۲: ۹۹۱-۹۹۵)

از منظر حقوقی، نقض داده‌های شخصی در اینترنت اشیاء می‌تواند پیامدهای متعددی در حوزه مسئولیت مدنی و اداری به همراه داشته باشد. افشای داده‌ها یا از دست رفتن اطلاعات ممکن است موجب ورود خسارت مادی یا معنوی به اشخاص شود و زمینه مطالبه جبران خسارت را فراهم آورد. افزون بر این، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا با پیش‌بینی ضمانت‌اجراهای اداری سنگین، از جمله جریمه‌های مالی قابل توجه، تلاش کرده است بازدارندگی مؤثری در برابر بی‌توجهی به الزامات امنیت داده‌ها ایجاد کند. این ضمانت‌اجراها نشان‌دهنده اهمیت بنیادین حمایت از داده‌های شخصی در نظم حقوقی معاصر است. در نهایت، باید تأکید کرد که مسئولیت ناشی از نقض داده‌ها در اینترنت اشیاء، صرفاً نتیجه یک حادثه فنی یا خطای فردی نیست، بلکه اغلب حاصل تصمیمات ساختاری، طراحی‌های ناکارآمد و فقدان رویکرد حقوق‌محور در توسعه فناوری است. از این‌رو، تحلیل مسئولیت در این حوزه مستلزم نگاهی جامع است که هم‌زمان ابعاد فنی، سازمانی و حقوقی را در بر گیرد. تنها در چنین چارچوبی می‌توان از حقوق اشخاص در برابر مخاطرات فزاینده اینترنت اشیاء حمایت مؤثر به عمل آورد و تعادلی معقول میان نوآوری فناورانه و تضمین حقوق بنیادین برقرار ساخت. (آقایی طوق، ناصر، ۱۳۹۹: ۳۵)

۳. تدابیر تضمین امنیت داده و صیانت از حریم خصوصی در اینترنت اشیاء در مقررات عمومی حفاظت از داده‌های اتحادیه اروپا

گسترش شتابان فناوری‌های مبتنی بر اینترنت اشیاء و نفوذ آن در حوزه‌های متنوعی همچون سلامت، حمل‌ونقل، انرژی، خانه‌های هوشمند، صنعت و خدمات عمومی، موجب افزایش چشمگیر حجم و تنوع داده‌های شخصی در گردش شده است. این داده‌ها غالباً به‌صورت مستمر، خودکار و در مقیاسی

وسیع جمع‌آوری، تحلیل و ذخیره می‌شوند و در بسیاری موارد شامل اطلاعات حساس مانند داده‌های زیستی، مکانی، رفتاری و الگوهای مصرفی اشخاص هستند. بدین ترتیب، اینترنت اشیاء محیطی ایجاد کرده است که در آن خطرات نقض حریم خصوصی، سوءاستفاده از داده، رهگیری غیرمجاز، دسترسی غیرقانونی و حتی مداخله در امنیت فیزیکی افراد، به‌طور هم‌زمان مطرح می‌شود.

مدیریت پایدار این چالش‌ها بدون چارچوب حقوقی منسجم و سازوکارهای تنظیم‌گری مؤثر امکان‌پذیر نمی‌باشد. مقررات عمومی حفاظت از داده‌های اتحادیه اروپا به‌عنوان یکی از اثرگذارترین چارچوب‌ها در حوزه حمایت از داده‌های شخصی شناخته می‌شود و به‌طور گسترده به‌عنوان استاندارد جهانی حفاظت از داده‌ها مورد استناد قرار می‌گیرد. دامنه شمول مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، بر اینترنت اشیاء بر اساس معیارهای سرزمینی و شخصی تعریف می‌شود. مطابق ماده ۳ این مقرره، دامنه قلمرو مقررات عمومی حفاظت از داده‌های اتحادیه اروپا در سه وضعیت اصلی اعمال می‌شود: نخست، هنگامی که پردازش داده‌های شخصی در چارچوب فعالیت‌های یک مؤسسه مستقر در اتحادیه اروپا انجام گیرد، حتی اگر خود عملیات پردازش در خارج از اتحادیه صورت پذیرد؛ دوم، زمانی که داده‌های شخصی اشخاص مقیم اتحادیه اروپا توسط نهادی خارج از اتحادیه پردازش شود، مشروط بر آنکه این پردازش با عرضه کالا یا خدمات به آنان یا نظارت بر رفتار آنان در اتحادیه مرتبط باشد؛ و سوم، در مواردی که حقوق بین‌الملل عمومی اجرای مقررات اتحادیه را ایجاب کند. (GDPR, 2016: Art. 3) با توجه به ماهیت فرامرزی اینترنت اشیاء و ارائه خدمات دیجیتال به کاربران در قلمروهای مختلف، بسیاری از تولیدکنندگان و ارائه‌دهندگان خدمات اینترنت اشیاء حتی اگر در خارج از اتحادیه اروپا مستقر باشند، در عمل مشمول الزامات مقررات عمومی حفاظت از داده‌های اتحادیه اروپا قرار می‌گیرند. بر این اساس، تولیدکنندگان، توسعه‌دهندگان، اپراتورها و بهره‌برداران سامانه‌های اینترنت اشیاء که در مقام کنترل‌کننده داده عمل می‌کنند، مکلف‌اند تدابیری برای تضمین امنیت داده و صیانت از حریم خصوصی کاربران اتخاذ نمایند.

