پژوهش‌نامه حقوق اسلامی

مقاله پژوهشی | دریافت: ۱۴۰۴/۱۱/۱۰ | پذیرش: ۱۴۰۵/۰۲/۲۱
DOI: 10.30497/law.2026.249866.3986

حریم خصوصی و تنظیم‌گری ریسک در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء: تحلیل سازوکارهای تقنینی اتحادیه اروپا و امکان‌سنجی اعمال آن در حقوق ایران

فاطمه نجیب‌زاده • دانشجوی دکتری فقه و مبانی حقوق اسلامی، دانشکده الهیات و معارف اسلامی، دانشگاه فردوسی مشهد، مشهد، ایران. fatemeh.najibzadeh@mail.um.ac.ir

سید محمدهادی قبولی درافشان • دانشیار، گروه فقه و مبانی حقوق اسلامی، دانشکده الهیات و معارف اسلامی، دانشگاه فردوسی مشهد، مشهد، ایران. (نویسنده مسئول) h.ghaboli@um.ac.ir

حسین ناصری مقدم • استاد، گروه فقه و مبانی حقوق اسلامی، دانشکده الهیات و معارف اسلامی، دانشگاه فردوسی مشهد، مشهد، ایران. naseri1962@um.ac.ir

چکیده

درهم‌تنیدگی هوش مصنوعی (AI) و اینترنت اشیاء (IoT)، حریم خصوصی را از قلمرو سنتی کنترل داده‌های شخصی به حوزه‌ای چندسطحی در تنظیم‌گری ریسک منتقل کرده است. در این اکوسیستم، داده‌های پیوسته، محیطی و رفتاری حاصل از ابزارهای متصل، از رهگذر تحلیل الگوریتمی، توصیه‌گری پلتفرمی، تصمیم‌گیری خودکار و آسیب‌پذیری امنیتی محصول، می‌توانند بر اختیار اطلاعاتی، حیثیت، عدم تبعیض، امنیت شخصی و امکان اعتراض مؤثر اشخاص اثر بگذارند. این مقاله با روش توصیفی تحلیلی و بر پایه مطالعه اسناد کتابخانه‌ای، سازوکارهای تقنینی اتحادیه اروپا را در مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری بررسی کرده و امکان کاربست منطق ریسک‌محور آن را در حقوق ایران می‌سنجد. داده‌های بخش ایران شامل قانون تجارت الکترونیکی، قانون جرائم رایانه‌ای، آیین‌نامه‌های ناظر بر خدمات اینترنتی، قواعد مسئولیت مدنی و قراردادی و نمونه‌هایی از رویه قضایی است. معیار تحلیل، ارزیابی کارکرد هر منبع در چهار سطح داده، پلتفرم، سامانه هوش مصنوعی و محصول متصل است. یافته‌های نوشتار نشان می‌دهد که کارآمدی الگوی اتحادیه اروپا در توزیع ریسک میان محل‌های متفاوت پیدایش آن و تبدیل هر سطح به تکالیف مشخص، پیشینی و قابل نظارت است: مشروعیت و پاسخ‌گویی در پردازش داده، شفافیت و مدیریت ریسک‌های پلتفرمی، کنترل سامانه‌های پرخطر و امنیت چرخه عمر محصول. در حقوق ایران، ظرفیت‌های موجود عمدتاً به حمایت محدود داده‌ای در روابط الکترونیکی، واکنش کیفری نسبت به تعرض‌های منصوص، کنترل اداری رفتار زیرساختی و جبران خسارت محدود می‌شود. ازاین‌رو، کارآمدسازی حمایت از حریم خصوصی مستلزم بازآرایی قواعد بر اساس محل پیدایش ریسک است، نه اقتباس لفظی از مقررات اروپایی یا توسعه تفسیری قوانین موجود.

واژگان کلیدی: هوش مصنوعی، اینترنت اشیاء، حریم خصوصی، تنظیم‌گری ریسک‌محور.

مقدمه

گسترش هم‌زمان هوش مصنوعی و اینترنت اشیاء، حریم خصوصی را از قلمرو سنتی صیانت از اطلاعات محرمانه یا منع افشای داده‌های شخصی فراتر برده و آن را به مسئله‌ای چندلایه در تنظیم‌گری ریسک تبدیل کرده است. در اکوسیستم‌های متصل، داده‌ها غالباً به‌صورت پیوسته، محیط محور، رفتاری و چندمنبعی تولید می‌شوند؛ از خانه هوشمند، ابزارهای پوشیدنی سلامت و خودروهای متصل گرفته تا زیرساخت‌های شهری، خدمات پلتفرمی و سامانه‌های تصمیم یار. اهمیت حقوقی این داده‌ها در امکان ترکیب، تحلیل، استنباط ویژگی‌های حساس، تصمیم‌گیری خودکار، بازنشر پلتفرمی و بهره‌برداری از آسیب‌پذیری‌های فنی محصول نهفته است. در چنین فضایی، نقض حریم خصوصی الزاماً به شکل افشای آشکار اطلاعات رخ نمی‌دهد، بلکه می‌تواند در قالب پروفایل‌سازی رفتاری، تصمیم الگوریتمی نامتناسب، کاهش امکان اعتراض مؤثر، تنظیم نامحسوس محیط دیجیتال یا ضعف امنیتی محصول متصل ظاهر شود. ازاین‌رو، حمایت حقوقی از حریم خصوصی در این حوزه، نیازمند چارچوبی است که بتواند ریسک را نه به‌صورت کلی و انتزاعی، بلکه در محل پیدایش آن شناسایی کند.

اتحادیه اروپا در سال‌های اخیر، برای مواجهه با ریسک‌های حریم خصوصی در محیط‌های هوشمند متصل، به یک قانون واحد اکتفا نکرده و چند متن تقنینی مکمل را در کنار یکدیگر به کار گرفته است. مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری، هر یک‌بخشی از مسئله را پوشش می‌دهند: پردازش داده‌های شخصی، رفتار پلتفرم‌ها، توسعه و به‌کارگیری سامانه‌های هوش مصنوعی، و امنیت محصولات متصل. در این مقاله، حقوق ایران از منظر امکان‌سنجی کارکردی بررسی می‌شود؛ به این معنا که قانون تجارت الکترونیکی، قانون جرائم رایانه‌ای، آیین‌نامه‌های خدمات اینترنتی و قواعد مسئولیت مدنی و قراردادی، بر اساس ظرفیت واقعی خود در مواجهه با ریسک‌های داده‌ای، پلتفرمی، سامانه‌ای و محصول‌محور ارزیابی می‌شوند.

در ادبیات داخلی، بخشی از پژوهش‌ها به نسبت هوش مصنوعی، حریم خصوصی و مسئولیت پرداخته‌اند. برای نمونه، مرتضوی و خدائی‌فام در پژوهش خود درباره آثار به‌کارگیری هوش مصنوعی بر حریم خصوصی و مسئولیت مدنی، به‌ویژه در زمینه تبلیغات هدفمند، برخی چالش‌های داده‌محور و مسئولیت ناشی از پردازش الگوریتمی را بررسی کرده‌اند. ظفریان و همکاران نیز در مقاله «حفظ حریم خصوصی در فنّاوری‌های مبتنی بر هوش مصنوعی» بر ضرورت تدوین چارچوب‌های حقوقی و اخلاقی برای حمایت از داده‌های شخصی در برابر فناوری‌های هوشمند تأکید کرده‌اند. همچنین موسوی در پژوهش «تحلیل حقوقی حریم خصوصی در فضای مجازی: چالش‌های رضایت و مسئولیت مدنی در عصر هوش مصنوعی» مسئله رضایت، مسئولیت مدنی و فناوری‌هایی مانند دیپ‌فیک را در فضای مجازی برجسته ساخته است. باوجود اهمیت این آثار، تمرکز غالب آن‌ها بر سطح داده، مسئولیت مدنی، رضایت یا برخی کاربردهای خاص هوش مصنوعی است و کمتر به تحلیل ساختارمند نسبت میان حریم خصوصی و تنظیم‌گری ریسک در اکوسیستم ترکیبی هوش مصنوعی و اینترنت اشیاء پرداخته‌اند.

وجه تمایز پژوهش حاضر در همین نقطه قرار دارد. این مقاله حریم خصوصی را صرفاً ذیل حمایت از داده‌های شخصی یا مسئولیت ناشی از نقض آن بررسی نمی‌کند، بلکه آن را در یک چارچوب چهارسطحی مطالعه می‌کند: داده، پلتفرم، سامانه هوش مصنوعی و محصول متصل. براین‌اساس، نوآوری مقاله در سه امر قابل‌بیان است: نخست، صورت‌بندی حریم خصوصی در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء بر پایه منطق ریسک‌محور و نه صرفاً بر پایه مفهوم داده شخصی؛ دوم، تحلیل سازوکارهای تقنینی اتحادیه اروپا به‌عنوان معماری چندلایه‌ای که در آن هر مقرره بخشی متفاوت از زنجیره تولید ریسک را پوشش می‌دهد؛ و سوم، امکان‌سنجی اعمال این منطق در حقوق ایران باهدف شناسایی ظرفیت‌ها، حدود تفسیری و خلأهای تقنینی قوانین موجود ایران در هر یک از سطوح چهارگانه.

بر این مبنا، پرسش اصلی پژوهش آن است که الگوی ریسک‌محور اتحادیه اروپا در حوزه حریم خصوصی مرتبط با هوش مصنوعی و اینترنت اشیاء، چگونه میان سطوح داده، پلتفرم، سامانه هوش مصنوعی و محصول متصل توزیع شده و چه ظرفیت‌هایی برای امکان‌سنجی کارکردی آن در حقوق ایران وجود دارد؟ در ذیل این پرسش اصلی، چند پرسش فرعی نیز مطرح می‌شود: نخست، هر یک از مقررات اصلی اتحادیه اروپا، یعنی مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری، کدام نوع ریسک حریم خصوصی را هدف قرار می‌دهند و چه نوع تکالیفی را بر بازیگران مربوط تحمیل می‌کنند؟ دوم، قوانین و مقررات موجود ایران، از جمله قانون تجارت الکترونیکی، قانون جرائم رایانه‌ای، آیین‌نامه‌های خدمات اینترنتی و قواعد مسئولیت مدنی و قراردادی، در کدام یک از سطوح چهارگانه قابلیت کاربست دارند؟ سوم، حدود این کاربست در حقوق ایران چیست و در چه مواردی توسعه تفسیری با موانعی مانند قلمرو خاص قانون تجارت الکترونیکی، اصل قانونی‌بودن جرم و مجازات، منع تفسیر موسع کیفری یا فقدان قواعد پلتفرمی، سامانه‌ای و محصول‌محور روبه‌رو می‌شود؟ چهارم، باتوجه‌به این ظرفیت‌ها و محدودیت‌ها، چه مسیرهایی برای بازآرایی تفسیری و تقنینی حقوق ایران در راستای حمایت مؤثرتر از حریم خصوصی در محیط‌های هوشمند متصل قابل‌طرح است؟

روش پژوهش حاضر از حیث ماهیت، توصیفی – تحلیلی و از حیث رویکرد، امکان‌سنجی تقنینی و تطبیقی کارکردی است. داده‌های پژوهش از طریق مطالعه اسنادی گردآوری شده و شامل متون تقنینی اتحادیه اروپا در حوزه حفاظت از داده، خدمات دیجیتال، هوش مصنوعی و تاب‌آوری سایبری، ادبیات تخصصی مرتبط، نمونه‌های منتخب از رویه قضایی، و نیز قوانین و مقررات ایران در زمینه تجارت الکترونیکی، جرائم رایانه‌ای، خدمات اینترنتی و مسئولیت مدنی و قراردادی است. معیار تحلیل، مقایسه صوری یا همسنگ‌سازی کامل دو نظام نیست؛ بلکه سنجش کارکرد هر متن در نسبت با چهار سطح داده، پلتفرم، سامانه و محصول متصل است. بر همین اساس، مقاله ابتدا ساختار ریسک‌محور اتحادیه اروپا را تبیین می‌کند، سپس ظرفیت و حدود اعمال این منطق را در حقوق ایران می‌سنجد و در نهایت، مسیرهای تفسیری و تقنینی مناسب برای سامان‌دهی منسجم‌تر حمایت از حریم خصوصی در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء را طرح می‌کند.

۱. سازوکار تقنینی اتحادیه اروپا

۱.۱. ساختار هنجاری

نظام تقنینی اتحادیه اروپا در فضای دیجیتال، به‌ویژه در پیوند هوش مصنوعی و اینترنت اشیاء، بر قانون واحدی استوار نیست؛ بلکه از مجموعه‌ای از مقررات تشکیل شده که هر یک‌بخشی از مسئله اعتماد، امنیت و حریم خصوصی را پوشش می‌دهند. در این میان، مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری، چهار سطح اصلی حکمرانی دیجیتال را سامان می‌دهند: سطح داده، پلتفرم، سامانه هوش مصنوعی و محصول متصل. از این منظر، «قابل‌اعتماد بودن» سامانه‌های الگوریتمی در حقوق اتحادیه، حاصل توزیع تکالیف میان مقرراتی است که به‌ترتیب از زاویه حفاظت از داده‌های شخصی، تنظیم رفتار پلتفرم‌ها، کنترل سامانه‌های هوش مصنوعی و تضمین امنیت سایبری محصولات دیجیتال به موضوع می‌نگرند (Graux et al., 2025, p. 18).

بااین‌حال، این چهار مقرره از حیث موضوع، مخاطب، ابزارهای انطباق و نهادهای ناظر یکسان نیستند. مقرره عمومی حفاظت از داده‌ها بر پردازش داده‌های شخصی و حمایت از حقوق بنیادین تمرکز دارد؛ مقرره خدمات دیجیتال، رفتار خدمات واسطه‌ای و پلتفرم‌های برخط را در زمینه‌هایی مانند تعدیل محتوا، سامانه‌های توصیه‌گر و تبلیغات هدفمند تنظیم می‌کند؛ قانون هوش مصنوعی به طبقه‌بندی و کنترل سامانه‌های هوش مصنوعی در مراحل طراحی، عرضه و بهره‌برداری می‌پردازد؛ و مقرره تاب‌آوری سایبری، امنیت محصولات دارای عناصر دیجیتال را از حیث طراحی ایمن، مدیریت آسیب‌پذیری و نظارت بازار دنبال می‌کند؛ بنابراین، نسبت این مقررات را باید هم از منظر تکمیل‌کنندگی و هم از منظر تفاوت‌های اجرایی و نهادی فهمید؛ زیرا هماهنگی میان آن‌ها همواره ساده و بی‌چالش نیست.

بر همین اساس، این پژوهش ساختار هنجاری اتحادیه اروپا را در چهار سطح تحلیل می‌کند. در سطح داده، شاخص‌هایی مانند مشروعیت پردازش، شفافیت، محدودیت هدف، کمینه‌سازی، امنیت پردازش، ارزیابی تأثیر بر حفاظت از داده و حقوق اشخاص اهمیت دارد. در سطح پلتفرم، شفافیت سامانه‌های توصیه‌گر، محدودیت هدف‌گیری تبلیغاتی، ارزیابی و کاهش ریسک‌های نظام‌مند، امکان اعتراض کاربران و دسترسی پژوهشگران واجد شرایط به داده‌های پلتفرم محور تحلیل است. در سطح سامانه هوش مصنوعی، معیارهایی چون طبقه‌بندی ریسک، حاکمیت داده، مستندسازی فنی، نظارت انسانی، دقت، استحکام، امنیت سایبری و ارزیابی اثر بر حقوق بنیادین مطرح می‌شود. در سطح محصول متصل نیز امنیت در طراحی، امنیت پیش‌فرض، مدیریت آسیب‌پذیری، به‌روزرسانی امنیتی، ارزیابی انطباق و نظارت بازار شاخص‌های اصلی‌اند. بدین ترتیب، مفهوم ریسک نه به‌صورت کلی، بلکه در پیوند با تعهدات مشخص هر سطح بررسی می‌شود.

بر این مبنا، تمرکز پژوهش بر آن است که هر مقرره از چه زاویه‌ای به ریسک می‌نگرد، چه تکالیفی را بر چه بازیگرانی تحمیل می‌کند و در کدام نقاط، میان منطق داده‌محور، پلتفرمی، سامانه‌ای و محصول‌محور اتحادیه اروپا امکان هم‌افزایی یا تنش اجرایی پدید می‌آید.

۱.۱.۱. تعاریف و مفاهیم مقدماتی

در ادبیات فنی، «قابل‌اعتماد بودن» به وضعیتی اشاره دارد که در آن سامانه بتواند محرمانگی، یکپارچگی، دسترس‌پذیری و حریم خصوصی را در سطح قابل‌قبول تضمین کند و در برابر اختلال، خطا و حمله تاب‌آور باشد (NIST, 2018, p. 32; Belanger et al., 2002, p. 245; Zhang & Gupta, 2018, p. 914; Liu et al., 2022; Li et al., 2023, p. 4). این برداشت در حقوق اتحادیه اروپا به‌صورت تعریف واحد و صریح وارد نشده، بلکه در قالب تکالیف متفاوت کنترل‌کنندگان داده، ارائه‌دهندگان خدمات پلتفرمی، عرضه‌کنندگان سامانه‌های هوش مصنوعی و تولیدکنندگان محصولات دارای عناصر دیجیتال بازتاب یافته است.

در این چارچوب، «قابلیت اعتماد» نه مفهومی صرفاً اخلاقی است و نه در اسناد اتحادیه معنای حقوقی کاملاً واحدی دارد؛ بلکه از ترکیب مؤلفه‌هایی مانند امنیت سایبری، حمایت از داده‌های شخصی، شفافیت، قابلیت توضیح، عدالت الگوریتمی، پاسخ‌گویی و ایمنی شکل می‌گیرد. امنیت سایبری در مقرره امنیت سایبری به مجموعه تدابیری برای حفاظت از شبکه‌ها، سامانه‌های اطلاعاتی و کاربران در برابر رویدادهای آسیب‌زا یا مختل‌کننده اشاره دارد (Regulation (EU) 2019/881, 2019). در کنار آن، مقرره عمومی حفاظت از داده‌ها با اصولی مانند مشروعیت، انصاف، شفافیت، محدودیت هدف، کمینه‌سازی، دقت، محدودیت نگهداری، یکپارچگی، محرمانگی و پاسخ‌گویی، حمایت از داده شخصی را به یکی از پایه‌های اعتماد در محیط دیجیتال تبدیل کرده است (Regulation (EU) 2016/679, 2016).