۳-۱. شناسایی کنترل‌کننده در اکوسیستم اینترنت اشیاء

یکی از بنیادی‌ترین اهداف نظام‌های حمایت از داده‌های شخصی، به‌ویژه در چارچوب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، ایجاد ساختاری روشن برای تخصیص مسئولیت، پاسخگویی و امکان انتساب تعهدات حقوقی در اکوسیستم‌های پیچیده پردازش داده است. در واقع، منطق حاکم بر

مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، مبتنی بر این فرض است که بدون شناسایی دقیق بازیگران اصلی پردازش و تعیین جایگاه حقوقی آنان، تحقق اصولی چون شفافیت، پاسخگویی[1] و تضمین حقوق موضوعه اشخاص داده ممکن نخواهد بود. (GDPR, 2016) بر اساس مقررات عمومی حفاظت از داده‌های اتحادیه اروپا:

کنترل‌کننده[2] شخص یا نهادی است که اهداف و شیوه‌های پردازش داده‌های شخصی را تعیین می‌کند.

کنترل‌کنندگان مشترک[3] دو یا چند نهادی هستند که مشترکاً اهداف و شیوه‌های پردازش را تعیین می‌کنند.

پردازشگر[4] نهادی است که به‌موجب قرارداد و به نمایندگی از کنترل‌کننده، داده‌ها را پردازش می‌کند.

دریافت‌کننده[5] هر شخص یا نهادی است که داده‌های شخصی برای او افشا می‌شود.

شخص ثالث[6] هر نهادی است که در دسته‌های فوق قرار نمی‌گیرد.

در بستر اینترنت اشیاء، تعیین مسئولیت حفاظت از داده و حریم خصوصی مستلزم بررسی این پرسش است که آیا توسعه‌دهنده، تولیدکننده یا فروشنده سامانه، در جایگاه کنترل‌کننده، کنترل‌کننده مشترک یا پردازشگر قرار می‌گیرد یا خیر. در بسیاری از سامانه‌های اینترنت اشیاء، اگر تولیدکننده یک دستگاه هوشمند، داده‌های کاربران را برای بهبود الگوریتم‌های اختصاصی خود جمع‌آوری و تحلیل کند، در این بخش از پردازش، نقش کنترل‌کننده خواهد داشت. اگر همان تولیدکننده داده‌ها را صرفاً به دستور یک ارائه‌دهنده خدمات سلامت پردازش کند، ممکن است در جایگاه پردازشگر قرار گیرد. چنانچه دو شرکت مشترکاً درباره طراحی سامانه، نحوه جمع‌آوری داده و مقاصد بهره‌برداری تصمیم‌گیری کنند، وضعیت کنترل مشترک شکل می‌گیرد. بنابراین، در اکوسیستم اینترنت اشیاء، نقش‌ها می‌توانند نسبی، چندلایه و حتی هم‌زمان باشند؛ به‌گونه‌ای که یک بازیگر در بخشی از زنجیره پردازش کنترل‌کننده و در بخش دیگر پردازشگر محسوب شود. (Hadzovic, et al. 2021: 13)

بر اساس ماده ۲۵ و بند ۷۸ مقدمه مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، کنترل‌کننده مکلف است اصول حفاظت از داده را از مرحله طراحی و تعیین شیوه پردازش در سیستم ادغام کند. همچنین، ماده ۲۸ این مقرره پردازشگران را ملزم می‌کند که تضمین‌های کافی درباره اجرای تدابیر فنی

1 Accountability
2 Controller
3 Joint Controllers
4 Processor
5 Recipient
6 Third Party

و سازمانی مناسب ارائه دهند. این تضمین‌ها باید در قالب قراردادهای پردازش داده[1] تنظیم شوند و شامل تعهداتی درباره محرمانگی، امنیت، همکاری با کنترل‌کننده و امکان بازرسی باشند. (GDPR, 2016: Arts. 25 and 28)

ماهیت پیچیده و چندلایه سامانه‌های اینترنت اشیاء موجب می‌شود توسعه‌دهندگان مستقل اجزای مختلف این سامانه‌ها، غالباً در زمره کنترل‌کنندگان مشترک یا کنترل‌کنندگان مستقل قرار گیرند؛ مگر در موارد استثنایی که در مرحله توسعه، داده شخصی پردازش نشده باشد. علاوه بر این، بازیگران دیگری نیز در شبکه اینترنت اشیاء ایفای نقش می‌کنند؛ از جمله مدیر داده، ارائه‌دهندگان خدمات، تأمین‌کنندگان داده اینترنت اشیاء، فراهم‌کنندگان چارچوب فنی، حاملان داده و توسعه‌دهندگان برنامه‌های کاربردی. هر یک از این بازیگران، بسته به میزان اختیار و نقش‌شان در تعیین اهداف یا وسایل پردازش، ممکن است در جایگاه کنترل‌کننده، کنترل‌کننده مشترک یا پردازشگر قرار گیرند. ازاین‌رو، تحلیل دقیق قراردادها، معماری فنی سامانه و جریان واقعی داده برای تعیین مسئولیت ضروری است. (Babalola, 2021: 314)

در نهایت، هر توسعه‌دهنده‌ای که در زنجیره پردازش داده در اینترنت اشیاء نقش دارد، در صورت پردازش داده شخصی، مکلف به رعایت اصول مقررات عمومی حفاظت از داده‌های اتحادیه اروپا و تضمین حفاظت از حریم خصوصی است. بنابراین، شناسایی دقیق نقش‌ها، تنظیم شفاف روابط قراردادی، مستندسازی جریان داده و اتخاذ رویکرد پاسخگویی فعال برای تمامی بازیگران زنجیره پردازش، پیش‌شرط تحقق واقعی حمایت از حریم خصوصی در این فناوری نوظهور است.

۳-۲. استفاده از بیانیه‌های حریم خصوصی در اکوسیستم اینترنت اشیاء

یکی از بنیادی‌ترین سازوکارهای تحقق اصل شفافیت در نظام‌های حمایت از داده‌های شخصی، به‌ویژه در چارچوب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، تدوین و ارائه بیانیه‌ها یا سیاست‌های حریم خصوصی است. در بستر اینترنت اشیاء، اهمیت این ابزار حقوقی به‌مراتب برجسته‌تر می‌شود؛ زیرا این سامانه‌ها غالباً به‌صورت مستمر، خودکار و در پس‌زمینه، داده‌های شخصی را جمع‌آوری، تحلیل، انتقال و ذخیره می‌کنند، بی‌آنکه کاربر در هر مرحله از این فرآیند نقش فعال یا آگاهی مستقیم داشته باشد. ویژگی‌هایی چون اتصال دائمی، پردازش آنی، تعامل میان‌دستگاهی و ذخیره‌سازی ابری موجب می‌شود که حجم، تنوع و حساسیت داده‌های گردآوری‌شده در اینترنت اشیاء بسیار گسترده

[1] Data Processing Agreements

باشد. در چنین شرایطی، تضمین حق آگاهی کاربران نسبت به ماهیت، دامنه و اهداف پردازش داده‌هایشان، به یکی از ارکان اساسی حمایت از حریم خصوصی تبدیل می‌شود.

اصل شفافیت که در ماده ۵ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا تصریح شده است، اقتضا دارد پردازش داده‌های شخصی به‌صورت قانونی، منصفانه و شفاف نسبت به شخص موضوع داده انجام گیرد. این اصل در مواد ۱۲ تا ١٤ این مقرره به‌طور تفصیلی نهادینه شده و به‌ویژه ماده ۱۳ کنترل‌کننده را مکلف می‌سازد در زمان جمع‌آوری داده‌های شخصی، اطلاعات مشخصی را در اختیار شخص موضوع داده قرار دهد. این اطلاعات شامل هویت و اطلاعات تماس کنترل‌کننده و در صورت لزوم نماینده یا مسئول حفاظت از داده، اهداف پردازش و مبنای قانونی آن، منافع مشروع مورد استناد، گیرندگان داده، احتمال انتقال داده به خارج از اتحادیه اروپا و تضمین‌های مربوط، مدت زمان نگهداری داده یا معیارهای تعیین آن، حقوق اشخاص داده از جمله حق دسترسی، اصلاح، حذف، محدودسازی پردازش، اعتراض و قابلیت انتقال داده، حق طرح شکایت نزد مقام نظارتی، الزام یا اختیاری بودن ارائه داده و نیز وجود تصمیم‌گیری خودکار و منطق کلی حاکم بر آن است. در محیط اینترنت اشیاء که غالباً با تحلیل‌های الگوریتمی، یادگیری ماشین و تصمیم‌گیری خودکار همراه است، افشای اطلاعات مربوط به منطق پردازش و پیامدهای احتمالی آن برای کاربران اهمیتی مضاعف دارد. (GDPR, 2016: Arts. 12-14)

بیانیه‌های حریم خصوصی در این چارچوب صرفاً اسنادی اطلاع‌رسانی نیستند، بلکه جلوه‌ای از اصل پاسخگویی محسوب می‌شوند. کنترل‌کننده نه‌تنها مکلف به رعایت مقررات است، بلکه باید بتواند این رعایت را اثبات کند. تدوین سیاست حریم خصوصی دقیق، منطبق با واقعیت‌های فنی سامانه و هماهنگ با جریان واقعی داده، بخشی از این سازوکار پاسخگویی است. در اکوسیستم اینترنت اشیاء که ممکن است چندین بازیگر از جمله تولیدکنندگان دستگاه، توسعه‌دهندگان نرم‌افزار، ارائه‌دهندگان خدمات ابری و شرکت‌های تحلیل‌گر داده در پردازش اطلاعات نقش داشته باشند، بیانیه حریم خصوصی باید ساختار زنجیره پردازش را به‌صورت شفاف منعکس کند و نقش هر بازیگر را در مقام کنترل‌کننده، کنترل‌کننده مشترک یا پردازشگر روشن سازد. عدم شفافیت در این زمینه نه‌تنها با الزامات قانونی ناسازگار است، بلکه می‌تواند به تضعیف اعتماد کاربران و افزایش مسئولیت حقوقی اپراتورها منجر شود.

از منظر ماهوی، بیانیه‌های حریم خصوصی در اینترنت اشیاء باید اهداف جمع‌آوری داده را به‌صورت مشخص و قابل فهم بیان کنند و از به‌کارگیری عبارات کلی و مبهم پرهیز نمایند. نحوه استفاده، ذخیره،

انتقال و اشتراک‌گذاری داده‌ها باید به‌روشنی توضیح داده شود، از جمله اینکه داده‌ها در چه زیرساختی نگهداری می‌شوند، چه مدت ذخیره خواهند شد و آیا به اشخاص ثالث یا به خارج از حوزه‌های قضایی خاص منتقل می‌شوند یا خیر. همچنین، در مواردی که پردازش مبتنی بر رضایت است، کاربران باید امکان واقعی برای انتخاب، مدیریت تنظیمات حریم خصوصی و انصراف از رضایت داشته باشند. بیانیه‌های حریم خصوصی باید سازوکارهای عملی برای اعمال حقوق قانونی کاربران را نیز پیش‌بینی کنند و اطلاعات مربوط به تصمیم‌گیری خودکار را به‌صورت روشن و قابل درک ارائه دهند. (Kuner, et al. 2020: 37)