بااین‌حال، اعتماد الگوریتمی در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء فقط به امنیت و حریم خصوصی محدود نمی‌شود. عدالت الگوریتمی به پیشگیری از آثار تبعیض‌آمیز، شفافیت و قابلیت توضیح به فهم منطق تصمیم یا توصیه، پاسخ‌گویی به انتساب روشن تکالیف در زنجیره طراحی، عرضه و بهره‌برداری، و ایمنی به پیشگیری از آسیب‌های ناشی از خطا، نقص یا کاربرد قابل‌پیش‌بینی سامانه مربوط است (Beltrán, 2025, p. 2; Regulation (EU) 2019/881, 2019, p. 15)؛ بنابراین، اعتماد در این حوزه هم‌زمان جنبه فنی، حقوقی و نهادی دارد.

مفهومی که این مؤلفه‌ها را به تکالیف اجرایی پیوند می‌دهد، «ریسک» است. در معنای پایه، ریسک به نسبت میان احتمال وقوع تهدید و شدت آسیب احتمالی اشاره دارد و با مفاهیمی چون تهدید، آسیب و آسیب‌پذیری توضیح داده می‌شود (Reichman & Sartor, 2022, p. 131; Bagni & Seferi, 2025, p. 132). تهدید، وضعیت یا رویدادی است که می‌تواند بر سامانه، عملیات، دارایی‌های سازمانی، اشخاص یا جامعه اثر نامطلوب بگذارد و در حوزه هوش مصنوعی، افزون بر حملات کلاسیک سایبری، نقص مدل، آلوده‌سازی داده و حملات مقابله‌ای را نیز در بر می‌گیرد (European Parliament and Council of the European Union, 2019). آسیب نیز اثر بالفعل یا بالقوه نامطلوب بر فرد، گروه یا جامعه است؛ از زیان جسمی و اقتصادی تا لطمه به‌سلامت روانی، تبعیض، نقض حریم خصوصی و تضعیف اعتماد عمومی (Liu et al., 2022, p. 5).

در این میان، آسیب‌پذیری نقطه‌ای است که از طریق آن تهدید می‌تواند به آسیب منتهی شود. در مقرره تاب‌آوری سایبری، آسیب‌پذیری به ضعف یا نقصی در محصول دارای عناصر دیجیتال گفته می‌شود که امکان بهره‌برداری توسط تهدید را فراهم می‌کند (Regulation (EU) 2024/2847, 2024). بااین‌حال، در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء، آسیب‌پذیری فقط نقص نرم‌افزاری یا ضعف امنیتی محصول نیست؛ کیفیت داده‌های آموزشی، سوگیری مدل، شیوه اتصال، وابستگی به پردازش ابری، طراحی رابط کاربر و الگوی گردآوری پیوسته داده نیز می‌توانند زمینه‌ساز آسیب باشند. ازاین‌رو، ممکن است یک دستگاه متصل از نظر فنی ایمن باشد، اما به دلیل گردآوری بیش از حد داده، استنباط ویژگی‌های حساس یا نبود کنترل مؤثر برای کاربر، همچنان از منظر حریم خصوصی و حقوق بنیادین پرریسک تلقی شود.

بر همین مبنا، ریسک در هر سطح از ساختار حقوقی اتحادیه معنای خاصی می‌یابد. در مقرره عمومی حفاظت از داده‌ها، ریسک عمدتاً به حقوق و آزادی‌های اشخاص در فرایند پردازش داده مربوط است. در مقرره خدمات دیجیتال، ریسک به آثار گسترده خدمات پلتفرمی بر کاربران، گفتمان عمومی، سلامت عمومی و فرایندهای دموکراتیک پیوند می‌خورد. در قانون هوش مصنوعی، ریسک مبنای طبقه‌بندی سامانه‌ها و تعیین شدت تکالیف در نسبت با سلامت، ایمنی و حقوق بنیادین است (Regulation (EU) 2024/1689, 2024). در مقرره تاب‌آوری سایبری نیز ریسک به امنیت محصول، امکان بهره‌برداری از آسیب‌پذیری‌ها و پیامدهای آن برای مصرف‌کنندگان، کسب‌وکارها و زیرساخت‌ها مربوط می‌شود (Regulation (EU) 2024/2847, 2024)؛ بنابراین، استفاده مشترک این مقررات از زبان ریسک به معنای وحدت منطق آن‌ها نیست؛ هر مقرره، ریسک را از زاویه موضوع، مخاطب و هدف خود تعریف و مدیریت می‌کند.

نتیجه آن است که ساختار هنجاری اتحادیه اروپا در حوزه هوش مصنوعی و اینترنت اشیاء، در عین جهت‌گیری مشترک به‌سوی پیشگیری از آسیب و تقویت پاسخ‌گویی، از حیث موضوع، ابزار اجرایی و نهاد ناظر همسان نیست. این وضعیت از یک‌سو امکان می‌دهد حریم خصوصی و اعتماد الگوریتمی در چهار سطح داده، پلتفرم، سامانه و محصول دنبال شود و ازسوی‌دیگر، احتمال هم‌پوشانی، اختلاف اجرایی و ابهام در تقسیم مسئولیت را افزایش می‌دهد. ازاین‌رو، بررسی جداگانه هر مقرره در ادامه، برای روشن‌کردن تکالیف مشخص، ظرفیت‌های مکمل و نقاط تنش میان آن‌ها ضروری است.

۲.۱.۱. مقرره عمومی حفاظت از داده‌ها[1]

مقرره عمومی حفاظت از داده‌ها نقطه آغاز سنجش حقوقی در سطح «داده» در نظام تقنینی اتحادیه اروپا است. این مقرره، همه صور «پردازش» داده شخصی، از گردآوری و ذخیره‌سازی تا تحلیل، پروفایل‌سازی و حذف را ذیل هدف کلان «حمایت از حقوق و آزادی‌های بنیادین اشخاص حقیقی» تنظیم می‌کند (Regulation (EU) 2016/679, 2016). اهمیت این مقرره در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء از آن روست که بسیاری از کارکردهای این سامانه‌ها، حتی زمانی که در

1. General Data Protection Regulation (GDPR).

ظاهر به تصمیم فنی یا بهینه‌سازی خدمات مربوط‌اند، در واقع بر جریان مداوم داده‌های شخصی، محیطی و رفتاری استوارند .ازاین‌رو، در سطح داده، پرسش اصلی فقط این نیست که داده گردآوری شده یا نه؛ بلکه این است که گردآوری، تحلیل و استفاده بعدی از داده بر چه مبنای مشروعی انجام می‌شود، تا چه حد برای هدف اعلام‌شده ضرورت دارد، چه میزان برای شخص قابل‌فهم است و چه تضمینی برای کنترل آثار آن وجود دارد .براین‌اساس، اصول ماده ۵ صرفاً قواعد عمومی مدیریت داده نیستند، بلکه معیارهای اصلی سنجش کیفیت حقوقی پردازش‌های الگوریتمی متکی بر داده شخصی به شمار می‌آیند؛ به‌ویژه از حیث مشروعیت، انصاف، شفافیت، محدودیت هدف، کمینه‌سازی داده، دقت، محدودیت نگهداری، امنیت و پاسخ‌گویی.

ساختار این مقرره به طور روشن با منطق ریسک پیوند دارد. کنترل‌کننده باید با لحاظ ماهیت، دامنه، بستر و اهداف پردازش و نیز احتمال و شدت ریسک برای حقوق و آزادی‌های اشخاص، تدابیر فنی و سازمانی متناسب اتخاذ کند و بتواند انطباق خود را اثبات نماید (ماده ۲۴) .در اینجا ریسک، صرفاً خطر فنی نقض امنیت یا افشای داده نیست؛ بلکه شامل پیامدهای احتمالی پردازش بر اختیار اطلاعاتی، حیثیت، آزادی انتخاب، عدم تبعیض و امکان اعتراض مؤثر اشخاص نیز می‌شود (Gellert, 2018, p. 281). این منطق در «حفاظت از داده با طراحی و به‌صورت پیش‌فرض» دقیق‌تر می‌شود؛ بدین معنا که ملاحظات حریم خصوصی و کمینه‌سازی داده باید از مرحله انتخاب ساختار فنی سامانه، تعیین داده‌های لازم، مدت نگهداری، حدود دسترسی و تنظیمات پیش‌فرض کاربر در طراحی لحاظ شود، نه آنکه پس از استقرار سامانه به‌صورت تدبیری تکمیلی افزوده گردد (Naudts et al., 2025, p. 281)؛ بنابراین، ماده ۲۵ مقرره، نقطه اتصال میان طراحی فنی و مسئولیت حقوقی است: سامانه‌ای که بیش از نیاز داده گردآوری می‌کند، امکان کنترل واقعی برای کاربر فراهم نمی‌سازد یا تنظیمات پیش‌فرض آن به نفع پردازش گسترده‌تر داده طراحی شده است، حتی پیش از وقوع نقض امنیتی نیز می‌تواند از منظر حریم خصوصی مسئله‌ساز باشد.

همین منطق در حوزه امنیت پردازش نیز ادامه می‌یابد. کنترل‌کننده و پردازشگر مکلف‌اند متناسب با ریسک و باتوجه‌به استانداردهای فنی روزآمد، سطحی از امنیت را تأمین کنند که احتمال و شدت نقض محرمانگی، یکپارچگی و دسترس‌پذیری را کاهش دهد (ماده ۳۲) .در محیط‌های مبتنی بر اینترنت اشیاء، این تکلیف اهمیت مضاعف دارد؛ زیرا ضعف امنیتی در یک حسگر، ابزار پوشیدنی، دستیار خانگی یا سامانه متصل، فقط به دسترسی غیرمجاز به یک پایگاه‌داده محدود نمی‌شود، بلکه

می‌تواند به بازسازی الگوهای زیست، سلامت، حضور، رفتار مصرفی یا روابط خانوادگی کاربر بینجامد .به همین دلیل، امنیت در مقرره عمومی حفاظت از داده‌ها در کنار محرمانگی، به تمامیت و دسترس‌پذیری داده نیز توجه دارد و همین امر آن را از یک قاعده صرفاً فنی به تضمینی برای حمایت از حقوق اشخاص تبدیل می‌کند.

هرگاه نوع، دامنه، بستر یا اهداف پردازش احتمالاً «ریسک بالایی» برای حقوق و آزادی‌های اشخاص ایجاد کند، سازوکار «ارزیابی تأثیر حفاظت از داده‌ها» پیش‌بینی شده است (ماده ۳۵). این ارزیابی مهم‌ترین ابزار مقرره برای تبدیل زبان ریسک به تصمیم حقوقی قابل مستندسازی است؛ زیرا کنترل‌کننده را ملزم می‌کند پیش از آغاز پردازش، ماهیت عملیات، ضرورت و تناسب آن، ریسک‌های خاص و تدابیر کاهش‌دهنده را بررسی و ثبت کند .در سامانه‌های هوش مصنوعی و اینترنت اشیاء، جایگاه این ارزیابی زمانی برجسته‌تر می‌شود که داده‌های ظاهراً عادی، مانند داده‌های مکانی، حرکتی، صوتی یا مصرف انرژی، در اثر ترکیب و تحلیل الگوریتمی به استنباط‌های حساس درباره سلامت، عادات شخصی، وضعیت خانوادگی یا گرایش‌های رفتاری منتهی شوند؛ مسئله‌ای که با گستردگی مفهوم «داده شخصی» در حقوق اتحادیه اروپا ارتباط مستقیم دارد (Purtova, 2018, p.45). ازاین‌جهت، ارزیابی تأثیر حفاظت از داده‌ها فقط یک تشریفات اداری نیست؛ بلکه معیاری برای سنجش این است که پردازش داده تا چه اندازه پیش از اجرا، از منظر ضرورت، تناسب، شفافیت و آثار احتمالی بر اشخاص مهار شده است.

در نهایت، مقرره با ایجاد سطحی از پاسخ‌گویی نهادی و توزیع نقش‌ها، اجرای این تکالیف را صرفاً به تصمیم داخلی کنترل‌کننده واگذار نمی‌کند. کنترل‌کننده در مرکز قرار دارد، اما پردازشگران، کنترل‌کنندگان مشترک و نمایندگان نیز تعهدات مشخص دارند و مراجع حفاظت از داده در دولت‌های عضو، با هماهنگی کارگروه حفاظت از داده‌ها، بر اجرای آن نظارت می‌کنند (van Mil & Quintais, 2022, p. 3). این توزیع نقش‌ها در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء اهمیت ویژه دارد؛ زیرا داده ممکن است میان تولیدکننده دستگاه، ارائه‌دهنده نرم‌افزار، پلتفرم ابری، توسعه‌دهنده مدل و بهره‌بردار نهایی گردش کند و در هر مرحله، خطر جابه‌جایی یا کم‌رنگ شدن مسئولیت وجود داشته باشد؛ بنابراین، در سطح داده، هر سامانه هوش مصنوعی یا زیرساخت اینترنت اشیاء مبتنی بر داده شخصی، پیش از آنکه از منظر پلتفرم، سامانه یا محصول متصل ارزیابی شود، باید با معیارهای بنیادین این مقرره درباره مشروعیت پردازش، کمینه‌سازی داده، امنیت، ارزیابی اثر و پاسخ‌گویی

قابل‌اثبات منطبق باشد.

۳.۱.۱. مقرره خدمات دیجیتال[1]

مقرره خدمات دیجیتال، سطح «پلتفرم» را در نظام تقنینی اتحادیه اروپا سامان می‌دهد. موضوع اصلی این مقرره، برخلاف مقرره عمومی حفاظت از داده‌ها، مشروعیت پردازش داده شخصی نیست؛ بلکه نحوه اعمال قدرت پلتفرم‌ها در سازمان‌دهی دسترسی کاربران به محتوا، کالا و خدمات است. پلتفرم‌ها در محیط دیجیتال صرفاً واسطه‌های فنی نیستند؛ آن‌ها از طریق رتبه‌بندی، توصیه، حذف، محدودسازی، تبلیغ و اولویت‌بندی محتوا، بر دیده‌شدن اشخاص، شکل‌گیری انتخاب‌ها و جهت‌گیری فضای عمومی اثر می‌گذارند(Gorwa et al., 2020, pp. 2-3) ؛ **بنابراین**، مسئله اصلی در مقرره خدمات دیجیتال این نیست که پلتفرم چه داده‌ای را بر چه مبنایی پردازش می‌کند؛ بلکه این است که چگونه میدان دسترسی، توجه و انتخاب کاربران را سامان می‌دهد. ازاین‌رو، اعتماد در این سطح با شفافیت تصمیم‌های پلتفرمی، امکان اعتراض، محدودیت هدف‌گیری تبلیغاتی، ارزیابی ریسک‌های نظام‌مند و نظارت بیرونی سنجیده می‌شود (Regulation (EU) 2022/2065 (Digital Services Act), 2022).

مقرره خدمات دیجیتال با تفکیک میان خدمات واسطه‌ای، خدمات میزبانی، پلتفرم‌های برخط و سپس «پلتفرم‌های بسیار بزرگ برخط» و «موتورهای جست‌وجوی بسیار بزرگ»، میان شدت اثرگذاری بازیگران مختلف تفاوت می‌گذارد. تعهدات سنگین‌تر برای پلتفرم‌ها و موتورهای جست‌وجوی بسیار بزرگ ازآن‌جهت مقرر شده است که این بازیگران، به سبب شمار گسترده کاربران و نقش مؤثر در دسترسی عمومی به اطلاعات، می‌توانند آثاری فراتر از رابطه قراردادی با کاربر ایجاد کنند(Söderlund et al., 2024, p. 3; Strowel & De Meyere, 2023, p. 70) ؛ **بنابراین**، معیار مداخله حقوقی در این مقرره، صرف فعالیت اقتصادی پلتفرم یا صرف استفاده از الگوریتم نیست؛ بلکه ترکیب مقیاس، قدرت واسطه‌گری و ظرفیت اثرگذاری جمعی است. هرچه پلتفرم در شکل‌دادن به دسترسی عمومی، بازار توجه و جریان اطلاعات نقش گسترده‌تری داشته باشد، تکالیف آن نیز از الزامات عادی خدمات واسطه‌ای فراتر می‌رود.

---

1. Digital Services Act (DSA).

نخستین محور این مسئولیت، شفافیت در تصمیم‌های پلتفرمی است. پلتفرم باید درباره تعدیل محتوا، دلایل محدودسازی یا حذف محتوا، تبلیغات و کارکرد سامانه‌های توصیه‌گر اطلاعات قابل‌فهم ارائه کند. این تکالیف در مواد ۱۵، ۱۷، ۲۴، ۲۶ و ۲۷ دیده می‌شود و هدف آن‌ها کاهش وضعیت نابرابر میان پلتفرم و کاربر است؛ وضعیتی که در آن کاربر معمولاً نمی‌داند چرا محتوایی حذف شده، چرا محتوایی به او پیشنهاد شده، یا چرا تبلیغ خاصی در معرض دید او قرار گرفته است. از این منظر، شفافیت در مقرره خدمات دیجیتال فقط ابزار اطلاع‌رسانی نیست؛ بلکه پیش‌شرط امکان اعتراض، پاسخ‌خواهی و کنترل بیرونی بر تصمیم‌هایی است که دسترسی کاربر به محتوا یا میزان دیده‌شدن او را تغییر می‌دهد(Leerssen, 2023, p. 3) ؛ **بنابراین**، شفافیت پلتفرمی در این مقرره به معنای آشکارکردن «نقطه اثر» تصمیم الگوریتمی است؛ یعنی جایی که توصیه، رتبه‌بندی، حذف یا تبلیغ، تجربه واقعی کاربر از محیط دیجیتال را شکل می‌دهد.