با وجود این الزامات، چالش‌های عملی متعددی در زمینه اثربخشی بیانیه‌های حریم خصوصی در اینترنت اشیاء وجود دارد. بسیاری از این اسناد طولانی، پیچیده و آکنده از اصطلاحات فنی هستند و کاربران عملاً آن‌ها را مطالعه نمی‌کنند. افزون بر این، برخی دستگاه‌های اینترنت اشیاء فاقد نمایشگر یا رابط کاربری گسترده‌اند، که ارائه اطلاعات تفصیلی را دشوار می‌سازد. همچنین، بخش قابل توجهی از پردازش داده در لایه‌های زیرساختی یا ابری انجام می‌شود و برای کاربر قابل مشاهده نیست. ازاین‌رو، تحقق واقعی اصل شفافیت مستلزم رویکردی فراتر از ارائه یک متن استاندارد است. برای افزایش کارآمدی، بیانیه‌های حریم خصوصی در اینترنت اشیاء باید به‌صورت لایه‌بندی‌شده، خلاصه و با زبان ساده تنظیم شوند و در صورت امکان در قالب‌های بصری یا تعاملی ارائه گردند. یکپارچه‌سازی این بیانیه‌ها در طراحی سامانه، ایجاد داشبوردهای مدیریت حریم خصوصی و به‌روزرسانی پویا متناسب با تغییرات پردازش می‌تواند به ارتقای قابلیت فهم و اعتماد کاربران کمک کند. چنین رویکردی با اصل حفاظت از داده از طریق طراحی و به‌صورت پیش‌فرض نیز هم‌راستا است و نشان‌دهنده گذار از نگاه شکلی به بیانیه‌های حریم خصوصی به‌سوی کارکردی حکمرانی داده‌محور است. (Babalola, 2021: 315)

در نهایت، در اکوسیستم اینترنت اشیاء، بیانیه‌های حریم خصوصی باید به‌عنوان ابزارهایی برای تضمین شفافیت، پاسخگویی و تقویت اعتماد عمومی تلقی شوند، نه صرفاً به‌عنوان اسنادی نمادین برای رفع تکلیف قانونی. اثربخشی این ابزارها زمانی محقق می‌شود که منطبق با واقعیت‌های فنی سامانه، قابل فهم برای کاربران و نهادینه‌شده در معماری فناوری باشند. در غیر این صورت، خطر آن وجود دارد که این بیانیه‌ها به متونی غیرکارآمد تقلیل یابند و نقش حمایتی خود در صیانت از حریم خصوصی را از دست بدهند.

۳-۳. حریم خصوصی و حفاظت از داده از طریق طراحی و به‌صورت پیش‌فرض

گسترش اینترنت اشیاء به‌عنوان یکی از مهم‌ترین جلوه‌های تحول دیجیتال، موجب شکل‌گیری محیطی شده است که در آن اشیاء فیزیکی و سامانه‌های دیجیتال به‌طور مستمر با یکدیگر و با اشخاص انسانی تعامل دارند. این تعامل گسترده و مداوم، مستلزم جمع‌آوری، پردازش و تحلیل حجم عظیمی از داده‌هاست که بخش قابل توجهی از آن‌ها ماهیت شخصی یا حتی حساس دارند. در چنین فضایی، مخاطرات نقض حریم خصوصی دیگر محدود به رفتارهای استثنایی یا سوءاستفاده‌های موردی نیست، بلکه به‌صورت ساختاری در دل طراحی و عملکرد سامانه‌های فناورانه نهفته است. همین ویژگی، سیاست‌گذاران و نهادهای تنظیم‌گر را واداشته است تا به‌جای واکنش‌های پسینی، به دنبال رویکردهای پیشگیرانه و ساختاری در حمایت از حریم خصوصی باشند. در این چارچوب، رویکرد حریم خصوصی در طراحی به‌عنوان پاسخی نظری و عملی به چالش‌های نوظهور حریم خصوصی مطرح شد. این رویکرد که نخستین بار در سال ۲۰۱۰ به‌طور منسجم صورت‌بندی گردید، بر این ایده بنیادین استوار است که حریم خصوصی نباید صرفاً در مرحله انطباق با قوانین یا پس از وقوع نقض داده‌ها مورد توجه قرار گیرد، بلکه باید از همان مراحل اولیه طراحی، توسعه و استقرار سامانه‌ها در نظر گرفته شود. به بیان دیگر، حریم خصوصی باید به‌عنوان یکی از عناصر ذاتی و جدایی‌ناپذیر معماری سیستم‌های فناورانه تلقی گردد، نه به‌عنوان ملاحظه‌ای حاشیه‌ای یا مانعی در برابر نوآوری. (Semantha, et al. 2020: 5)

یکی از نوآوری‌های بنیادین مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، نهادینه‌سازی اصل حفاظت از داده از طریق طراحی و به‌صورت پیش‌فرض[1] است؛ اصلی که در ماده ۲۵ این مقرره تصریح شده و بیانگر گذار از رویکرد واکنشی به رویکردی پیشگیرانه در حکمرانی داده‌های شخصی است. بر اساس این رویکرد، حمایت از داده و صیانت از حریم خصوصی نه صرفا امری الحاقی و پسینی، بلکه باید جزء لاینفک معماری فنی و سازمانی سامانه‌ها از نخستین مراحل طراحی تلقی شود. اهمیت این رویکرد در حوزه اینترنت اشیاء دو چندان است. سامانه‌های مبتنی بر اینترنت اشیاء، به‌طور ذاتی داده‌محور، خودکار و فراگیر هستند و اغلب بدون مداخله مستقیم کاربر فعالیت می‌کنند. در چنین سامانه‌هایی، اگر الزامات حریم خصوصی در مرحله طراحی لحاظ نشود، امکان اعمال کنترل مؤثر بر داده‌ها در مراحل بعدی به‌شدت محدود خواهد شد. از این رو، رویکرد حریم خصوصی در طراحی

[1] Data Protection by Design and by Default

می‌کوشد با پیش‌بینی ریسک‌ها و ادغام ملاحظات حقوقی در تصمیمات فنی، از بروز نقض‌های گسترده حریم خصوصی جلوگیری کند. بر اساس این رویکرد، سامانه‌ها باید به‌گونه‌ای طراحی شوند که حتی در صورت عدم اقدام فعال کاربر، بیشترین سطح حفاظت از حریم خصوصی به‌طور خودکار اعمال شود. این امر، به‌ویژه در اینترنت اشیاء که کاربران غالباً از جزئیات پردازش داده‌ها آگاه نیستند، اهمیت اساسی دارد. (Luthfi, Minhar, 2022: 461)

در واقع مقررات عمومی حفاظت از داده‌های اتحادیه اروپا با پذیرش رویکرد حمایت از داده‌ها و حریم خصوصی در طراحی و به‌صورت پیش‌فرض، تلاش کرده است اصول حریم خصوصی از بدو طراحی را به تعهدات الزام‌آور حقوقی تبدیل کند. بر اساس این مقررات، کنترل‌کنندگان داده موظف‌اند در تعیین ابزارها و شیوه‌های پردازش داده‌ها، تدابیر فنی و سازمانی مناسب را به‌گونه‌ای اتخاذ کنند که اصول بنیادین حمایت از داده‌ها به‌طور مؤثر رعایت شود. بدین ترتیب، حریم خصوصی دیگر صرفاً یک ارزش اخلاقی یا توصیه سیاستی نیست، بلکه به یک الزام حقوقی صریح تبدیل می‌شود. (معینی‌فر، وحیدزاده، ۱٤۰۱، ٦۸) اصل حفاظت از داده از طریق طراحی اقتضا دارد که کنترل‌کنندگان، با لحاظ وضعیت دانش فنی، هزینه‌های اجرا، ماهیت، دامنه، زمینه و اهداف پردازش و نیز میزان خطر برای حقوق و آزادی‌های اشخاص، تدابیر فنی و سازمانی مناسب را به‌گونه‌ای در سامانه ادغام کنند که اصول بنیادین حفاظت از داده‌ها در عمل محقق شود. در کنار آن، مفهوم حفاظت از داده به‌صورت پیش‌فرض ایجاب می‌کند که به‌طور پیش‌فرض، تنها آن دسته از داده‌های شخصی که برای هر هدف مشخص ضروری است پردازش شود؛ به بیان دیگر، تنظیمات اولیه سامانه باید حداکثر سطح حمایت از حریم خصوصی را تضمین کند، بدون آنکه کاربر ناگزیر به مداخله فعال برای محدودسازی پردازش باشد. در چارچوب ماده ۲۵ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، کنترل‌کنندگان مکلف‌اند اصولی همچون حداقل‌گرایی در جمع‌آوری داده،[1] محدودیت نگهداری،[2] مشروعیت پردازش، شفافیت، و تضمین محرمانگی و تمامیت داده‌ها[3] را در ساختار سامانه‌های خود تعبیه کنند. این الزام، به‌ویژه در اینترنت اشیاء که دستگاه‌ها به‌صورت مستمر داده‌های محیطی، رفتاری، زیستی یا مکانی را جمع‌آوری می‌کنند، مستلزم

1. Data Minimization
2. Storage Limitation
3. Integrity and Confidentiality

بازنگری اساسی در نحوه طراحی سخت‌افزار، نرم‌افزار و زیرساخت‌های ارتباطی است. (GDPR, 2016: Art. 25)

حداقل‌گرایی در جمع‌آوری داده اقتضا دارد که سامانه‌های اینترنت اشیاء صرفاً داده‌هایی را گردآوری کنند که برای هدف مشخص و مشروع ضروری است و از جمع‌آوری گسترده و بی‌ضابطه اطلاعات پرهیز نمایند. این امر مستلزم تحلیل دقیق اهداف پردازش در مرحله طراحی و محدودسازی قابلیت‌های جمع‌آوری داده در سطح فنی است. محدودیت نگهداری نیز ایجاب می‌کند داده‌ها تنها برای مدتی که برای تحقق هدف لازم است ذخیره شوند و سازوکارهای حذف یا ناشناس‌سازی خودکار در معماری سامانه پیش‌بینی شود. مشروعیت پردازش مستلزم تعیین و مستندسازی مبنای قانونی مناسب، اعم از رضایت، اجرای قرارداد، تکلیف قانونی یا منافع مشروع، پیش از آغاز پردازش است. افزون بر این، تضمین محرمانگی و تمامیت داده‌ها مستلزم به‌کارگیری تدابیر امنیتی نظیر رمزنگاری، کنترل دسترسی، ثبت وقایع و ارزیابی مستمر آسیب‌پذیری‌هاست. در این چارچوب، تولیدکنندگان و توسعه‌دهندگان اینترنت اشیاء مسئولیت مضاعفی بر عهده دارند. آنان باید پیش از عرضه محصول به بازار، تحلیل اثرات حفاظت از داده[1]را در موارد پرخطر انجام دهند، جریان داده‌ها را مستندسازی کنند و از هم‌راستایی معماری فنی با الزامات حقوقی اطمینان حاصل نمایند. همچنین، تعیین دقیق مبنای قانونی پردازش، پیش‌بینی سازوکارهای اخذ و مدیریت رضایت، تضمین امنیت ارتباطات میان دستگاه‌ها و جلوگیری از سوءاستفاده یا دسترسی غیرمجاز به داده‌ها، بخشی از تعهدات ساختاری آنان است. پرهیز از نگهداری بیش از حد ضرورت و خودداری از جمع‌آوری داده‌های نامرتبط یا مازاد نیز باید در سطح طراحی فنی به‌صورت پیش‌فرض اعمال شود، نه اینکه صرفاً در اسناد سیاستی مورد اشاره قرار گیرد. (EDPB, 2020: Guidelines 4/2019)