محور دوم، سامانه‌های توصیه‌گر و تبلیغات هدفمند است. پلتفرم‌ها باید عامل‌های اصلی سامانه‌های توصیه‌گر و اثر آن‌ها بر نمایش محتوا را برای کاربران توضیح دهند و دست‌کم یک گزینه جایگزین ارائه کنند که بر پروفایل‌سازی رفتاری متکی نباشد .(Naudts et al., 2025, p. 270) اهمیت این حکم در آن است که کاربر را فقط صاحب داده نمی‌بیند، بلکه او را مخاطب محیطی الگوریتمی می‌داند که می‌تواند توجه، ترجیح و انتخاب او را شکل دهد. همچنین محدودیت‌های مربوط به تبلیغات هدفمند، به‌ویژه درباره داده‌های حساس و حمایت از کودکان، نشان می‌دهد که مقرره خدمات دیجیتال تبلیغ را صرفاً ابزار تجاری نمی‌داند؛ بلکه آن را یکی از مسیرهای اثرگذاری پلتفرم بر رفتار و آسیب‌پذیری کاربران تلقی می‌کند. در نتیجه، سنجه اصلی در این قسمت، صرف وجود رضایت یا اطلاع‌رسانی نیست؛ بلکه میزان اختیار واقعی کاربر در برابر شخصی‌سازی پیش‌فرض و امکان خروج از الگوی تحمیلی توصیه و تبلیغ است.

محور سوم، ارزیابی و کاهش ریسک‌های نظام‌مند است. پلتفرم‌ها و موتورهای جست‌وجوی بسیار بزرگ باید به طور منظم ریسک‌هایی را ارزیابی کنند که از طراحی، کارکرد یا استفاده از خدمات آنان پدید می‌آید؛ از جمله انتشار محتوای غیرقانونی، آثار منفی بر حقوق بنیادین، فرایندهای انتخاباتی، سلامت عمومی، امنیت عمومی، حمایت از کودکان، خشونت مبتنی بر جنسیت و سلامت جسمی و روانی کاربران. سپس باید متناسب با این ریسک‌ها، تدابیر معقول، مؤثر و متناسب برای کاهش آسیب طراحی و اجرا کنند (مواد ۳۴ و ۳۵؛ Naudts et al., 2025, p. 274.) اهمیت این بخش در آن است که مقرره خدمات دیجیتال از منطق نقض منفرد عبور می‌کند و به اثر تجمعی تصمیم‌های پلتفرمی توجه دارد: رتبه‌بندی، توصیه، تبلیغ یا تعدیل محتوا ممکن است در یک مورد خاص کم‌اهمیت باشد، اما در مقیاس میلیون‌ها کاربر می‌تواند به قطبی‌سازی، گسترش اطلاعات زیان‌آور، تبعیض، آسیب به کودکان یا تضعیف اعتماد عمومی منتهی شود. به همین دلیل، «ریسک نظام‌مند» در این مقرره، معیاری برای سنجش اثر اجتماعی طراحی و بهره‌برداری از پلتفرم است، نه صرفاً خطای فنی یا نقض موردی.(Griffin, 2025, pp. 227–229)

محور چهارم، پاسخ‌گویی بیرونی است. مقرره خدمات دیجیتال به گزارش‌دهی داخلی پلتفرم اکتفا نمی‌کند و برای پلتفرم‌ها و موتورهای جست‌وجوی بسیار بزرگ، ممیزی مستقل، نظارت کمیسیون و دسترسی پژوهشگران واجد شرایط به داده‌های پلتفرم را پیش‌بینی می‌کند (مواد ۳۷ و ۴۰). دسترسی پژوهشگران به داده‌ها ازآن‌جهت مهم است که بخش بزرگی از ریسک‌های پلتفرمی از بیرون کاملاً قابل‌مشاهده نیست و بدون داده‌های معتبر، ارزیابی ادعاهای پلتفرم درباره کاهش آسیب دشوار خواهد بود .(Liesenfeld, 2025, pp. 537–538) در اینجا مقرره خدمات دیجیتال از پاسخ‌گویی صرفاً اعلامی فاصله می‌گیرد و آن را به قابلیت آزمون‌پذیری تبدیل می‌کند؛ یعنی پلتفرم باید امکان سنجش مستقل آثار خدمات خود را فراهم آورد؛ بنابراین، پاسخ‌گویی در سطح پلتفرم فقط به معنای سیاست داخلی یا گزارش شفافیت نیست؛ بلکه مستلزم بررسی مستقل، پژوهش بیرونی و نظارت نهادی است.

براین‌اساس، مقرره خدمات دیجیتال جایگاه مستقلی در حکمرانی دیجیتال اتحادیه دارد. این مقرره با مقرره عمومی حفاظت از داده‌ها هم‌پوشانی‌هایی دارد، اما موضوع آن همان نیست. مقرره عمومی حفاظت از داده‌ها بر مشروعیت، کیفیت و امنیت پردازش داده شخصی تمرکز دارد؛ درحالی‌که مقرره خدمات دیجیتال بر قدرت پلتفرم در سامان‌دهی محیط اطلاعاتی، شکل‌دهی به دسترسی و مدیریت آثار نظام‌مند تصمیم‌های الگوریتمی نظارت می‌کند. ازاین‌جهت، مقرره خدمات دیجیتال سطح پلتفرمی اعتماد را شکل می‌دهد؛ سطحی که در آن معیارهای اصلی عبارت‌اند از: شفافیت تصمیم‌های پلتفرمی، محدودیت هدف‌گیری تبلیغاتی، اختیار کاربر در برابر توصیه‌گری، ارزیابی ریسک‌های نظام‌مند، ممیزی مستقل و دسترسی پژوهشگران به داده‌های پلتفرم.

۴.۱.۱. قانون هوش مصنوعی[1]

قانون هوش مصنوعی، سطح «سامانه هوش مصنوعی» را در نظام تقنینی اتحادیه اروپا سامان می‌دهد. موضوع اصلی این قانون، برخلاف مقرره عمومی حفاظت از داده‌ها که بر مشروعیت و کیفیت پردازش داده شخصی تمرکز دارد، و برخلاف مقرره خدمات دیجیتال که رفتار پلتفرم‌ها در سازمان‌دهی محیط اطلاعاتی را تنظیم می‌کند، خودِ سامانه هوش مصنوعی و شرایط توسعه، عرضه و بهره‌برداری از آن است .(Regulation (EU) 2024/1689, 2024) در این قانون، سامانه هوش مصنوعی به سامانه‌ای ماشینی اطلاق می‌شود که با درجاتی از خودمختاری عمل می‌کند و با دریافت داده ورودی، خروجی‌هایی مانند پیش‌بینی، توصیه یا تصمیم تولید می‌نماید که می‌تواند بر محیط فیزیکی یا مجازی اثر بگذارد .نقطه اصلی در این تعریف، «خودمختاری نسبی» و «اثرگذاری خروجی» است؛ زیرا قانون‌گذار اتحادیه دقیقاً در جایی مداخله می‌کند که سامانه از یک ابزار محاسباتی ساده فراتر می‌رود و خروجی آن می‌تواند در تصمیم‌های انسانی، اداری، اقتصادی یا زیرساختی اثر بگذارد؛ بنابراین، در این سطح، پرسش اصلی این نیست که چه داده‌ای پردازش شده یا محتوا چگونه در پلتفرم نمایش داده می‌شود؛ پرسش این است که خروجی سامانه چگونه تولید می‌شود، در چه زمینه‌ای به کار می‌رود، چه میزان بر موقعیت اشخاص اثر می‌گذارد و آیا امکان کنترل مؤثر بر آن وجود دارد یا نه.

[1]. Artificial Intelligence Act (AI Act).

مبنای اصلی قانون، طبقه‌بندی سامانه‌ها بر پایه شدت ریسک است. قانون هوش مصنوعی میان روش‌های ممنوع با ریسک غیرقابل‌قبول، سامانه‌های پرخطر، سامانه‌های با ریسک محدود و سامانه‌های کم‌ریسک تمایز می‌گذارد .(Balcioğlu et al., 2025; Chamberlain, 2023, p. 6) این طبقه‌بندی صرفاً برای نظم‌بخشی شکلی به انواع فناوری نیست؛ کارکرد آن تعیین آستانه تحمل‌پذیری حقوقی در برابر آثار سامانه است .در واقع، قانون با این پرسش شروع می‌کند که آیا کاربرد خاص هوش مصنوعی چنان با سلامت، ایمنی یا حقوق بنیادین درگیر است که مداخله پیشینی را توجیه کند یا نه .ازاین‌رو، «ریسک» در این قانون نه به معنای خطر مبهم فناوری، بلکه به معنای نسبت میان کاربرد سامانه، زمینه استفاده، گروه‌های متأثر و شدت پیامد احتمالی است .به همین دلیل، کاربردهایی مانند زیرساخت‌های حیاتی، آموزش، اشتغال، دسترسی به خدمات اساسی، اجرای قانون و مدیریت مهاجرت اهمیت ویژه می‌یابند؛ زیرا در این حوزه‌ها خروجی سامانه می‌تواند دسترسی، فرصت، امنیت یا آزادی اشخاص را تغییر دهد .پس شاخص این سطح را باید در سه محور جست‌وجو کرد: جایگاه کاربرد، شدت اثر خروجی، و امکان کنترل یا اصلاح تصمیم سامانه.

در مورد سامانه‌های پرخطر، مواد ۸ تا ۱۵ مجموعه‌ای از الزامات مشخص را پیش‌بینی می‌کند. این الزامات شامل استقرار نظام مدیریت ریسک در سراسر چرخه عمر سامانه، حاکمیت داده و توجه به کیفیت مجموعه‌داده‌های آموزشی، اعتبارسنجی و آزمون، مستندسازی فنی، اطلاع‌رسانی کافی به بهره‌برداران، نظارت انسانی، و تضمین دقت، استحکام و امنیت سایبری است (Ebers et al., 2021, p. 599). ارزش این الزامات در این است که قانون، خطر سامانه را به لحظه نهایی تولید خروجی محدود نمی‌کند؛ بلکه منشأهای پیشینی آن را نیز در نظر می‌گیرد: داده نامتوازن، طراحی مدل، آزمون ناکافی، مستندسازی ضعیف، ابهام در حدود استفاده، یا حذف نقش انسانی .از این منظر، سامانه قابل‌اعتماد سامانه‌ای نیست که صرفاً در شرایط آزمایشگاهی دقت بالایی داشته باشد؛ بلکه سامانه‌ای است که حدود توانایی و ناتوانی آن معلوم باشد، خطاهای قابل‌پیش‌بینی آن شناسایی شده باشد، بهره‌بردار بداند چگونه و در چه محدوده‌ای از آن استفاده کند، و در موقعیت‌های حساس امکان مداخله، توقف یا اصلاح وجود داشته باشد؛ بنابراین، ملاک این سطح «کارآمدی فنی» به‌تنهایی نیست؛ بلکه قابلیت ردیابی، کنترل، توضیح، نظارت انسانی و انتساب مسئولیت در سراسر چرخه عمر سامانه است.

قانون هوش مصنوعی همچنین مسئولیت را بر یک فاعل واحد متمرکز نمی‌کند. تعهدات میان ارائه‌دهندگان، واردکنندگان، توزیع‌کنندگان و بهره‌برداران تقسیم می‌شود و هر یک به‌تناسب نقش خود در زنجیره توسعه و استفاده از سامانه تکالیف خاصی دارند .این تقسیم مسئولیت صرفاً تکنیکی نیست؛ پاسخ به ماهیت پخش‌شده خطر در سامانه‌های هوش مصنوعی است .آسیب ممکن است از طراحی مدل آغاز شود، در داده‌های آموزشی تقویت گردد، در مرحله آزمون پنهان بماند، هنگام عرضه نادیده گرفته شود، و در مرحله بهره‌برداری به دلیل استفاده نادرست یا نبود نظارت انسانی بالفعل شود .اگر مسئولیت فقط به یک بازیگر نسبت داده شود، بخش مهمی از منشأ واقعی خطر از قلم می‌افتد .ازاین‌رو، قانون می‌کوشد مسئولیت را بر اساس «نقش مؤثر در ایجاد یا کنترل ریسک» توزیع کند؛ یعنی هر بازیگر به همان اندازه که در طراحی، عرضه، استقرار یا استفاده از سامانه نقش دارد، باید پاسخ‌گو باشد .این منطق، نقطه تمایز قانون هوش مصنوعی با مقرراتی است که بیشتر بر یک رابطه حقوقی یا یک نوع کنشگر تمرکز دارند.

افزون بر این، در برخی حوزه‌ها انجام «ارزیابی تأثیر بر حقوق بنیادین» پیش از استقرار سامانه پرخطر الزام‌آور است .اهمیت این ابزار در آن است که قانون را از سنجش صرفاً مهندسی سامانه عبور می‌دهد و پرسش را به سطح آثار حقوقی و اجتماعی خروجی می‌برد .در اینجا پرسش اصلی آن است که خروجی آن چه اثری بر کرامت انسانی، عدم تبعیض، دسترسی برابر، آزادی بیان، حریم خصوصی و حمایت از داده‌های شخصی دارد. بااین‌حال، این ابزار را نباید با ارزیابی تأثیر حفاظت از داده‌ها در مقرره عمومی حفاظت از داده‌ها یکی دانست .ارزیابی تأثیر حفاظت از داده‌ها بر منطق پردازش داده متمرکز است، اما ارزیابی مقرر در قانون هوش مصنوعی بر اثر خود سامانه و خروجی آن بر وضعیت حقوقی و اجتماعی اشخاص تمرکز دارد؛ بنابراین، حتی اگر پردازش داده از نظر مقرره عمومی حفاظت از داده‌ها قابل‌توجیه باشد، خروجی سامانه ممکن است از نظر تبعیض، حذف، محدودیت دسترسی یا اثر نامتناسب بر گروه‌های خاص همچنان مسئله‌ساز باشد .همین تمایز نشان می‌دهد که ریسک در سطح سامانه از مسیر «اثر تصمیم یا توصیه» سنجیده می‌شود، نه‌فقط از مسیر «پردازش داده».

از منظر نهادی نیز، قانون هوش مصنوعی به تعیین تکالیف مادی بسنده نمی‌کند و سازوکار نظارتی ویژه‌ای را بر پایه مراجع ملی ذی‌صلاح، «دفتر هوش مصنوعی» در سطح اتحادیه و «هیئت هوش مصنوعی» به‌عنوان نهاد هماهنگ‌کننده و مشورتی پیش‌بینی می‌کند .(Novelli et al., 2025, p. 570) این سازوکار نشان می‌دهد که کنترل سامانه‌های هوش مصنوعی با خوداظهاری بازیگران بازار پایان نمی‌یابد؛ زیرا تشخیص پرخطر بودن، ارزیابی کفایت مستندات، کیفیت نظارت انسانی و سنجش آثار حقوق بنیادین، نیازمند تخصص و هماهنگی نهادی است .براین‌اساس، جایگاه قانون هوش مصنوعی در نظام تقنینی اتحادیه ازآن‌جهت مستقل است که معیار آن نه مشروعیت پردازش داده است، نه رفتار پلتفرمی و نه امنیت محصول؛ بلکه توانایی حقوق برای قابل‌سنجش، قابل‌کنترل و پاسخ‌گو کردن خروجی سامانه در نسبت با سلامت، ایمنی و حقوق بنیادین است .شاخص‌های این سطح عبارت‌اند از :طبقه‌بندی ریسک، مدیریت چرخه عمر، کیفیت و حاکمیت داده، مستندسازی فنی، اطلاع‌رسانی به بهره‌بردار، نظارت انسانی، دقت و استحکام، امنیت سایبری، ارزیابی اثر بر حقوق بنیادین و توزیع مسئولیت بر اساس نقش بازیگران.

۵.۱.۱. مقرره تاب‌آوری سایبری[1]

1. Cyber Resilience Act (CRA).

مقرره تاب‌آوری سایبری، سطح «محصول متصل» را در نظام تقنینی اتحادیه اروپا سامان می‌دهد. موضوع اصلی این مقرره، برخلاف قانون هوش مصنوعی که بر کارکرد و ریسک سامانه هوش مصنوعی تمرکز دارد، امنیت سایبری محصولات دارای عناصر دیجیتال است؛ یعنی محصولات نرم‌افزاری یا سخت‌افزاری و نیز راه‌حل‌های پردازش راه دور که استفاده مقصود یا معقول قابل‌پیش‌بینی از آن‌ها مستلزم اتصال مستقیم یا غیرمستقیم به دستگاه یا شبکه ارتباطی باشد (Regulation (EU) 2024/2847, 2024). دامنه این تعریف از ابزارهای مصرفی متصل تا تجهیزات صنعتی و زیرساختی را در بر می‌گیرد .در این سطح، محصول فقط کالایی در بازار دیجیتال نیست؛ بلکه نقطه اتصال نرم‌افزار، سخت‌افزار، شبکه، داده، کاربر و گاه سامانه هوش مصنوعی است .ازاین‌رو، ضعف امنیتی محصول صرفاً یک نقص فنی محدود نیست؛ ممکن است مسیر نفوذ به داده، دست‌کاری کارکرد سامانه، اختلال در خدمت یا حتی آسیب فیزیکی را فراهم کند .به همین دلیل، مقرره تاب‌آوری سایبری به بخشی از اعتماد می‌پردازد که در بسیاری از بحث‌های داده، پلتفرم و سامانه مفروض گرفته می‌شود :اینکه محصول حامل فناوری، از نظر امنیتی قابل‌اتکا باشد.