فناوری‌های تقویت‌کننده حریم خصوصی[2]در این میان نقشی کلیدی ایفا می‌کنند. استفاده از تکنیک‌هایی نظیر رمزنگاری سرتاسری، ناشناس‌سازی یا شبه‌ناشناس‌سازی داده‌ها، پردازش محلی به‌جای انتقال متمرکز داده و طراحی شناسه‌های موقتی به‌جای شناسه‌های دائمی می‌تواند به کاهش خطرات نقض حریم خصوصی بینجامد. با این حال، تحقق واقعی اصل حفاظت از داده از طریق طراحی مستلزم تغییر پارادایم در صنعت فناوری است. در بسیاری از موارد، انگیزه‌های تجاری مبتنی بر تحلیل

1Data Protection Impact Assessment – DPIA
2Privacy Enhancing Technologies – PETs

کلان‌داده و بهره‌برداری حداکثری از اطلاعات رفتاری کاربران، با منطق حداقل‌گرایی در جمع‌آوری داده در تعارض قرار می‌گیرد. ازاین‌رو، نقش مقررات‌گذاری و نظارت مؤثر نهادهای صلاحیت‌دار، در کنار ارتقای فرهنگ مسئولیت‌پذیری در میان تولیدکنندگان، اهمیت اساسی دارد. اصل حفاظت از داده از طریق طراحی در واقع تلاشی برای درونی‌سازی الزامات حقوقی در معماری فناوری و تبدیل حمایت از حریم خصوصی به یک معیار رقابتی و کیفیت‌محور در بازار دیجیتال است. (Kuner, et al. 2020: 43)

در مجموع، در نظام اینترنت اشیاء که ویژگی‌هایی مانند اتصال گسترده دستگاه‌ها، جمع‌آوری و پردازش مستمر داده‌ها و مشارکت بازیگران متعدد در آن مشاهده می‌شود، اصل «حفاظت از داده از طریق طراحی و به‌صورت پیش‌فرض» صرفاً یک الزام شکلی یا اداری نیست، بلکه پیش‌شرط اساسی برای مشروعیت و مقبولیت این فناوری به شمار می‌آید. رعایت این اصل تضمین می‌کند که حمایت از حریم خصوصی کاربران از همان ابتدای طراحی سامانه‌ها در نظر گرفته شود، نه آنکه تنها پس از بروز نقض یا خسارت مورد توجه قرار گیرد. این رویکرد با تغییر جهت از واکنش پس از وقوع تخلف، به پیشگیری ساختاری و پیش‌دستانه از مخاطرات، تلاش می‌کند خطرات احتمالی برای حقوق و آزادی‌های اشخاص را پیش از تحقق، کاهش دهد. در نتیجه، میان توسعه و نوآوری فناورانه از یک سو و حمایت مؤثر از حقوق بنیادین اشخاص، به‌ویژه حق بر حریم خصوصی و حفاظت از داده‌های شخصی، نوعی توازن برقرار می‌شود. چنین رویکردی زمینه‌ساز شکل‌گیری نظامی پایدار و مسئولانه برای حکمرانی داده‌ها در عصر فناوری‌های هوشمند و متصل است؛ نظمی که در آن پیشرفت فناوری با احترام به کرامت و حقوق انسان همراه باشد.

نتیجه‌گیری

تحول فناورانه ناشی از گسترش اینترنت اشیاء، ساختار سنتی پردازش داده‌های شخصی را به‌طور بنیادین دگرگون ساخته و محیطی ایجاد کرده است که در آن جمع‌آوری، تحلیل و تبادل داده‌ها به‌صورت مستمر، خودکار و در مقیاسی گسترده انجام می‌گیرد. ویژگی‌هایی همچون اتصال دائمی اشیاء، پردازش در زمان واقعی، تجمیع کلان‌داده‌ها و تعامل میان‌دستگاهی، اگرچه ظرفیت‌های قابل توجهی برای ارتقای کارایی، بهره‌وری و کیفیت زندگی فراهم می‌آورد، اما هم‌زمان مخاطرات ساختاری و چندلایه‌ای را برای حریم خصوصی و حمایت از داده‌های شخصی ایجاد می‌کند. بر این اساس، مسئله اصلی این پژوهش