این مقرره عمدتاً تولیدکنندگان، واردکنندگان، توزیع‌کنندگان و سایر فاعلان بازار را مخاطب قرار می‌دهد و هدف آن ارتقای امنیت سایبری محصولات دیجیتال برای مصرف‌کنندگان و کسب‌وکارهاست. محصولات بر پایه سطح ریسک امنیت سایبری در طبقات مختلف، از جمله «مهم» و «بحرانی»، قرار می‌گیرند و شدت تکالیف بر همین اساس تغییر می‌کند (مواد ۷ و ۸) .در اینجا معیار مداخله، اثر خروجی سامانه هوش مصنوعی یا قدرت پلتفرم در شکل‌دهی به جریان اطلاعات نیست؛ بلکه احتمال بهره‌برداری از ضعف امنیتی محصول و شدت پیامدهای آن است .به بیان دقیق‌تر، مقرره تاب‌آوری سایبری با این پرسش سروکار دارد که آیا محصول در برابر نفوذ، دست‌کاری، اختلال، سوءاستفاده یا بهره‌برداری از آسیب‌پذیری‌های شناخته‌شده و قابل‌پیش‌بینی مقاوم است یا نه؛ بنابراین، سنجه این سطح، تاب‌آوری محصول در چرخه عمر آن است: از طراحی و عرضه تا نگهداری، به‌روزرسانی و رسیدگی به آسیب‌پذیری‌های کشف‌شده.

هسته اصلی مقرره در دو اصل «امنیت در طراحی» و «امنیت به‌صورت پیش‌فرض» دیده می‌شود. تولیدکننده باید از مرحله طراحی تا عرضه و نگهداری، ریسک‌های امنیت سایبری را شناسایی و مدیریت کند؛ محصول عرضه‌شده تاحدامکان فاقد آسیب‌پذیری‌های شناخته‌شده و قابل‌بهره‌برداری باشد؛ و در طول عمر موردانتظار محصول یا دوره حداقلی مقرر، سازوکار رسیدگی به آسیب‌پذیری‌ها، ارائه به‌روزرسانی امنیتی و اطلاع‌رسانی مؤثر برقرار شود .اهمیت این قواعد در آن است که امنیت را از سطح واکنش پس از حادثه به مرحله طراحی و مسئولیت پیشینی تولیدکننده منتقل می‌کند .در محیط‌های متصل، نقص امنیتی غالباً پس از ورود محصول به زندگی روزمره کاربر آشکار می‌شود؛ جایی که دوربین خانگی، ابزار پوشیدنی، قفل هوشمند، خودرو متصل یا تجهیز صنعتی، با فضای خصوصی، بدن، رفت‌وآمد، مصرف انرژی یا زیرساخت حیاتی گره‌خورده است . در چنین وضعی، آسیب‌پذیری محصول فقط خطر نفوذ به یک دستگاه نیست؛ ممکن است به افشای الگوهای زیست، تغییر عملکرد فیزیکی، ازکارافتادن خدمت یا کاهش اعتماد به کل سامانه متصل منتهی شود .از همین رو، الزام به به‌روزرسانی، اطلاع‌رسانی و رسیدگی مستمر به آسیب‌پذیری‌ها بخشی از ماهیت حقوقی امنیت محصول است، نه صرفاً الزام فنی تولیدکننده.

مقرره تاب‌آوری سایبری با قانون هوش مصنوعی ارتباط عملی دارد، اما نباید در آن ادغام شود. هرگاه یک محصول هم‌زمان «محصول دارای عناصر دیجیتال» باشد و دربردارنده سامانه پرخطر هوش مصنوعی نیز تلقی شود، رعایت الزامات اساسی امنیت سایبری می‌تواند در ارزیابی انطباق با الزامات امنیتی قانون هوش مصنوعی نیز مؤثر باشد .(Beltrán, 2025, p. 11) بااین‌حال، ارتباط عملی میان دو متن به معنای وحدت موضوع آن‌ها نیست .قانون هوش مصنوعی می‌پرسد خروجی سامانه چه اثری بر سلامت، ایمنی یا حقوق بنیادین دارد؛ مقرره تاب‌آوری سایبری می‌پرسد محصول حامل آن سامانه تا چه اندازه در برابر تهدیدهای سایبری پایدار است .ممکن است سامانه از نظر طبقه‌بندی ریسک، مستندسازی و نظارت انسانی قابل‌دفاع باشد، اما محصولی که آن را اجرا می‌کند، به دلیل ضعف امنیتی، همچنان مسیر نفوذ یا دست‌کاری را باز بگذارد. در مقابل، ممکن است محصول از نظر امنیتی مقاوم باشد، اما سامانه مستقر بر آن از نظر سوگیری، نبود نظارت انسانی یا آثار نامتناسب بر حقوق بنیادین مسئله‌ساز شود .همین تفکیک، مرز «ریسک سامانه» و «ریسک محصول» را روشن می‌کند و مانع می‌شود همه الزامات امنیت، ایمنی و حریم خصوصی در یک عنوان کلی و مبهم ادغام شوند.

نظارت بر اجرای مقرره تاب‌آوری سایبری بر عهده مراجع ملی نظارت بر بازار در کشورهای عضو است و آژانس اتحادیه اروپا برای امنیت سایبری نقش پشتیبان و هماهنگ‌کننده دارد؛ از جمله از طریق تدوین راهنماها و استانداردها و تسهیل تبادل اطلاعات درباره آسیب‌پذیری‌ها و تهدیدهای مشترک .این شیوه نظارت نشان می‌دهد که امنیت محصول متصل فقط موضوع رابطه خصوصی میان تولیدکننده و خریدار نیست؛ بلکه به دلیل قابلیت سرایت آسیب‌پذیری‌ها، نیازمند نظارت عمومی، استانداردگذاری و تبادل اطلاعات میان نهادهای تخصصی است .براین‌اساس، مقرره تاب‌آوری سایبری معیار مستقلی برای سطح محصول متصل ارائه می‌کند :امنیت در طراحی، امنیت پیش‌فرض، مدیریت آسیب‌پذیری، به‌روزرسانی امنیتی، اطلاع‌رسانی درباره ضعف‌های امنیتی، ارزیابی انطباق و نظارت بر بازار .ازاین‌جهت، این مقرره نشان می‌دهد که اعتماد به سامانه‌های هوشمند فقط با کنترل داده، شفافیت پلتفرمی یا الزامات خاص هوش مصنوعی حاصل نمی‌شود؛ بلکه به محصولی نیاز دارد که از ابتدا برای مقاومت در برابر تهدیدهای سایبری طراحی، عرضه و نگهداری شده باشد.

۲.۱. کاربست تقنینی در حیطه حمایت از حریم خصوصی هوش مصنوعی و اینترنت اشیاء

کاربست هم‌زمان مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء را نباید به معنای وجود یک سازوکار کاملاً یکپارچه، بی اصطکاک و از پیش هماهنگ دانست. این چهار مقرره، هرچند در مجموع بخش مهمی از مسئله اعتماد، امنیت و حریم خصوصی را پوشش می‌دهند، از یک منطق واحد پیروی نمی‌کنند. هر یک از آن‌ها از زاویه‌ای متفاوت وارد مسئله می‌شود: مقرره عمومی حفاظت از داده‌ها از منظر پردازش داده شخصی و حقوق بنیادین؛ مقرره خدمات دیجیتال از منظر رفتار پلتفرم‌ها و مدیریت ریسک‌های نظام‌مند محیط برخط؛ قانون هوش مصنوعی از منظر کارکرد و خروجی سامانه هوش مصنوعی؛ و مقرره تاب‌آوری سایبری از منظر امنیت محصول دارای عناصر دیجیتال و آسیب‌پذیری‌های فنی آن.(Beltrán, 2025, p. 12)

ازاین‌رو، نقطه اصلی در کاربست این مقررات، صرفاً جمع‌کردن آن‌ها ذیل عنوان کلی «حکمرانی دیجیتال» نیست؛ بلکه تشخیص این است که هر مقرره در چه وضعیتی فعال می‌شود، چه منفعتی را حمایت می‌کند، چه بازیگری را مخاطب قرار می‌دهد و با چه ابزارهایی انطباق را می‌سنجد. در سطح داده، پرسش اصلی این است که داده شخصی با چه مبنای مشروع، چه میزان شفافیت، چه حدود هدف و چه تضمین‌هایی برای امنیت و حقوق اشخاص پردازش می‌شود. در سطح پلتفرم، پرسش به رفتار واسطه‌های دیجیتال مربوط می‌شود: اینکه پلتفرم چگونه محتوا، تبلیغات، توصیه‌ها و دسترسی کاربران را سامان می‌دهد و آثار نظام‌مند این تصمیم‌ها را چگونه مدیریت می‌کند. در سطح سامانه، تمرکز بر این است که خروجی هوش مصنوعی تا چه اندازه بر سلامت، ایمنی یا حقوق بنیادین اثر می‌گذارد و چه سازوکارهایی برای کنترل، مستندسازی، نظارت انسانی و اصلاح آن وجود دارد. در سطح محصول متصل نیز معیار اصلی، تاب‌آوری سایبری محصول، مدیریت آسیب‌پذیری‌ها، به‌روزرسانی امنیتی و نظارت بر بازار است.

براین‌اساس، نسبت میان این چهار مقرره را باید رابطه‌ای مبتنی بر «تکمیل مشروط» دانست، نه هم‌افزایی خودکار. ممکن است یک محصول هوشمند متکی بر اینترنت اشیاء، مانند ترموستات هوشمند، هم‌زمان چند سطح از این قواعد را درگیر کند، اما این هم‌زمانی به معنای وحدت موضوع یا وحدت روش نیست. اگر محصول داده‌های رفتاری یا مکانی کاربر را گردآوری و تحلیل کند، مقرره عمومی حفاظت از داده‌ها فعال می‌شود. اگر همان محصول از طریق یک خدمت واسطه‌ای یا پلتفرمی به کاربران، محتوا یا خدمات متصل شود، مقرره خدمات دیجیتال می‌تواند از منظر رفتار پلتفرمی و ریسک‌های نظام‌مند اهمیت یابد. اگر درون محصول سامانه‌ای وجود داشته باشد که خروجی آن به تصمیم، توصیه یا پیش‌بینی مؤثر بر اشخاص یا محیط منتهی شود، قانون هوش مصنوعی وارد می‌شود و اگر خود محصول از حیث اتصال، نرم‌افزار، سخت‌افزار یا به‌روزرسانی امنیتی آسیب‌پذیر باشد، مقرره تاب‌آوری سایبری معیار اصلی ارزیابی خواهد بود.

اهمیت این تفکیک در آن است که حمایت از حریم خصوصی در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء صرفاً با رعایت یکی از این مقررات تضمین نمی‌شود. انطباق با مقرره عمومی حفاظت از داده‌ها می‌تواند پردازش داده را مشروع‌تر و شفاف‌تر کند، اما لزوماً پاسخ‌گوی ریسک‌های نظام‌مند ناشی از توصیه‌گرهای پلتفرمی نیست. رعایت مقرره خدمات دیجیتال می‌تواند شفافیت و پاسخ‌گویی پلتفرمی را تقویت کند، اما جایگزین کنترل خروجی سامانه هوش مصنوعی یا امنیت محصول متصل نمی‌شود. به همین ترتیب، رعایت قانون هوش مصنوعی درباره سامانه پرخطر، اگر محصول حامل آن از نظر سایبری آسیب‌پذیر باشد، برای تضمین اعتماد کافی نیست؛ و رعایت مقرره تاب‌آوری سایبری نیز به‌تنهایی تبعیض الگوریتمی، نبود نظارت انسانی یا آثار نامتناسب خروجی سامانه را برطرف نمی‌کند.

بنابراین، کاربست تقنینی در این حوزه باید بر پایه تفکیک دقیق چهار سطح انجام شود: داده، پلتفرم، سامانه و محصول. هر سطح، معیار مستقل خود را دارد؛ اما در عمل، میان آن‌ها نقاط تماس و گاه تنش اجرایی پدید می‌آید. مسئله اصلی این بخش نشان‌دادن این است که حمایت مؤثر از حریم خصوصی و اعتماد الگوریتمی زمانی شکل می‌گیرد که نخست مرز هر مقرره روشن شود و سپس نسبت آن با سایر مقررات، در موارد هم‌پوشانی یا تعارض، به‌صورت موردی سنجیده شود. بر همین مبنا، در ادامه ابتدا نقاط اتصال مستقیم میان این مقررات بررسی می‌شود و سپس نشان داده خواهد شد که اشتراک آن‌ها در زبان ریسک، به معنای یکسان بودن منطق حکمرانی، ابزار انطباق یا نهادهای نظارتی آن‌ها نیست.

۱.۲.۱. هم‌افزایی‌های مستقیم

در نخستین سطح، نسبت میان مقرره عمومی حفاظت از داده‌ها و مقرره خدمات دیجیتال را باید **هم‌افزایی کارکردی**، نه **وحدت هنجاری** دانست. هر دو مقرره از اشخاص در محیط دیجیتال حمایت می‌کنند، اما از دو منطق متفاوت آغاز می‌شوند: مقرره عمومی حفاظت از داده‌ها بر کنترل داده شخصی، مشروعیت پردازش، محدودیت هدف، کمینه‌سازی و تضمین حقوق بنیادین در فرایند پردازش تمرکز دارد؛ درحالی‌که مقرره خدمات دیجیتال، قدرت پلتفرم در سازمان‌دهی محیط برخط،

نمایش محتوا، تبلیغات، سامانه‌های توصیه‌گر و مدیریت ریسک‌های نظام‌مند را تنظیم می‌کند. نقطه اتصال این دو مقرره زمانی پدید می‌آید که داده شخصی یا استنباط حاصل از آن، از سطح پردازش فراتر رفته و به ابزار اثرگذاری پلتفرمی بر توجه، انتخاب، رفتار یا آسیب‌پذیری کاربر تبدیل شود. در این نقطه، مرز تحلیلی دو متن آشکار است: مقرره عمومی حفاظت از داده‌ها می‌پرسد داده با چه مبنایی و در چه حدودی پردازش شده است؛ مقرره خدمات دیجیتال می‌پرسد پلتفرم چگونه از داده، استنباط یا پروفایل برای شکل‌دادن به تجربه کاربر و مدیریت محیط دیجیتال استفاده می‌کند.

بند ۳ ماده ۲۶ مقرره خدمات دیجیتال نمونه روشن این هم‌افزایی محدود است. این ماده، تبلیغات مبتنی بر پروفایل‌سازی را هرگاه بر «دسته‌بندی‌های ویژه داده‌های شخصی» موضوع ماده ۹(۱) مقرره عمومی حفاظت از داده‌ها متکی باشد، ممنوع می‌کند. اهمیت حکم در آن است که مقرره خدمات دیجیتال، قاعده داده‌ای مقرر در مقرره عمومی حفاظت از داده‌ها را تکرار نمی‌کند، بلکه آن را به قلمرو رفتار تبلیغاتی پلتفرم منتقل می‌سازد. در نتیجه، اگر پلتفرم از طریق استنباط الگوریتمی و بر پایه داده‌های دستگاه‌های متصل، به اطلاعات حساسی مانند وضعیت سلامت یا باور مذهبی کاربر دست یابد، نمی‌تواند آن را مبنای هدف‌گیری تبلیغاتی قرار دهد؛ برای نمونه، برآورد احتمال ابتلا به یک اختلال از داده‌های خواب و ضربان قلب ساعت هوشمند، مبنای مجاز تبلیغ محصولات دارویی نیست(Wolters & Zuiderveen Borgesius, 2025, p. 3) ؛ بنابراین، مقرره عمومی حفاظت از داده‌ها حساسیت داده یا استنباط را شناسایی می‌کند، اما مقرره خدمات دیجیتال از تبدیل آن به اهرم اثرگذاری تبلیغاتی جلوگیری می‌کند؛ در نتیجه، انطباق داده‌ای شرط مهم است، اما برای مشروعیت رفتار پلتفرمی کافی نیست.

رویه قضایی نیز این تمایز را تقویت می‌کند، بی‌آنکه منطق دو مقرره را در یکدیگر ادغام کند. در پرونده گوگل اسپانیا علیه آژانس اسپانیایی حفاظت از داده‌ها، موتور جست‌وجو «کنترل‌کننده داده» شناخته شد و دیوان، توازن میان حفاظت از داده، حریم خصوصی و آزادی اطلاع‌رسانی را صورت‌بندی کرد .(Google Spain, 2014, para. 33) این رأی بر نقش واسطه دیجیتال در دسترس‌پذیرکردن، رتبه‌بندی و استمرار نمایش داده متمرکز است و در منطق داده‌محور فهم می‌شود. در مقابل، در پرونده گلاویشنیشگ –پیشچک، مسئولیت پلتفرم برای حذف محتوای غیرقانونی و محتوای معادل پس از اطلاع‌رسانی به رسمیت شناخته شد .(Glawischnig-Piesczek, 2019, para. 41)این رأی به منطق مدیریت محتوای غیرقانونی و جلوگیری از استمرار اثر زیان‌بار آن نزدیک‌تر

است؛ بنابراین، دو رأی دو صورت متفاوت از مسئولیت واسطه‌های دیجیتال را نشان می‌دهند: مسئولیت ناشی از دسترس‌پذیرکردن داده و مسئولیت ناشی از استمرار یا بازتولید محتوای غیرقانونی. مقرره خدمات دیجیتال منطق دوم را با تعهدات ساختاری درباره شفافیت، تعدیل محتوا و مدیریت ریسک‌های نظام‌مند توسعه می‌دهد؛ درحالی‌که اصول مشروعیت، شفافیت، محدودیت هدف و کمینه‌سازی در مقرره عمومی حفاظت از داده‌ها همچنان معیار مستقل پردازش داده باقی می‌مانند و می‌توانند اجرای تعهدات حمایتی مقرره خدمات دیجیتال، به‌ویژه نسبت به کودکان ذیل ماده ۲۸، را تقویت کنند.(OECD, 2021, OECD/LEGAL/0389)

در زوج دوم، یعنی قانون هوش مصنوعی و مقرره تاب‌آوری سایبری، هم‌افزایی در نقطه تماس میان «سامانه» و «محصول متصل» شکل می‌گیرد؛ اما این تماس نباید به ادغام معیارهای انطباق منتهی شود. قانون هوش مصنوعی بر سامانه، خروجی آن و اثر احتمالی آن بر سلامت، ایمنی و حقوق بنیادین تمرکز دارد؛ درحالی‌که مقرره تاب‌آوری سایبری بر امنیت محصول دارای عناصر دیجیتال، آسیب‌پذیری، به‌روزرسانی و مسئولیت تولیدکننده در چرخه عمر محصول متمرکز است. به بیان دقیق‌تر، قانون هوش مصنوعی ریسک را از مسیر اثر تصمیم، توصیه یا پیش‌بینی سامانه می‌سنجد؛ اما مقرره تاب‌آوری سایبری ریسک را از مسیر امکان نفوذ، دست‌کاری، اختلال یا بهره‌برداری از ضعف امنیتی محصول ارزیابی می‌کند؛ بنابراین، وقتی سامانه هوش مصنوعی در قالب محصول متصل عرضه می‌شود، ممکن است هر دو متن هم‌زمان اعمال شوند، اما پرسش حقوقی آن‌ها متفاوت می‌ماند: آیا خروجی سامانه از حیث حقوق بنیادین و ایمنی قابل‌قبول است؟ و آیا محصول حامل سامانه از حیث امنیت سایبری قابل اتکاست؟

بر همین مبنا، هرگاه محصولی هم‌زمان مشمول مقرره تاب‌آوری سایبری و واجد وصف «سامانه پرخطر» ذیل قانون هوش مصنوعی باشد، رعایت الزامات امنیت سایبری مقرره تاب‌آوری سایبری می‌تواند در ارزیابی انطباق با الزامات امنیتی قانون هوش مصنوعی مؤثر باشد؛ همچنین «اظهارنامه انطباق اتحادیه اروپا» صادره بر اساس مقرره تاب‌آوری سایبری می‌تواند در ارزیابی انطباق سامانه نیز مورداستفاده قرار گیرد (Regulation (EU) 2024/1689, 2024b; Regulation (EU) 2024/2847, 2024). بااین‌حال، اثر این هم‌افزایی به قلمرو امنیت و تاب‌آوری فنی محدود است. انطباق امنیتی محصول ثابت نمی‌کند که سامانه از حیث تبعیض، شفافیت، نظارت انسانی، توضیح‌پذیری یا اثر بر حقوق بنیادین نیز منطبق است؛ همان‌گونه که انطباق سامانه با قانون هوش

مصنوعی، ضعف امنیتی محصول حامل آن را جبران نمی‌کند. ازاین‌رو، امنیت محصول شرط لازم اعتماد به سامانه است، اما شرط کافی آن نیست؛ و کنترل خروجی سامانه نیز جایگزین مدیریت آسیب‌پذیری محصول نمی‌شود.

رأی بوستن ساینتیفیک مدیزین‌تکنیک درباره دستگاه‌های پزشکی کاشتنی، هرچند مستقیماً درباره هوش مصنوعی نیست، از حیث منطق ایمنی محصول اهمیت دارد؛ زیرا دیوان پذیرفت که خطر نقص در یک «دسته کامل» از محصولات می‌تواند برای احراز عیب و لزوم تعویض کافی باشد (Boston Scientific, 2015, para. 37). اهمیت این رأی برای محصولات متصل آن است که نقص یا آسیب‌پذیری ممکن است از سطح یک دستگاه منفرد فراتر رود و به خطری مشترک در یک گروه از محصولات تبدیل شود. بااین‌حال، این منطق همچنان در سطح ایمنی و عیب محصول باقی می‌ماند و نمی‌تواند جایگزین ارزیابی اثر سامانه هوش مصنوعی بر حقوق بنیادین شود؛ بنابراین، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری در نقطه امنیت با یکدیگر تماس دارند، اما از حیث موضوع، معیار انطباق، نوع ریسک و آثار نظارتی مستقل‌اند.

در سطح نهادی نیز «محیط‌های آزمون مقرراتی» محل تلاقی مقررات‌اند، نه ابزار ادغام آن‌ها. قانون هوش مصنوعی کشورهای عضو را به ایجاد این محیط‌ها برای آزمایش سامانه‌ها ترغیب می‌کند و مقرره تاب‌آوری سایبری نیز سازوکارهایی برای آزمون تاب‌آوری و امنیت محصول پیش‌بینی کرده است. ماده ۵۹ قانون هوش مصنوعی درباره استفاده مجدد از داده‌های شخصی در این محیط‌ها، به اصول مشروعیت، کمینه‌سازی، محدودیت هدف و امنیت در مقرره عمومی حفاظت از داده‌ها متصل است. ازاین‌جهت، «ارزیابی تأثیر حفاظت از داده‌ها» ذیل ماده ۳۵ مقرره عمومی حفاظت از داده‌ها می‌تواند برای سنجش ریسک‌های داده‌ای در محیط آزمون لازم باشد، اما کافی نیست. در همان محیط، سه سنجش باید از هم جدا بمانند: سنجش داده‌ای درباره مشروعیت و حدود پردازش؛ سنجش سامانه‌ای درباره اثر خروجی هوش مصنوعی بر حقوق بنیادین؛ و سنجش محصولی درباره امنیت، آسیب‌پذیری و تاب‌آوری سایبری (Baldini, 2025, p. 72) ؛ بنابراین، هم‌افزایی نهادی زمانی قابل‌دفاع است که این ارزیابی‌ها به یکدیگر فروکاسته نشوند، بلکه هر یک در سطح خود انجام شود و سپس نقاط تماس یا تنش میان آن‌ها ارزیابی گردد.

۲.۲.۱. هم‌افزایی‌های غیرمستقیم

هم‌افزایی غیرمستقیم میان مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش

مصنوعی و مقرره تاب‌آوری سایبری، نه از وحدت موضوع آن‌ها ناشی می‌شود و نه از وجود یک آزمون مشترک برای همه ریسک‌ها؛ بلکه از این واقعیت برمی‌خیزد که هر چهار متن، بازیگران دیجیتال را به سمت تصمیم‌گیری مستند، ارزیابی پیشینی، بازبینی مستمر و پاسخ‌گویی قابل‌اثبات سوق می‌دهند .به بیان دقیق‌تر، نقطه اشتراک این مقررات در «نتیجه حقوقی» آن‌ها نیست، بلکه در نوعی انضباط نهادی است که بر شناسایی ریسک، ثبت مبانی تصمیم، اتخاذ تدابیر کاهش‌دهنده و امکان نظارت بیرونی استوار می‌شود .ازاین‌رو، هم‌افزایی غیرمستقیم را باید در سطح ظرفیت‌های سازمانی و اثباتی فهمید، نه در سطح ادغام معیارهای ماهوی.

بر همین مبنا، هرچند هر چهار مقرره از زبان ریسک استفاده می‌کنند، موضوع ریسک در آن‌ها متفاوت است .در مقرره عمومی حفاظت از داده‌ها، ریسک به اثر پردازش بر حقوق و آزادی‌های اشخاص مربوط می‌شود؛ در مقرره خدمات دیجیتال، ریسک به آثار نظام‌مند طراحی و بهره‌برداری خدمات پلتفرمی بر محیط برخط و جامعه بازمی‌گردد؛ در قانون هوش مصنوعی، ریسک از مسیر خروجی سامانه و اثر آن بر سلامت، ایمنی و حقوق بنیادین سنجیده می‌شود؛ و در مقرره تاب‌آوری سایبری، ریسک به امکان بهره‌برداری از آسیب‌پذیری‌های محصول و پیامدهای امنیتی آن مربوط است؛ بنابراین، عبارت «رویکرد مبتنی بر ریسک» در این چهار متن، معنای یکسان ندارد. آنچه قابل‌انتقال است، روش کلی مستندسازی و مدیریت ریسک است؛ نه خود معیار حقوقی ریسک. این تمایز برای پرهیز از ساده‌سازی رابطه مقررات اهمیت اساسی دارد.

از این منظر، یک سازمان فعال در اکوسیستم هوش مصنوعی و اینترنت اشیاء می‌تواند از برخی ظرفیت‌های مشترک میان این مقررات بهره ببرد؛ برای مثال، ایجاد دفترچه ثبت ریسک، سازوکار مستندسازی تصمیمات فنی، فرایند بازبینی دوره‌ای، نظام گزارش‌دهی رخدادها، آموزش داخلی و تعیین مسئولیت میان واحدهای فنی، حقوقی و مدیریتی، می‌تواند اجرای چند مقرره را هم‌زمان تسهیل کند .بااین‌حال، چنین ظرفیت‌هایی فقط «زیرساخت انطباق» ایجاد می‌کنند و جایگزین ارزیابی‌های خاص هر مقرره نمی‌شوند .ارزیابی تأثیر حفاظت از داده‌ها می‌تواند سازمان را نسبت به پیامدهای پردازش داده حساس کند، اما به‌تنهایی ریسک‌های نظام‌مند پلتفرمی، آثار خروجی سامانه هوش مصنوعی یا آسیب‌پذیری امنیتی محصول را نمی‌سنجد .به همین ترتیب، نظام مدیریت آسیب‌پذیری در مقرره تاب‌آوری سایبری می‌تواند احتمال نقض امنیت یا دست‌کاری محصول را کاهش دهد، اما مسئله تبعیض الگوریتمی، نبود نظارت انسانی یا آثار اجتماعی سامانه‌های توصیه‌گر

را برطرف نمی‌کند.

رأی پرونده حقوق دیجیتال ایرلند همین مرز را از منظر حقوق بنیادین روشن می‌کند. دیوان، نگهداری عام و نامتمایز داده‌های ترافیک و مکان را به دلیل مداخله شدید و نامتناسب در حقوق حریم خصوصی و حمایت از داده‌ها باطل اعلام کرد و یادآور شد که حتی هدف مشروعی مانند مبارزه با جرایم جدی نیز نمی‌تواند شدت مداخله و ضعف تضمین‌ها را توجیه کند (Digital Rights Ireland Ltd, 2014, para. 57). اهمیت این رأی در بحث حاضر آن است که ارزیابی ریسک در حقوق دیجیتال، صرفاً محاسبه احتمال وقوع یک تهدید یا زیان فنی نیست؛ بلکه باید شدت مداخله، ضرورت اقدام، کیفیت تضمین‌ها، امکان نظارت و تناسب میان هدف و ابزار را نیز در بر گیرد .این منطق می‌تواند در همه مقررات یادشده الهام‌بخش باشد، اما خروجی آن در هر متن متفاوت خواهد بود: در مقرره عمومی حفاظت از داده‌ها، به محدودسازی یا بازطراحی پردازش می‌انجامد؛ در مقرره خدمات دیجیتال، به تدابیر کاهش ریسک نظام‌مند؛ در قانون هوش مصنوعی، به کنترل سامانه پرخطر؛ و در مقرره تاب‌آوری سایبری، به اصلاح یا به‌روزرسانی محصول.

براین‌اساس، هم‌افزایی غیرمستقیم زمانی قابل‌دفاع است که میان «اشتراک در ابزارهای مدیریتی» و «تفاوت در معیارهای حقوقی» تفکیک شود .ممکن است یک نظام داخلی مدیریت ریسک، داده‌های لازم برای چند ارزیابی را فراهم کند؛ اما نهاد ناظر، معیار اثبات، موضوع ارزیابی و پیامد عدم انطباق در هر مقرره متفاوت است .برای نمونه، مستندات امنیتی یک محصول می‌تواند برای بررسی تاب‌آوری سایبری و تا حدی برای ارزیابی امنیت سامانه هوش مصنوعی مفید باشد، اما نمی‌تواند نشان دهد که سامانه از نظر تبعیض، شفافیت یا نظارت انسانی نیز منطبق است .همچنین، مستندات مربوط به مشروعیت پردازش داده، برای سنجش حقوق موضوع داده ضروری است، اما به‌خودی‌خود نشان نمی‌دهد که طراحی پلتفرم آثار نظام‌مند زیان‌بار ندارد.

در نتیجه، هم‌افزایی غیرمستقیم این چهار مقرره را باید هم‌افزایی در سطح ظرفیت انطباق دانست، نه هم‌افزایی در سطح معیار نهایی .این مقررات می‌توانند سازمان‌ها را به سمت فرهنگ مشترک پیشگیری، مستندسازی، بازبینی و پاسخ‌گویی سوق دهند؛ اما هر سطح همچنان آزمون مستقل خود را حفظ می‌کند: آزمون داده‌ای در مقرره عمومی حفاظت از داده‌ها، آزمون پلتفرمی در مقرره خدمات دیجیتال، آزمون سامانه‌ای در قانون هوش مصنوعی و آزمون محصولی در مقرره تاب‌آوری سایبری . به همین دلیل، در ادامه بررسی ریسک‌های سازمانی، ریسک‌های متوجه حقوق و آزادی‌ها،

ریسک‌های نظام‌مند و ریسک‌های مرتبط با امنیت ملی، باید با حفظ همین تفکیک انجام شود؛ زیرا تنها در این صورت می‌توان از فروکاستن رابطه مقررات اتحادیه اروپا به یک روایت کلی و ساده‌انگارانه از «هماهنگی ریسک‌محور» پرهیز کرد.

۱.۲.۲.۱. ریسک‌های سازمانی

ریسک‌های سازمانی در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء، صرفاً پیامد فرعی نقض داده یا حمله سایبری نیستند؛ بلکه از نسبت میان سه عامل پدید می‌آیند: پیچیدگی فنی محصول یا خدمت، تعدد تکالیف حقوقی، و توان سازمان برای اثبات تصمیمات انطباقی خود .مسئولیت حقوقی، زیان مالی، لطمه اعتباری، اختلال در تداوم کسب‌وکار و هزینه‌های انطباق، هنگامی تشدید می‌شوند که سازمان نتواند نشان دهد در هر سطح، ریسک مربوط را با معیار مناسب همان سطح شناسایی، ارزیابی و کنترل کرده است .ازاین‌رو، ریسک سازمانی در اینجا نه یک ریسک مستقل از مقررات، بلکه اثر انعکاسی ناهماهنگی یا اجرای ناقص تعهداتی است که از مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری ناشی می‌شود.

در این میان، مقرره تاب‌آوری سایبری از مسیر امنیت محصول، ریسک سازمانی را کاهش می‌دهد، اما آن را به طور کامل منتفی نمی‌سازد. الزام تولیدکنندگان به طراحی ایمن، مدیریت آسیب‌پذیری‌ها، به‌روزرسانی امنیتی و اطلاع‌رسانی درباره ضعف‌های امنیتی، احتمال بهره‌برداری از نقص‌های فنی و در نتیجه احتمال حمله موفق علیه کاربران و سازمان را محدود می‌کند .اهمیت این مقرره برای سازمان در آن است که امنیت سایبری را از قلمرو تدابیر اختیاری یا واکنش پس از حادثه خارج می‌سازد و به تعهدی مستمر در چرخه عمر محصول تبدیل می‌کند .در دستگاه‌های متصل مبتنی بر هوش مصنوعی، این تعهد می‌تواند ریسک مسئولیت مدنی، قراردادی یا مسئولیت ناشی از عیب محصول را کاهش دهد؛ زیرا بخشی از معیار انتساب مسئولیت، به قابل‌پیش‌بینی بودن آسیب‌پذیری و کیفیت واکنش تولیدکننده در برابر آن وابسته می‌شود .(Colonna, 2025, p. 106105) بااین‌حال، انطباق امنیتی محصول فقط از حیث تاب‌آوری فنی به سازمان کمک می‌کند و جایگزین کنترل آثار خروجی سامانه یا مشروعیت پردازش داده نمی‌شود.

ازسوی‌دیگر، مقرره عمومی حفاظت از داده‌ها ریسک سازمانی را از مسیر پاسخ‌گویی و بار اثبات کنترل می‌کند. مواد ۲۴، ۲۵، ۳۲ و ۳۵ این مقرره، سازمان را صرفاً به رعایت قواعد شکلی مکلف نمی‌کنند؛ بلکه از آن می‌خواهند بتواند نسبت میان هدف پردازش، نوع داده، شدت ریسک، تدابیر

امنیتی و آثار احتمالی بر اشخاص را مستند سازد؛ بنابراین، ریسک سازمانی در این سطح هنگامی افزایش می‌یابد که سازمان از داده‌های رفتاری، مکانی یا زیستی حاصل از دستگاه‌های متصل برای پروفایل‌سازی یا تصمیم‌سازی تجاری استفاده کند، اما نتواند ضرورت پردازش، حدود هدف، مبنای مشروع و تدابیر کاهش ریسک را نشان دهد .رأی پرونده «پست اتریش» همین پیوند میان پردازش داده و مسئولیت‌سازمانی را روشن می‌سازد: شرکت پستی با تحلیل داده‌های شهروندان، گرایش سیاسی آنان را برآورد و این داده‌ها را به مشتریان تجاری فروخته بود؛ دیوان ضمن تأکید بر ضرورت اثبات «آسیب واقعی» برای استحقاق غرامت، تصریح کرد صرف نقض مقرره برای مطالبه خسارت کافی نیست .(UI v Österreichische Post AG, 2023, para. 42) اهمیت رأی برای بحث حاضر در این است که هرچند مسئولیت مدنی منوط به اثبات آسیب است، بهره‌برداری تجاری از داده‌های پروفایلی بدون مستندسازی و ارزیابی ریسک، سازمان را در معرض دعوایی قرار می‌دهد که در آن موضوع اصلی فقط وقوع نقض نیست، بلکه کیفیت تصمیمات انطباقی سازمان نیز ارزیابی می‌شود.