بررسی چگونگی مواجهه نظام حقوقی با این مخاطرات در پرتو مقررات عمومی حفاظت از داده‌های اتحادیه اروپا بود. تحلیل انجام‌شده در این مقاله نشان داد که چالش‌های حریم خصوصی در اینترنت اشیاء صرفاً ناشی از نقض‌های موردی یا خطاهای فنی نیست، بلکه ریشه در معماری داده‌محور و طراحی ساختاری این فناوری دارد. ردیابی مستمر مکانی، امکان شناسایی و انتساب داده‌های ظاهراً غیرشخصی از طریق تجمیع و تحلیل الگوریتمی، پردازش نامرئی و بدون آگاهی مؤثر کاربران و نیز آسیب‌پذیری‌های امنیتی ناشی از اتصال گسترده دستگاه‌ها، همگی می‌توانند به نقض گسترده حقوق بنیادین اشخاص منجر شوند. به‌ویژه در حوزه داده‌های مکانی و رفتاری، قابلیت ترسیم الگوهای دقیق از زندگی خصوصی افراد، مرز میان بهره‌برداری مشروع فناورانه و نظارت فراگیر را به‌شدت باریک ساخته است. از سوی دیگر، ساختار چندبازیگری اینترنت اشیاء، از جمله تولیدکنندگان سخت‌افزار، توسعه‌دهندگان نرم‌افزار، ارائه‌دهندگان خدمات ابری، اپراتورهای شبکه و تحلیل‌گران داده، تعیین دقیق نقش‌ها و تخصیص مسئولیت را با پیچیدگی‌های جدی مواجه می‌سازد. یافته‌های پژوهش نشان داد که در چنین اکوسیستمی، تمایز میان کنترل‌کننده، کنترل‌کننده مشترک و پردازشگر اهمیت بنیادین دارد؛ زیرا تحقق اصول پاسخگویی، شفافیت و امکان اعمال حقوق موضوعه اشخاص، منوط به شناسایی دقیق بازیگر مسئول است. در بسیاری از موارد، یک بازیگر ممکن است در بخشی از زنجیره پردازش نقش کنترل‌کننده و در بخش دیگر نقش پردازشگر داشته باشد، امری که مستلزم تحلیل موردی جریان داده و تنظیم شفاف روابط قراردادی است. در پاسخ به پرسش اصلی پژوهش مبنی بر میزان کفایت چارچوب حقوقی مقررات عمومی حفاظت از داده‌های اتحادیه اروپا در مدیریت مخاطرات اینترنت اشیاء، یافته‌ها حاکی از آن است که این مقرره با اتخاذ رویکردی جامع، پیشگیرانه و مبتنی بر اصول بنیادین حمایت از داده‌ها، ابزارهای حقوقی قابل توجهی برای مواجهه با چالش‌های مذکور فراهم کرده است. اصل شفافیت، تعهد به اعلام نقض داده‌ها، الزام به انجام ارزیابی اثرات حفاظت از داده در موارد پرخطر، نهادینه‌سازی اصل حفاظت از داده از طریق طراحی و به‌صورت پیش‌فرض، همگی بیانگر گذار از رویکرد واکنشی به رویکردی ساختاری و پیش‌دستانه در حکمرانی داده‌ها می‌باشد. به‌طور خاص، اصل حفاظت از داده از طریق طراحی و به‌صورت پیش‌فرض را می‌توان مهم‌ترین پاسخ حقوقی به مخاطرات اینترنت اشیاء دانست؛ زیرا این اصل، حمایت از حریم خصوصی را از مرحله انطباق شکلی با قانون به سطح معماری فنی سامانه‌ها ارتقا می‌دهد. بر اساس این رویکرد، حداقل‌گرایی در جمع‌آوری داده، محدودیت نگهداری،

تعیین مبنای قانونی روشن برای پردازش، تضمین محرمانگی و تمامیت داده‌ها و پیش‌بینی سازوکارهای اعمال حقوق کاربران باید در همان مرحله طراحی سخت‌افزار و نرم‌افزار ادغام شود. بدین ترتیب، حریم خصوصی به‌عنوان یک ارزش الحاقی یا پسینی تلقی نمی‌شود، بلکه به عنصر ذاتی طراحی فناوری تبدیل می‌گردد. رویکرد حریم خصوصی از بدو طراحی، نقشی کلیدی در ایجاد تعادل میان نوآوری فناورانه و حمایت از حقوق بنیادین اشخاص ایفا می‌کند. ادغام ملاحظات حقوقی در مراحل اولیه طراحی و توسعه سامانه‌های اینترنت اشیاء امکان پیشگیری از بخش قابل توجهی از مخاطرات حریم خصوصی را فراهم می‌سازد و اعتماد عمومی به فناوری‌های نوین را تقویت می‌کند. تدوین و پذیرش استانداردهای بین‌المللی مبتنی بر این رویکرد می‌تواند گامی مؤثر در جهت همگرایی نظام‌های حقوقی و تضمین حمایت از داده‌های شخصی در سطح جهانی باشد. با این حال، پژوهش حاضر نشان می‌دهد که هرچند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا ظرفیت هنجاری بالایی برای مدیریت ریسک‌های اینترنت اشیاء دارد، تحقق عملی حمایت مؤثر از حریم خصوصی در این حوزه با چالش‌هایی مواجه است. نخست، پیچیدگی فنی سامانه‌ها و عدم تقارن اطلاعاتی میان کاربران و ارائه‌دهندگان خدمات، اعمال واقعی رضایت آگاهانه را دشوار می‌سازد. دوم، انگیزه‌های اقتصادی مبتنی بر تحلیل کلان‌داده و بهره‌برداری تجاری از داده‌های رفتاری، ممکن است با منطق حداقل‌گرایی در جمع‌آوری داده در تعارض قرار گیرد. سوم، ماهیت فرامرزی اینترنت اشیاء اجرای مؤثر مقررات و نظارت هماهنگ میان مراجع صلاحیت‌دار را با دشواری‌هایی همراه می‌کند. بر این اساس، فرضیه پژوهش مبنی بر اینکه «اگرچه مقررات عمومی حفاظت از داده‌های اتحادیه اروپا ابزارهای مناسبی برای مدیریت مخاطرات اینترنت اشیاء فراهم کرده است، اما اثربخشی آن منوط به ادغام واقعی الزامات حقوقی در طراحی فنی و تقویت سازوکارهای پاسخگویی است»، مورد تأیید قرار می‌گیرد. به بیان دیگر، کارآمدی این چارچوب نه صرفاً در سطح متن مقرره، بلکه در نحوه اجرا، نظارت و درونی‌سازی آن در فرهنگ سازمانی بازیگران فناوری معنا می‌یابد.

از منظر نظری، این پژوهش نشان می‌دهد که حکمرانی داده در عصر اینترنت اشیاء مستلزم بازاندیشی در مفاهیمی چون رضایت، کنترل فردی، مسئولیت و شفافیت است. در محیط‌هایی که پردازش داده به‌صورت نامرئی و الگوریتمی انجام می‌شود، اتکای صرف به رضایت به‌عنوان مبنای مشروعیت، کفایت ندارد و باید با سازوکارهای ساختاری و پیشگیرانه تکمیل شود. از منظر عملی نیز، پیشنهاد می‌شود:

۱. تحلیل اثرات حفاظت از داده در پروژه‌های اینترنت اشیاء به‌عنوان یک الزام واقعی و نه تشریفاتی اجرا شود؛
۲. قراردادهای میان بازیگران زنجیره پردازش با شفافیت کامل درباره تخصیص نقش‌ها و مسئولیت‌ها تنظیم گردد؛
۳. فناوری‌های تقویت‌کننده حریم خصوصی مانند رمزنگاری پیشرفته، ناشناس‌سازی مؤثر و پردازش محلی داده‌ها به‌صورت گسترده‌تری به‌کار گرفته شود؛
٤. مراجع نظارتی با رویکردی فعال، اجرای اصل حفاظت از داده از طریق طراحی را در محصولات اینترنت اشیاء ارزیابی و پایش کنند؛
۵. در نظام حقوقی داخلی نیز با بهره‌گیری از تجربیات اتحادیه اروپا، چارچوبی جامع و منسجم برای حمایت از داده‌های شخصی در بستر فناوری‌های نوین تدوین شود.

در نهایت، بایستی بیان کرد که آینده اینترنت اشیاء و مقبولیت اجتماعی آن، به میزان موفقیت در برقراری توازن میان نوآوری فناورانه و صیانت از کرامت و حقوق بنیادین اشخاص وابسته است. چارچوب ارائه‌شده در مقررات عمومی حفاظت از داده‌های اتحادیه اروپا الگویی پیشرو در این مسیر محسوب می‌شود، اما تحقق عملی این توازن مستلزم تعامل مستمر میان حقوق، فناوری و سیاست‌گذاری عمومی است. تنها با اتخاذ رویکردی پیشگیرانه، ساختاری و حقوق‌محور می‌توان اطمینان یافت که پیشرفت فناوری به بهای تضعیف حریم خصوصی و آزادی‌های فردی تمام نخواهد شد، بلکه در خدمت توسعه‌ای مسئولانه و انسان‌محور قرار خواهد گرفت.

فهرست منابع

آقایی طوق، مسلم؛ ناصر، مهدی(۱۳۹۹). چالش‌های حفاظت از داده‌های خصوصی در حوزه اینترنت اشیا: مطالعه تطبیقی حقوق ایران و اتحادیه اروپا، حقوق اداری، ۷(۲۳)، ۳۳-۵۵.

اقدسی، فاطمه؛ محقق داماد، مریم سادات(۱٤۰۰). ابعاد حقوقی حریم خصوصی در اینترنت اشیا، پژوهش‌های حقوقی میان رشته‌ای، ۲(۲)، ٤۹-٦۷.

ساکت، توحید(۱۳۹۸). امنیت اینترنت اشیا: نقش چالش‌ها و کاربردها، پژوهش در علوم رایانه، ٤(۱۳)، ۲۲-۳۲.

قناد، فاطمه؛ شریف، الهام(۱٤۰۰). مطالعه اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، حقوق فناوری‌های نوین، ۲(٤)، ۱-۲۲.

لطیف‌زاده، مهدیه؛ قبولی درافشان، سید محمدمهدی؛ محسنی، سعید؛ عابدی، محمد(۱٤۰۲). حمایت از داده شخصی در حقوق اتحادیه اروپا و امکان سنجی آن در نظام حقوقی ایران، مطالعات حقوق عمومی، ۵۳(۲)، ۹۸۱-۱۰۰۵.

معینی‌فر، محدثه؛ وحیدزاده، دل‌آرام(۱٤۰۱). الزامات استیفای حق بر حریم خصوصی در بستر اینترنت اشیاء از منظر حقوق ایران، حقوق فناوری‌های نوین، ۳(٦)، ٦۱-۷۵.

Babalola, O. (2021). Internet of Things (IoT): Data Security and Privacy Concerns under the General Data Protection Regulation (GDPR). Natural Language Processing. 309-320.

Babalola, O. (2021). Internet of Things (IoT): Data Security and Privacy Concerns under the General Data Protection Regulation (GDPR). Computer Science & Information Technology. 309-320.

Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009).

European Data Protection Board (EDPB). (2020). Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (Version 2.0).

European Parliament & Council of the European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, L 281, 31–50.

European Parliament & Council of the European Union. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Official Journal of the European Union, L 257, 73–114.

European Union. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Brussels: EU.

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.

Hadzovic, S., Mrdovic, S., Radonjic, M. (2021). Identification of IoT Actors. Sensors, 21, 2093.

International Telecommunication Union (ITU). (2012). Recommendation ITU-T Y.2060: Overview of the Internet of Things. Geneva: ITU.

Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press.

Luthfi, A., Minhar, E., (2022). Towards Privacy by Design on the Internet of Things (IoT) Use: A Qualitative Descriptive Study. Journal of Information Systems and Informatics. 4(2). 457-468.

Oktay, S., Heitmann, S., Kray, ch. (2024). Linking location privacy, digital sovereignty and location-based services: a Meta review. Journal of Location Based Services. 18(1). 1-52.

Pettorru, G., Pilloni, V., Martalo, M. (2024). Trustworthy Localization in IoT Networks: A Survey of Localization Techniques, Threats, and Mitigation. Sensors. 24. 2214.

Semantha, F., Azam, S., Yeo, Kh., Shanmugam, B. (2020). A Systematic Literature Review on Privacy by Design in the Healthcare Sector. Electronics. 9(3). 452.

Wazirali, R. (2022). A Review on Privacy Preservation of Location-Based Services in Internet of Things. Tech Science Press. 31(2). 767-779.