باوجود این، اجرای هم‌زمان این مقررات برای سازمان‌ها همواره اثر کاهنده ندارد و می‌تواند خود به ریسک انطباقی تبدیل شود .تفاوت در مفاهیمی مانند «کنترل‌کننده داده»، «خدمت پلتفرمی»، «سامانه پرخطر هوش مصنوعی» و «محصول دارای عناصر دیجیتال» سبب می‌شود سازمان با یک مسیر واحد و ساده برای انطباق روبه‌رو نباشد .یک تولیدکننده دستگاه متصل ممکن است هم‌زمان ناچار باشد مبنای پردازش داده را ذیل مقرره عمومی حفاظت از داده‌ها توجیه کند، امنیت محصول را ذیل مقرره تاب‌آوری سایبری نشان دهد، در صورت وجود سامانه پرخطر، الزامات قانون هوش مصنوعی را رعایت کند، و اگر خدمت او واجد کارکرد پلتفرمی باشد، به تعهدات مقرره خدمات دیجیتال نیز توجه داشته باشد .در چنین وضعی، ریسک سازمانی دقیقاً از جایی پدید می‌آید که سازمان یک ارزیابی را به‌جای ارزیابی دیگر می‌نشاند؛ برای مثال، امنیت محصول را معادل انطباق سامانه می‌گیرد، یا مشروعیت پردازش داده را برای توجیه همه آثار پلتفرمی کافی می‌داند.

براین‌اساس، مدیریت ریسک سازمانی در این حوزه مستلزم ادغام ساده مقررات نیست، بلکه نیازمند تفکیک درونی ارزیابی‌ها و اتصال مستند نتایج آن‌هاست .سازمان باید بتواند نشان دهد کدام تصمیم به سطح داده مربوط بوده، کدام تصمیم به امنیت محصول، کدام تصمیم به عملکرد سامانه و کدام تصمیم به رفتار پلتفرمی .تنها در این صورت است که مستندسازی انطباق، به دفاعی قابل‌اتکا در برابر جریمه‌های اداری، دعاوی مسئولیت، آسیب اعتباری و اختلال عملیاتی تبدیل می‌شود؛ بنابراین،

ریسک سازمانی نه با اجرای صوری یک سازوکار عمومی مدیریت ریسک، بلکه با ایجاد نظامی قابل‌ردیابی برای تفکیک، ثبت و هماهنگ‌سازی ارزیابی‌های داده‌ای، محصولی، سامانه‌ای و پلتفرمی کاهش می‌یابد.

۲.۲.۲.۱. ریسک‌های متوجه حقوق و آزادی‌ها

ریسک‌های متوجه حقوق و آزادی‌ها در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء زمانی شکل می‌گیرند که داده، اتصال فنی و تصمیم‌سازی الگوریتمی از کارکرد صرفاً فنی فراتر روند و به تغییر واقعی در وضعیت فرد منتهی شوند؛ مانند برچسب‌گذاری رفتاری، افزایش هزینه دسترسی به خدمت، حذف از فضای ارتباطی، قرار گرفتن در معرض تصمیم خودکار یا کاهش امکان اعتراض مؤثر؛ بنابراین، نقطه تمرکز این بخش نه هزینه سازمانی و نه صرف اجرای هم‌زمان مقررات، بلکه لحظه‌ای است که فناوری به مداخله در حریم خصوصی، آزادی بیان، عدم تبعیض، امنیت شخصی یا فرایند منصفانه تبدیل می‌شود. از این منظر، ریسک حقوق و آزادی‌ها باید بر اساس آثار آن بر شخص سنجیده شود، نه صرفاً بر پایه نوع فناوری یا عنوان مقرره.

در مقرره عمومی حفاظت از داده‌ها، این ریسک بیش از همه در استنباط و تصمیم‌گیری بر پایه داده‌های رفتاری و محیطی ظاهر می‌شود. داده‌های حاصل از دستگاه‌های متصل، مانند داده‌های سلامت، الگوی حضور در منزل، مصرف انرژی، داده‌های مکانی یا زیستی، ممکن است در ظاهر پراکنده باشند، اما با ترکیب و تحلیل الگوریتمی به تصویری دقیق از سبک زندگی، وضعیت سلامت، عادات شخصی یا آسیب‌پذیری‌های فرد تبدیل شوند. خطر اصلی، صرف گردآوری داده نیست؛ بلکه تبدیل داده‌های روزمره به مبنای تصمیمی اثرگذار بر فرصت‌ها، تعهدات یا وضعیت حقوقی شخص است. ازاین‌رو، محدودیت تصمیم‌گیری صرفاً خودکار ذیل ماده ۲۲ اهمیت ویژه دارد. برای نمونه، اگر بیمه‌گر بر پایه داده‌های خانه هوشمند درباره نرخ یا شرایط پوشش تصمیم بگیرد، تصمیم باید با امکان مداخله انسانی، حق اظهارنظر و حق اعتراض همراه باشد؛ وگرنه فرد با تصمیمی مواجه می‌شود که نه منطق آن را می‌فهمد و نه امکان مؤثر برای مقابله با آثارش دارد؛ وضعیتی که می‌تواند با خطر تبعیض ناشی از پردازش داده نیز پیوند یابد.(Piasecki & Chen, 2022, p. 118)

در مقرره خدمات دیجیتال، ریسک حقوق و آزادی‌ها از مسیر مدیریت الگوریتمی میدان بیان و دسترسی به اطلاعات پدید می‌آید. مقابله با محتوای غیرقانونی، اطلاعات زیان‌آور یا محتوای ناقض حیثیت و حریم خصوصی نباید به حذف ناموجه بیان مشروع یا محدودشدن دسترسی به اطلاعات

بینجامد. ازاین‌رو، ریسک پلتفرمی دوگانه است: تعدیل ناکافی می‌تواند حیثیت، امنیت یا حریم خصوصی اشخاص را در معرض آسیب قرار دهد؛ اما تعدیل افراطی نیز آزادی بیان و مشارکت در گفتمان عمومی را محدود می‌کند. سامانه‌های خودکار تشخیص محتوا، به‌ویژه هنگامی که از داده‌های تصویری، ویدئویی یا گزارش‌های خودکار محیط‌های متصل استفاده می‌کنند، مستعد هر دو خطا هستند. در این زمینه، شفافیت تصمیم‌های محدودکننده، امکان اعتراض و نظارت بیرونی ضمانت‌های صرفاً شکلی نیستند؛ بلکه از تبدیل مدیریت پلتفرمی به محدودیتی پنهان و دشوار اعتراض بر آزادی‌های ارتباطی جلوگیری می‌کنند.

در قانون هوش مصنوعی، ریسک حقوق و آزادی‌ها از مسیر اثر خروجی سامانه بر وضعیت فرد ظاهر می‌شود. ممنوعیت روش‌هایی مانند دست‌کاری پنهان و امتیازدهی اجتماعی، و الزامات سامانه‌های پرخطر، نشان می‌دهد نگرانی قانون فقط خطای فنی نیست؛ بلکه پیامد خروجی بر کرامت انسانی، برابری، امکان انتخاب و دسترسی منصفانه است. پرسش اصلی این است که آیا پیش‌بینی، تشخیص، رتبه‌بندی یا توصیه سامانه می‌تواند فرد را از فرصت، خدمت، امنیت یا حق مشخصی محروم کند، یا او را در معرض تصمیمی نامتناسب و غیرقابل‌اعتراض قرار دهد. در اینترنت اشیاء، این مسئله در سامانه‌های تشخیص چهره در فضاهای عمومی، تحلیل‌گرهای رفتاری در محیط کار و مدیریت دسترسی مبتنی بر حسگرها آشکار می‌شود؛ زیرا خطای مدل، سوگیری داده یا نبود نظارت انسانی می‌تواند به محرومیت، تبعیض یا کنترل رفتاری ناموجه بینجامد (Iliopoulou-Penot, 2025, p. 14).

رأی مربوط به سامانه شناسایی ریسک در هلند، نمونه مهمی از همین منطق است. دادگاه لاهه این سامانه را به دلیل فقدان شفافیت، عدم تناسب میان حجم داده و هدف، و خطر تبعیض ساختاری، مغایر ماده ۸ کنوانسیون اروپایی حقوق بشر و معیارهای پردازش داده دانست (SyRI, 2020, para. 6.90). اهمیت رأی در آن است که نقض حقوق و آزادی‌ها را به یک داده حساس یا تصمیم منفرد محدود نمی‌کند؛ بلکه نشان می‌دهد ترکیب گسترده داده‌ها، ابهام در منطق ارزیابی، ضعف تناسب و نبود تضمین‌های نظارتی می‌تواند خود به مداخله نامتناسب در حقوق اشخاص تبدیل شود. از همین رو، منطق رأی با مواد ۲۲ و ۳۵ مقرره عمومی حفاظت از داده‌ها و الزامات قانون هوش مصنوعی هم‌سو است و نشان می‌دهد ریسک حقوقی ممکن است از انباشت داده‌های ظاهراً عادی و تصمیم‌های الگوریتمی غیر شفاف پدید آید.

در این میان، مقرره تاب‌آوری سایبری نقش پشتیبان اما مهمی دارد. در ریسک‌های متوجه حقوق و

آزادی‌ها، امنیت سایبری موضوعی صرفاً فنی نیست؛ زیرا نفوذ به دوربین خانگی، قفل هوشمند، ابزار پوشیدنی یا خودرو متصل می‌تواند مستقیماً به افشای زندگی خصوصی، دست‌کاری عملکرد محصول، تهدید ایمنی جسمی یا نظارت غیرمجاز منتهی شود؛ بنابراین، امنیت در طراحی و رسیدگی مستمر به آسیب‌پذیری‌ها از تبدیل ضعف محصول به مداخله عملی در حریم خصوصی، امنیت شخصی و آزادی رفتاری جلوگیری می‌کند. بدین ترتیب، مقرره تاب‌آوری سایبری در این بخش نه بحثی مستقل درباره محصول، بلکه شرط فنی جلوگیری از تحقق آسیب‌های حقوقی نسبت به فرد است.

۳.۲.۲.۱. ریسک‌های متوجه جامعه (ریسک‌های نظام‌مند)

ریسک‌های نظام‌مند در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء، زمانی پدید می‌آیند که اثر یک فناوری از سطح تصمیم فردی، زیان موردی یا مسئولیت‌سازمانی عبور کند و به دلیل مقیاس، تکرار، تمرکز یا وابستگی متقابل، ساختارهای جمعی را تحت‌تأثیر قرار دهد .در این سطح، مسئله اصلی این نیست که یک شخص مشخص زیان‌دیده یا یک سازمان با مسئولیت حقوقی مواجه شده است؛ بلکه این است که یک الگوی فنی، تصمیم‌گیری الگوریتمی یا آسیب‌پذیری مشترک چگونه می‌تواند در مقیاس وسیع بازتولید شود و بر گفتمان عمومی، بازار، خدمات عمومی، زیرساخت‌های حیاتی یا اعتماد اجتماعی اثر بگذارد .ازاین‌رو، ریسک نظام‌مند را باید ریسک سرایت، انباشت و وابستگی دانست؛ ریسکی که ممکن است از تصمیم‌های کوچک و پراکنده آغاز شود، اما به دلیل تکرار در سامانه‌های توصیه‌گر، مدل‌های هوش مصنوعی، محصولات متصل یا خدمات زیرساختی، پیامد اجتماعی پیدا کند.(Iliopoulou-Penot, 2025)

در این چارچوب، مقرره خدمات دیجیتال ریسک نظام‌مند را از مسیر قدرت توزیع و تقویت پلتفرم‌ها صورت‌بندی می‌کند. پلتفرم‌های بسیار بزرگ برخط و موتورهای جست‌وجوی بسیار بزرگ صرفاً محل انتشار محتوا نیستند؛ آن‌ها با رتبه‌بندی، توصیه، تبلیغ و شخصی‌سازی، تعیین می‌کنند چه محتوایی دیده شود، چه محتوایی تکرار شود و چه الگویی در مقیاس عمومی تقویت گردد؛ بنابراین، مداخله این مقرره صرفاً ناظر به وجود محتوای غیرقانونی یا زیان‌آور نیست؛ بلکه به ظرفیت ساختاری پلتفرم در تکثیر اطلاعات نادرست، تشدید قطبی‌سازی، دست‌کاری افکار عمومی و اثرگذاری بر سلامت عمومی و فرایندهای دموکراتیک مربوط می‌شود .در اینجا، ریسک نظام‌مند از منطق «تقویت الگوریتمی» پدید می‌آید: طراحی سامانه‌های توصیه‌گر و تبلیغاتی می‌تواند محتوایی محدود را به الگوی غالب توجه عمومی تبدیل کند. این وضعیت به‌ویژه هنگامی حساس‌تر می‌شود که شخصی‌سازی محتوا بر داده‌های رفتاری حاصل از دستگاه‌های متصل تکیه کند و تجربه فردی کاربران، به شکل‌گیری الگوهای جمعی مانند حباب‌های اطلاعاتی یا تقویت محتوای افراطی منتهی شود.

قانون هوش مصنوعی، ریسک نظام‌مند را از مسیر دیگری می‌سنجد :وابستگی خدمات عمومی و زیرساخت‌های حیاتی به خروجی سامانه‌های هوش مصنوعی .در اینجا، خطر اصلی گردش محتوا در پلتفرم نیست، بلکه اتکای تصمیم‌های نهادی و زیرساختی به سامانه‌هایی است که ممکن است در مقیاس وسیع خطا کنند، سوگیری را بازتولید کنند یا در برابر حمله و سوءاستفاده تاب‌آوری کافی نداشته باشند .در حوزه‌هایی مانند انرژی، حمل‌ونقل، سلامت، آموزش و زیرساخت‌های دیجیتال، نقص سامانه یا حمله موفق می‌تواند به اختلال خدمات عمومی، تخصیص ناعادلانه منابع یا کاهش اعتماد به تصمیم‌های نهادی منتهی شود. از همین رو، نظام مدیریت ریسک، نظارت انسانی و آزمون‌های استحکام در قانون هوش مصنوعی فقط ابزارهای تضمین کیفیت فنی نیستند؛ بلکه برای جلوگیری از تبدیل خطای الگوریتمی به اختلال اجتماعی یا زیرساختی طراحی شده‌اند .این منطق در سطح مدل‌های هوش مصنوعی باهدف عام شدت بیشتری می‌یابد، زیرا یک مدل واحد می‌تواند در حوزه‌های متعدد به کار رود و خطا، سوگیری یا سوءاستفاده از آن در چند بخش بازتولید شود. به همین دلیل، ارائه‌دهندگان مدل‌های دارای ریسک نظام‌مند باید ارزیابی‌های مستند انجام دهند و هر «حادثه جدی» را به «دفتر هوش مصنوعی» و مراجع ملی گزارش کنند (Palmieri et al., 2024, p. 24).

مقرره تاب‌آوری سایبری با همین مسئله از زاویه شکست مشترک محصول و آسیب‌پذیری تکرارشونده مواجه می‌شود. اگر یک آسیب‌پذیری امنیتی در طیف وسیعی از تجهیزات متصل یا نرم‌افزارهای تعبیه‌شده در زیرساخت‌هایی مانند انرژی، آب، حمل‌ونقل یا خدمات شهری وجود داشته باشد، خطر دیگر به یک محصول منفرد محدود نمی‌ماند؛ بلکه به نقطه شکست مشترک تبدیل می‌شود .در اینجا، ریسک نظام‌مند از وابستگی زیرساخت‌ها به محصولات هم‌نوع و آسیب‌پذیری‌های مشترک ناشی می‌شود؛ بنابراین، الزامات امنیت در طراحی، مدیریت آسیب‌پذیری و به‌روزرسانی امنیتی در مقرره تاب‌آوری سایبری، صرفاً برای حمایت از مصرف‌کننده یا کاهش مسئولیت تولیدکننده نیست؛ بلکه کارکردی زیرساختی دارد و احتمال سرایت نقص فنی به اختلال ملی یا فراملی را کاهش می‌دهد.

مقرره عمومی حفاظت از داده‌ها در این سطح نقشی مکمل اما محدود دارد. این مقرره ابزار اصلی مهار ریسک نظام‌مند پلتفرمی یا زیرساختی نیست، اما ازآن‌جهت اهمیت دارد که بسیاری از ریسک‌های نظام‌مند بر داده‌های گسترده، نامتوازن، آلوده یا فاقد زمینه مناسب بنا می‌شوند .داده ناقص یا تبعیض‌آمیز، هنگامی که در سامانه‌های شهری، آموزشی، سلامت یا خدمات عمومی به کار رود، می‌تواند خطای موردی را به الگوی جمعی نابرابر تبدیل کند؛ بنابراین، اصول دقت، امنیت، پاسخ‌گویی و محدودیت هدف در مقرره عمومی حفاظت از داده‌ها، منشأ داده‌ای برخی ریسک‌های نظام‌مند را کنترل می‌کند، اما جایگزین سازوکارهای خاص مقرره خدمات دیجیتال، قانون هوش مصنوعی یا مقرره تاب‌آوری سایبری نمی‌شود.

دستور موقت رئیس دادگاه عمومی اتحادیه در پرونده آمازون علیه کمیسیون، اهمیت منافع عمومی در اعمال تعهدات شدیدتر بر پلتفرم‌های بسیار بزرگ را نشان می‌دهد (Amazon v Commission, 2023). اهمیت این پرونده در آن است که طبقه‌بندی یک سکوی برخط به‌عنوان پلتفرم بسیار بزرگ، صرفاً تصمیمی اداری یا تجاری نیست؛ بلکه تعیین می‌کند آیا آن پلتفرم باید در برابر آثار اجتماعی خدمات خود، به‌ویژه ریسک‌های نظام‌مند، پاسخ‌گویی شدیدتری داشته باشد یا خیر .براین‌اساس، مدیریت ریسک نظام‌مند مستلزم ترکیب ظرفیت‌های چند مقرره است، اما این ترکیب نباید به معنای وحدت منطق آن‌ها فهمیده شود. مقرره خدمات دیجیتال با تقویت پلتفرمی و آثار عمومی محتوا سروکار دارد؛ قانون هوش مصنوعی با وابستگی زیرساختی به خروجی سامانه؛ مقرره تاب‌آوری سایبری با شکست مشترک محصولات متصل؛ و مقرره عمومی حفاظت از داده‌ها باکیفیت و امنیت داده‌های مبنا .همین تفاوت نشان می‌دهد که ریسک نظام‌مند با یک ابزار واحد مهار نمی‌شود؛ بلکه هر مسیر تولید ریسک باید با معیار خاص همان مسیر سنجیده و سپس در سطح نهادی هماهنگ شود.

۴.۲.۲.۱. ریسک‌های متوجه امنیت ملی

ریسک‌های مرتبط با امنیت ملی در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء را نباید به تهدیدهای کلاسیک امنیتی فروکاست. در این حوزه، امنیت ملی هم‌زمان با تاب‌آوری زیرساخت‌های حیاتی، سلامت فضای اطلاعاتی، اعتماد عمومی به نهادهای حکمرانی و حدود مجاز دسترسی دولت‌ها به داده‌های شهروندان پیوند می‌خورد. ازاین‌رو، مسئله اصلی آن نیست که مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری را ابزارهایی هماهنگ برای امنیت ملی بدانیم؛ بلکه باید نشان داد هر یک از آن‌ها مسیر متفاوتی از تولید یا مهار ریسک امنیتی را پوشش می‌دهد.

در سطح زیرساختی، مقرره تاب‌آوری سایبری از مسیر امنیت محصولات دارای عناصر دیجیتال اهمیت می‌یابد. هنگامی که حسگرها، تجهیزات صنعتی متصل، نرم‌افزارهای تعبیه‌شده و سامانه‌های کنترل در شبکه‌های انرژی، آب، حمل‌ونقل یا خدمات عمومی به کار می‌روند، آسیب‌پذیری مشترک در یک دسته از محصولات می‌تواند از سطح نقص فنی عبور کند و به مسیر اخلال، خرابکاری یا دسترسی غیرمجاز در مقیاس ملی تبدیل شود؛ بنابراین، امنیت در طراحی، مدیریت آسیب‌پذیری و به‌روزرسانی امنیتی، صرفاً ابزار حمایت از مصرف‌کننده نیست؛ بلکه در این سطح، کارکردی زیرساختی و امنیتی پیدا می‌کند.

قانون هوش مصنوعی از زاویه‌ای دیگر وارد می‌شود. مسئله این قانون، امنیت محصول به معنای فنی نیست، بلکه کنترل‌پذیری اتکای نهادهای عمومی به خروجی سامانه‌های هوش مصنوعی است. کاربرد هوش مصنوعی در اجرای قانون، کنترل مرزها، مدیریت مهاجرت، مدیریت بحران یا زیرساخت‌های حیاتی، اگر با خطا، سوگیری، دست‌کاری یا نبود نظارت انسانی همراه باشد، می‌تواند اعتماد عمومی و مشروعیت تصمیم‌های حاکمیتی را تضعیف کند. ازاین‌رو، الزامات شفافیت، مدیریت ریسک، نظارت انسانی و مستندسازی در قانون هوش مصنوعی، برای جلوگیری از واگذاری تصمیم‌های حساس به خروجی‌های غیرشفاف، غیرقابل‌توضیح یا غیرقابل‌اعتراض اهمیت امنیتی پیدا می‌کند.

مقرره خدمات دیجیتال، امنیت ملی را از مسیر تاب‌آوری اطلاعاتی و سلامت فضای عمومی لمس می‌کند. کارزارهای هماهنگ اطلاعاتی، جعل عمیق، تبلیغات هدفمند، تقویت خودکار پیام‌ها و دست‌کاری الگوریتمی جریان محتوا می‌توانند اعتماد عمومی به انتخابات، نهادهای حکمرانی و تصمیم‌های عمومی را تضعیف کنند. در اینجا تهدید امنیتی نه از خرابی محصول و نه از تصمیم اداری منفرد، بلکه از قدرت پلتفرم‌ها در توزیع، تقویت و عادی‌سازی پیام‌ها در مقیاس وسیع ناشی می‌شود. از این منظر، تعهدات مقرره خدمات دیجیتال درباره ارزیابی و کاهش ریسک‌های نظام‌مند، شفافیت تبلیغات و پاسخ‌گویی پلتفرم‌های بسیار بزرگ، می‌تواند در برابر کارزارهای هدفمند اطلاعاتی نقش پیشگیرانه داشته باشد.(Palmieri et al., 2024)

بااین‌حال، استناد به امنیت ملی در حقوق اروپایی مجوز نامحدود برای گردآوری، تحلیل یا انتقال داده نیست. رأی «بیگ برادر واچ» نشان می‌دهد که حتی در حوزه امنیت ملی، شنود گسترده ارتباطات باید با تضمین‌های کافی، نظارت مستقل، محدودیت‌های روشن درباره نگهداری و استفاده از داده، و معیارهای شفاف برای جست‌وجو همراه باشد؛ در غیر این صورت، با مواد ۸ و ۱۰ کنوانسیون اروپایی حقوق بشر ناسازگار خواهد بود (Big Brother Watch and Others v. the United Kingdom, 2021). اهمیت این رأی برای هوش مصنوعی و اینترنت اشیاء در آن است که داده‌های حسگرها، فراداده‌های ارتباطی و الگوهای رفتاری می‌توانند نظارت دولتی را از سطح جمع‌آوری محدود اطلاعات به بازسازی پیوسته زندگی خصوصی شهروندان نزدیک کنند.

رأی «شرمز ۲» همین تنش را در سطح فرامرزی نشان می‌دهد. دیوان دادگستری اتحادیه اروپا، چارچوب «سپر حریم خصوصی» برای انتقال داده به ایالات متحده را به دلیل سطح نامتناسب دسترسی‌های اطلاعاتی و فقدان تضمین‌های کافی برای حقوق اشخاص اروپایی باطل کرد (Case C-311/18, 2020, para. 184). پیام این رأی برای اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء آن است که محل ذخیره‌سازی و پردازش داده، انتخاب زیرساخت ابری و امکان دسترسی دولت ثالث، بخشی از طراحی حقوقی و امنیتی سامانه است، نه مسئله‌ای صرفاً فنی یا قراردادی.

در این چارچوب، مقرره عمومی حفاظت از داده‌ها نقش تعیین کننده قلمرو دارد: نه ابزار عملیات امنیتی است و نه مانع مطلق اقدامات مشروع امنیتی؛ بلکه بهره‌برداری امنیتی از داده را در محدوده مشروعیت، ضرورت، تناسب، امنیت و پاسخ‌گویی نگه می‌دارد. منازعات مربوط به رمزنگاری سرتاسری، نگهداری داده و دسترسی قانونی نهادهای امنیتی دقیقاً در همین نقطه قرار می‌گیرند؛ جایی که کارآمدی امنیتی باید با خطر مداخله نامتناسب در حریم خصوصی و آزادی‌های ارتباطی سنجیده شود.

بنابراین، ریسک‌های مرتبط با امنیت ملی با یک منطق واحد مهار نمی‌شوند. مقرره تاب‌آوری سایبری مسیر تاب‌آوری محصول و زیرساخت را پوشش می‌دهد؛ قانون هوش مصنوعی اتکای نهادی به خروجی سامانه‌های حساس را کنترل‌پذیر می‌کند؛ مقرره خدمات دیجیتال با تهدیدهای اطلاعاتی و دست‌کاری فضای عمومی مواجه می‌شود؛ و مقرره عمومی حفاظت از داده‌ها حدود مداخله داده‌محور و انتقال‌های پرریسک را تعیین می‌کند. نتیجه آن است که امنیت ملی در این حوزه محصول هماهنگی ساده میان چهار مقرره نیست، بلکه حاصل مدیریت حقوقی تنش میان امنیت زیرساخت، قدرت تصمیم‌گیری سامانه‌های هوشمند، سلامت فضای اطلاعاتی و تضمین‌های بنیادین حریم خصوصی و آزادی ارتباطات است.

۳.۱. ارزیابی انتقادی و پیشنهادهای تفسیری و تقنینی

بر پایه بررسی پیشین، ساختار تقنینی اتحادیه اروپا در حوزه حریم خصوصی، هوش مصنوعی و اینترنت اشیاء را باید چارچوبی متکثر با ظرفیت هم‌گرایی محدود دانست، نه مجموعه‌ای کاملاً یکپارچه و بی اصطکاک. مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری، هر یک‌بخشی متفاوت از زنجیره تولید ریسک را پوشش می‌دهند: داده، پلتفرم، سامانه و محصول. ازاین‌رو، نقطه قوت اصلی این چارچوب در آن نیست که همه این مقررات از مفهوم واحدی از ریسک پیروی می‌کنند؛ بلکه در آن است که هرکدام، ریسک را در قلمرو خود به تکالیف قابل‌سنجش تبدیل می‌کند. مقرره عمومی حفاظت از داده‌ها، کنترل‌کننده را باتوجه‌به ماهیت، دامنه، بستر و اهداف پردازش و نیز احتمال و شدت آثار بر حقوق و آزادی‌ها به اتخاذ تدابیر متناسب مکلف می‌سازد .(Gellert, 2018, p. 281) قانون هوش مصنوعی همین منطق پیشگیرانه را در طبقه‌بندی و کنترل سامانه‌های پرخطر دنبال می‌کند و مقرره تاب‌آوری سایبری آن را به سطح امنیت محصول و مدیریت آسیب‌پذیری‌ها منتقل می‌سازد؛ بنابراین، یافته انتقادی نخست این است که مزیت اتحادیه اروپا نه در وحدت مفهومی کامل، بلکه در تبدیل اصول کلی اعتماد، شفافیت، ایمنی و پاسخ‌گویی به ابزارهای اجرایی ارزیابی، مستندسازی، نظارت و کاهش ریسک است؛ نکته‌ای که با نقد ادبیات «هوش مصنوعی قابل‌اعتماد» نسبت به کافی‌نبودن اصول انتزاعی نیز سازگار است.(Floridi, 2019, p. 261)

بااین‌حال، همین نقطه قوت، هم‌زمان منشأ نخستین کاستی ساختاری نیز هست .هم‌گرایی ریسک‌محور در اتحادیه، به معنای وحدت معنای ریسک در چهار متن نیست .ریسک در مقرره عمومی حفاظت از داده‌ها عمدتاً به آثار پردازش بر حقوق و آزادی‌های اشخاص مربوط می‌شود؛ در مقرره خدمات دیجیتال به آثار پلتفرمی و نظام‌مند خدمات برخط؛ در قانون هوش مصنوعی به خروجی سامانه و تأثیر آن بر سلامت، ایمنی و حقوق بنیادین؛ و در مقرره تاب‌آوری سایبری به امنیت محصول و آسیب‌پذیری‌های چرخه عمر آن. ازاین‌رو، مسئله اصلی فقدان مقرره نیست، بلکه پراکندگی معیارهای ارزیابی و احتمال جانشین‌کردن نادرست یک سنجش به‌جای سنجش دیگر است. یک ابزار پوشیدنی، دوربین هوشمند یا سامانه خانگی متصل، ممکن است هم‌زمان موضوع پردازش داده، محصول دارای عناصر دیجیتال، حامل سامانه هوش مصنوعی و بخشی از خدمت برخط باشد؛ اما انطباق در هر سطح با معیار متفاوتی سنجیده می‌شود. این وضعیت می‌تواند برای کنشگران بازار، به‌ویژه بنگاه‌های کوچک و متوسط فعال در اینترنت اشیاء، به مجموعه‌ای از ارزیابی‌های موازی و گاه دشوارفهم تبدیل شود. ابهام مشابهی در ادبیات مقرره عمومی حفاظت از داده‌ها نیز درباره نوسان مفهوم ریسک میان ریسک سازمانی و ریسک متوجه حقوق بنیادین گزارش شده است.(Gellert, 2018, p. 285)

کاستی دوم، به اتکای گسترده بر خودارزیابی و مستندسازی درون‌سازمانی بازمی‌گردد. ابزارهایی مانند ارزیابی تأثیر حفاظت از داده‌ها، ارزیابی اثر بر حقوق بنیادین، ارزیابی ریسک نظام‌مند و ارزیابی امنیت محصول، در ظاهر ظرفیت پیشگیرانه دارند؛ اما اگر با ممیزی مستقل، راهنمای تفسیری دقیق و ظرفیت نهادی کافی همراه نشوند، ممکن است به تشریفات انطباقی بدل شوند .این خطر به‌ویژه در حوزه اینترنت اشیاء جدی است؛ زیرا تولیدکننده یا ارائه‌دهنده خدمت، هم به اطلاعات فنی سامانه دسترسی بیشتری دارد و هم ممکن است انگیزه اقتصادی برای کم‌اهمیت جلوه‌دادن ریسک داشته باشد. در چنین وضعی، تشخیص سطح واقعی ریسک به بازیگری واگذار می‌شود که خود از کاهش هزینه‌های انطباق منتفع است. همین نگرانی در ادبیات مربوط به ارزیابی تأثیر حفاظت از داده‌ها و امکان صوری‌شدن آن نیز مطرح شده است.(Quelle, 2018, p. 508)

کاستی سوم، محدودیت نگاه فردمحور در مواجهه با آسیب‌های جمعی و تدریجی است. داده‌های تولیدشده در خانه هوشمند، محیط کار متصل و شهر هوشمند، صرفاً داده‌هایی درباره یک شخص منفرد نیستند؛ بلکه می‌توانند الگوهای جمعی، روابط قدرت و شیوه‌های نظارت را نیز آشکار کنند . در این زمینه، آسیب ممکن است نه به‌صورت نقض آشکار یک حق فردی، بلکه در قالب عادی‌سازی نظارت، تبعیض ساختاری، کاهش تدریجی انتظار معقول حریم خصوصی یا تغییر رفتار گروهی ظاهر شود .ادبیات مربوط به تبعیض الگوریتمی و حق بر توضیح نیز نشان داده است که اتکای صرف به حقوق فردی، برای شناسایی و مهار همه پیامدهای اجتماعی سامانه‌های الگوریتمی کافی نیست (Edwards & Veale, 2017, p. 60; Wachter et al., 2018, pp. 848, 860). این مشکل در محیط‌های متصل تشدید می‌شود؛ زیرا بسیاری از تصمیم‌ها به شکل تنظیمات محیطی، مانند دسترسی فیزیکی، کنترل روشنایی، مدیریت انرژی، امتیازدهی رفتاری یا تغییر شرایط بیمه و کار ظاهر می‌شوند و آثار حقوقی آن‌ها غیرمستقیم، تدریجی و دشوار اثبات است.

تا اینجا، گزاره‌ها ناظر به ارزیابی انتقادی چارچوب موجود است؛ اما پیشنهادهای این مقاله در دو سطح جداگانه مطرح می‌شوند: نخست، پیشنهادهای تفسیری در چارچوب مقررات موجود؛ دوم، پیشنهادهای تقنینی برای اصلاح آینده .در سطح تفسیری، نخستین راهکار آن است که ارزیابی تأثیر حفاظت از داده‌ها، ارزیابی اثر بر حقوق بنیادین و ارزیابی امنیت سایبری نه در یک فرم واحد و مبهم ادغام شوند و نه کاملاً جدا از یکدیگر اجرا گردند؛ بلکه به‌صورت بسته‌ای هماهنگ اما تفکیک‌شده طراحی شوند. بدین معنا که هر ارزیابی موضوع مستقل خود را حفظ کند، اما خروجی آن برای ارزیابی‌های دیگر قابل‌استفاده باشد. تدوین دستورالعمل مشترک میان هیئت اروپایی حفاظت از داده‌ها، دفتر هوش مصنوعی و آژانس اتحادیه اروپا برای امنیت سایبری می‌تواند بدون تغییر متن قوانین، از تکرار بی‌فایده ارزیابی‌ها و نیز از خلط معیارهای آن‌ها جلوگیری کند؛ پیشنهادی که با نقدهای وارد بر پراکندگی ابزارهای ارزیابی و افزایش هزینه‌های انطباق نیز هم‌خوان است (Quelle, 2018, p. 515).

راهکار تفسیری دوم، توسعه معنای «حقوق و آزادی‌های اشخاص» به‌گونه‌ای است که آسیب‌های جمعی، زمینه‌مند و ساختاری ناشی از سامانه‌های متصل را نیز در بر گیرد. این توسعه به معنای کنارگذاشتن محور فردی نیست؛ بلکه به معنای پذیرش این نکته است که تعرض به حریم خصوصی در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء گاه از مسیر الگوهای جمعی و روابط قدرت رخ می‌دهد. تحلیل‌های نظری درباره حق بر حفاظت از داده نیز نشان داده‌اند که این حق صرفاً به کنترل فرد بر داده‌های خویش فروکاستنی نیست، بلکه با ساختارهای دموکراتیک و توزیع قدرت در فضای دیجیتال پیوند دارد .(Lynskey, 2015, p. 52) در همین راستا، معیار «خطر بالا» در قانون هوش مصنوعی باید به‌صورت زمینه‌محور تفسیر شود؛ به‌گونه‌ای که خانه هوشمند، محیط کار متصل و زیرساخت شهری هوشمند، به سبب تراکم داده، استمرار نظارت و عدم تقارن قدرت، موقعیت‌هایی ذاتاً حساس تلقی شوند، حتی اگر همه کاربردهای خاص آن‌ها در پیوست‌ها تصریح نشده باشد (Veale & Zuiderveen Borgesius, 2021, p. 109).

در سطح تقنینی، پیشنهادها ماهیت متفاوتی دارند و باید به‌عنوان ترجیح سیاستی برای اصلاح آینده فهم شوند، نه نتیجه مستقیم و ضروری از تفسیر متن موجود. نخست، لازم است در بازنگری‌های بعدی، واژگان مشترک اما محدود درباره ریسک، آسیب و آسیب‌پذیری میان مقرره عمومی حفاظت از داده‌ها، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری ایجاد شود. مقصود از این پیشنهاد یکی‌کردن همه معیارها نیست؛ بلکه جلوگیری از آن است که ریسک داده‌ای، ریسک سامانه‌ای و ریسک محصولی به‌جای یکدیگر به کار روند .(Gellert, 2018, p. 285; Quelle, 2018, p. 515) دوم، اینترنت اشیاء به قواعد بخشی دقیق‌تری نیاز دارد؛ زیرا حضور دائمی در فضای خصوصی، تولید پیوسته داده‌های محیطی و اتصال به سامانه‌های هوش مصنوعی، آن را از بسیاری از خدمات دیجیتال کلاسیک متمایز می‌کند. در این زمینه، می‌توان قواعدی مانند فرض حساسیت برای داده‌های تولیدشده در خانه، محدودیت شدیدتر بر پروفایل‌سازی رفتاری در محیط خانگی و ترجیح پردازش محلی برای برخی داده‌ها را پیش‌بینی کرد.(Floridi, 2019, p. 261; Smuha, 2021, p. 4)

سوم، باید تعهدی افقی به پاسخ‌گویی الگوریتمی برای استفاده از سامانه‌های هوش مصنوعی مبتنی بر داده‌های اینترنت اشیاء تقویت شود؛ تعهدی که مستقل از طبقه‌بندی دقیق سامانه، مستندسازی منطق کلی، ثبت خطاها، رسیدگی به شکایات و ارائه اطلاعات معنادار به کاربران را الزام‌آور سازد. مناقشه درباره حق بر توضیح نشان داده است که اتکای صرف به حقوق فردی، بدون تعهدات نهادی مستمر برای ممیزی، اصلاح و توضیح سامانه‌ها کافی نیست .(Wachter et al., 2018, p. 865) چهارم، هیچ اصلاح تقنینی بدون تقویت ظرفیت مراجع حفاظت از داده، نهادهای نظارت بر بازار، دفتر هوش مصنوعی و دسترسی پژوهشگران مستقل به مستندات سامانه‌های پرخطر از سطح متن فراتر نمی‌رود. ادبیات انتقادی درباره قانون هوش مصنوعی نیز هشدار داده است که اعتماد بدون ممیزی مؤثر و ظرفیت نهادی، به شعار تقلیل می‌یابد (Veale & Zuiderveen Borgesius, 2021, p. 110).

در جمع‌بندی، ارزیابی انتقادی نشان می‌دهد که چارچوب اتحادیه اروپا توانسته است حمایت از حریم خصوصی را از سطح کنترل داده فراتر ببرد و آن را به پلتفرم، سامانه و محصول متصل پیوند دهد؛ اما این مزیت تنها زمانی حفظ می‌شود که تفاوت منطق حقوقی این سطوح پنهان نشود .بر همین مبنا، پیشنهادهای تفسیری به دنبال هماهنگ‌سازی ارزیابی‌ها، توسعه فهم حقوق و آزادی‌ها و تفسیر زمینه‌محور خطر بالا در چارچوب موجود است؛ درحالی‌که پیشنهادهای تقنینی ناظر به اصلاح آینده در جهت کاهش ابهام مفهومی، تنظیم خاص اینترنت اشیاء، پاسخ‌گویی الگوریتمی و ممیزی مستقل‌اند.

۲. امکان‌سنجی اعمال الگوی ریسک‌محور اتحادیه اروپا در حمایت از حریم خصوصی در حقوق ایران

در این بخش، امکان کاربست رویکرد ریسک‌محور اتحادیه اروپا در حقوق ایران، با تمرکز بر حمایت از حریم خصوصی در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء، بررسی می‌شود. معیار تحلیل، چهار سطح داده، پلتفرم، سامانه هوش مصنوعی و محصول متصل است و مقررات ایران بر پایه میزان توانایی آن‌ها در پاسخ‌گویی به مخاطرات هر سطح ارزیابی می‌شوند. بر این مبنا، بحث حاضر می‌کوشد میان ظرفیت‌های تفسیری موجود، محدودیت‌های ساختاری قوانین فعلی و ضرورت‌های تقنینی آینده، تفکیکی روشن و قابل‌اتکا برقرار کند.

در امکان‌سنجی اعمال الگوی ریسک‌محور اتحادیه اروپا در حقوق ایران، نقطه عزیمت آن است که حقوق ایران در حوزه داده، حریم خصوصی، هوش مصنوعی و اینترنت اشیاء فاقد یک نظام جامع و یکپارچه است و به‌جای آن، با مجموعه‌ای از منابع پراکنده روبه‌روست: قانون تجارت الکترونیکی ۱۳۸۲ به‌عنوان نخستین متن صریح درباره داده‌های شخصی در بستر مبادلات و خدمات الکترونیکی؛ قانون جرائم رایانه‌ای ۱۳۸۸ به‌عنوان لایه کیفری حمایت از محرمانگی، تمامیت و دسترسی مجاز به داده و سامانه؛ آیین‌نامه‌های ناظر بر دفاتر خدمات حضوری اینترنت و واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت به‌عنوان مقررات اداری ناظر بر برخی بازیگران زیرساختی؛ و قواعد مسئولیت مدنی و قراردادی که پس از ورود زیان یا نقض تعهد مراقبت، امکان جبران خسارت یا انتساب مسئولیت را فراهم می‌سازند. این متون با فرض صریح هوش مصنوعی یا اینترنت اشیاء تدوین نشده‌اند، اما در عمل بر گردآوری، پردازش، انتقال، افشا و حفاظت از داده در سامانه‌های مبتنی بر هوش مصنوعی متکی بر دستگاه‌های متصل اثر می‌گذارند. ازاین‌رو، تحلیل حقوق ایران نباید بر شباهت لفظی مفاهیمی مانند «داده‌پیام»، «داده رایانه‌ای» یا «سامانه رایانه‌ای» با فناوری‌های نوظهور متوقف شود؛ بلکه باید از منظر امکان‌سنجی کارکردی بررسی کند هر متن ایرانی در نسبت با چهار سطح الگوی اتحادیه اروپا، یعنی داده، پلتفرم، سامانه هوش مصنوعی و محصول متصل، چه ظرفیتی دارد، در کجا متوقف می‌شود و کدام بخش بدون تقنین مستقل قابل‌جبران نیست.

در این چارچوب، قانون تجارت الکترونیکی ۱۳۸۲ را باید عمدتاً در سطح «داده» جای داد، و کمتر قابلیت جاگیری در سطح پلتفرم، سامانه هوش مصنوعی یا محصول متصل را داراست. در الگوی اتحادیه اروپا، سطح داده با مشروعیت پردازش، محدودیت هدف، کمینه‌سازی، شفافیت، امنیت، حقوق اشخاص، پاسخ‌گویی و ارزیابی قبلی آثار پردازش پیوند دارد. قانون تجارت الکترونیکی، باوجود تقدم زمانی بر مباحث امروزین هوش مصنوعی و اینترنت اشیاء، نخستین متن تقنینی ایران است که به طور صریح از داده‌های شخصی در محیط دیجیتال سخن گفته و در مواد ۵۸ و ۵۹، مؤلفه‌هایی مانند رضایت، حساسیت برخی داده‌ها، هدفمندی، تناسب، صحت، دسترسی و امکان اصلاح یا حذف داده را شناسایی کرده است (نیسی و مدحج، ۱۳۹۰، ص. ۵؛ احمدی ناطور و آقابابایی، ۱۳۹۵، ص. ۱۴–۱۵). ارزش تحلیلی این قانون در آن است که نشان می‌دهد حقوق ایران ظرفیت اولیه‌ای برای پذیرش بخشی از منطق حمایت داده‌ای دارد؛ ظرفیتی که البته محدود، بخشی و وابسته به قلمرو «مبادلات و خدمات الکترونیکی» است. به همین دلیل، نمی‌توان مواد ۵۸ و ۵۹ را بدون مبنای تفسیری روشن به همه داده‌های تولیدشده در خانه هوشمند، ابزار پوشیدنی، حسگر شهری یا محصول متصل تسری داد. ملاک اعمال قانون تجارت الکترونیکی، صرف تولید داده به‌وسیله ابزار متصل نیست، بلکه وجود رابطه‌ای حقوقی است که بتوان آن را در قلمرو خدمت، مبادله یا تعامل الکترونیکی قرارداد. برای نمونه، اگر ابزار پوشیدنی در قالب خدمتی مستمر برای پایش سلامت، مدیریت فعالیت بدنی یا ارائه توصیه‌های شخصی، داده را به عرضه‌کننده خدمت منتقل کند، تحلیل مواد ۵۸ و ۵۹ قابل‌طرح است؛ اما اگر داده در محیط خانگی یا شهری تولید شود و نسبت آن با خدمت الکترونیکی، قرارداد مصرف‌کننده یا مبادله دیجیتال روشن نباشد، اعمال مستقیم قانون تجارت الکترونیکی با قلمرو خاص آن سازگار نیست. به بیان دقیق‌تر، این قانون فقط زمانی می‌تواند وارد اکوسیستم اینترنت اشیاء شود که «اتصال فنی» به «رابطه حقوقی الکترونیکی» تبدیل شده باشد.

این محدودسازی بر چند مبنای حقوقی استوار است. نخست، اصل حاکمیت اراده اقتضا دارد حدود رابطه قراردادی میان کاربر و ارائه‌دهنده خدمت روشن باشد؛ حال‌آنکه در خدمات متصل، اراده کاربر غالباً از مسیر شروط الحاقی، تنظیمات پیش‌فرض و پذیرش سریع شرایط استفاده ابراز می‌شود و اتکای صرف به چنین رضایتی، بدون توجه به عدم توازن اطلاعاتی و فنی، می‌تواند به مشروع‌نمایی پردازش‌های گسترده بینجامد. دوم، قواعد حمایت مصرف‌کننده اقتضا دارد رضایت، اطلاع‌رسانی و انتخاب کاربر واقعی و قابل‌فهم باشد، نه اینکه صرفاً در قالب عباراتی طولانی و غیرقابل‌مذاکره درج شود. سوم، صلاحیت نهادهای تخصصی در حوزه‌هایی مانند ارتباطات، سلامت، بیمه، حمل‌ونقل یا خدمات شهری ممکن است برخی پردازش‌های داده‌ای را تابع قواعد بخشی سخت‌گیرانه‌تر کند؛ بنابراین، قانون تجارت الکترونیکی فقط با سه قید قابل اتکاست: وجود رابطه الکترونیکی، رعایت حمایت مصرف‌کننده، و عدم تزاحم با صلاحیت‌های تنظیم‌گرانه تخصصی. افزون بر این، اصول بالادستی حقوق ایران نیز جهت تفسیری مهمی فراهم می‌کنند؛ زیرا داده شخصی در محیط دیجیتال صرفاً موضوع مبادله نیست، بلکه باحیثیت، حریم خصوصی، اختیار اطلاعاتی و امنیت ارتباطی اشخاص پیوند دارد. اصول مربوط به مصونیت حیثیت، حقوق اشخاص و مصونیت مکاتبات و ارتباطات، به‌ویژه اصول ۲۲ و ۲۵ قانون اساسی، اقتضا دارند حتی اگر پردازش داده در قالب رابطه قراردادی یا خدمت الکترونیکی انجام شود، مداخله در داده‌های شخصی از حیث ضرورت، تناسب، شفافیت، حدود رضایت و منع تعرض ناموجه سنجیده شود. این اصول جای قانون جامع حمایت از داده را نمی‌گیرند، اما مانع می‌شوند قانون تجارت الکترونیکی به ابزاری صرفاً قراردادی برای مشروع‌سازی گردآوری گسترده داده تبدیل شود. مسئولیت مدنی و قراردادی نیز در همین نقطه نقش مکمل دارد؛ زیرا بسیاری از آسیب‌های داده‌محور در اینترنت اشیاء جرم نیستند، بلکه از نقص اطلاع‌رسانی، ضعف امنیت، نقض تعهد مراقبت، شروط ناعادلانه یا کاستی فنی سامانه پدید می‌آیند.

ماده ۵۸ قانون تجارت الکترونیکی، ذخیره، پردازش و توزیع پیام داده‌های شخصی دارای ماهیت حساس، مانند داده‌های مربوط به ریشه‌های قومی یا نژادی، عقاید دینی، ویژگی‌های اخلاقی و وضعیت جسمانی، روانی یا جنسی را بدون رضایت صریح ممنوع کرده و برای آن ضمانت اجرای کیفری مقرر می‌کند (احمدی ناطور و آقابابایی، ۱۳۹۵، ص. ۱۴). هسته هنجاری این ماده، شناسایی حساسیت برخی داده‌ها و لزوم رضایت صریح برای پردازش آن‌هاست؛ اما همین ضمانت اجرای کیفری، دامنه اعمال آن را محدود می‌سازد. اصل قانونی‌بودن جرم و مجازات و منع تفسیر موسع به زیان متهم اقتضا دارد ماده فقط نسبت به داده‌ها و رفتارهایی اعمال شود که با الفاظ و ارکان قانونی آن منطبق‌اند. براین‌اساس، باید میان سه وضعیت تمایز گذاشت: نخست، داده‌ای که خود به طور مستقیم در یکی از دسته‌های حساس ماده ۵۸ قرار می‌گیرد؛ مانند داده صریح سلامت جسمانی یا روانی. دوم، داده‌ای که در ظاهر عادی است، اما در ترکیب با داده‌های دیگر می‌تواند نشانه‌ای از وضعیت حساس شخص ایجاد کند؛ مانند الگوی خواب، مصرف انرژی، رفت‌وآمد یا رفتار خانگی. سوم، استنباطی که سامانه هوش مصنوعی از داده‌های عادی استخراج می‌کند؛ مانند برآورد وضعیت روانی، احتمال بیماری یا آسیب‌پذیری رفتاری. ماده ۵۸ در قلمرو کیفری، با اطمینان فقط در وضعیت نخست و در صورت تحقق رفتارهای منصوص، مانند ذخیره، پردازش یا توزیع غیرمجاز، قابل‌اعمال است. دو وضعیت دیگر، یعنی داده‌های قابل‌ترکیب و استنباط‌های الگوریتمی، بیش از آنکه با تفسیر کیفری قابل‌حل باشند، خلأ قانون جامع داده و قواعد خاص پردازش استنباطی را آشکار می‌کنند. این تفکیک، هم از توسعه بی‌ضابطه حقوق کیفری جلوگیری می‌کند و هم نشان می‌دهد کدام بخش از الگوی داده‌محور اتحادیه اروپا در حقوق ایران فاقد معادل کافی است.

ماده ۵۹ نیز در فرض وجود رضایت، پردازش داده‌های شخصی را به شرایطی مقید می‌کند که می‌توان آن‌ها را بازتاب هدفمندی، تناسب، کمینه‌سازی، صحت، روزآمدی، حق دسترسی و حق اصلاح یا محو دانست (احمدی ناطور و آقابابایی، ۱۳۹۵، ص. ۱۵). اهمیت ماده در آن است که پردازش داده را پس از اخذ رضایت، نامحدود و رها نمی‌گذارد. بااین‌حال، در محیط‌های هوش مصنوعی و اینترنت اشیاء، رضایت غالباً در فضایی نامتقارن اخذ می‌شود: کاربر ابزار متصل را برای استفاده روزمره می‌پذیرد، اما معمولاً از دامنه پردازش، انتقال داده به اشخاص ثالث، تحلیل ابری، ترکیب داده‌ها یا استنباط‌های ثانویه آگاهی کافی ندارد؛ بنابراین، رضایت موضوع ماده ۵۹ باید در پرتو حمایت مصرف‌کننده، تعهدات قراردادی ارائه‌دهنده خدمت و اصل شفافیت هدف پردازش خوانده شود. رضایت معتبر در این حوزه صرف پذیرش ظاهری شرایط استفاده نیست؛ بلکه باید با اطلاع‌رسانی قابل‌فهم، امکان انتخاب معنادار و پرهیز از پردازش فراتر از ضرورت همراه باشد. از منظر امکان‌سنجی، ماده ۵۹ ظرفیت آن را دارد که در روابط الکترونیکی متکی بر ابزار متصل، پرسش‌های اصلی سطح داده را فعال کند: هدف پردازش چیست؟ داده تا چه حد برای آن هدف لازم است؟ کاربر چه میزان از پردازش را می‌فهمد؟ آیا داده صحیح و قابل‌اصلاح است؟ آیا امکان حذف یا توقف پردازش وجود دارد؟ بااین‌حال، همین ماده، در مقایسه با سطح داده در الگوی اتحادیه اروپا، فاقد چند سازوکار اساسی است: ارزیابی تأثیر بر حفاظت از داده را پیش‌بینی نمی‌کند؛ نهاد مستقل ناظر ایجاد نمی‌کند؛ امنیت پردازش و پاسخ‌گویی قابل ممیزی را به‌صورت نظام‌مند مقرر نمی‌سازد؛ و درباره انتقال داده به اشخاص ثالث، پردازش ابری، پروفایل‌سازی رفتاری و استنباط الگوریتمی حکم تفصیلی ندارد. در نتیجه، ماده ۵۹ می‌تواند زبان اولیه حمایت از داده را وارد تحلیل حقوق ایران کند، اما نمی‌تواند به‌تنهایی منطق پیشگیرانه و ریسک‌محور سطح داده در اتحادیه اروپا را بازتولید کند.

مواد ۶۴ و ۷۵ قانون تجارت الکترونیکی با جرم‌انگاری تحصیل غیرقانونی و افشای اسرار تجاری و اقتصادی، بیشتر بر محرمانگی اقتصادی و تجاری تمرکز دارند تا حمایت جامع از داده‌های شخصی. در مقابل، ماده ۷۸ از حیث امکان‌سنجی اهمیت بیشتری دارد؛ زیرا با پذیرش مسئولیت مؤسسات در قبال خسارات ناشی از نقص یا ضعف دستگاه، مسیر تحلیل مسئولیت مدنی و قراردادی را در کنار قانون تجارت الکترونیکی باز می‌کند (عامل نجف‌آبادی، ۱۳۸۷، ص. ۵۲). اگر ضعف سامانه، نقص اطلاع‌رسانی، کاستی امنیت یا نقض تعهد مراقبت حرفه‌ای موجب افشای داده یا ورود زیان شود، ماده ۷۸ می‌تواند در کنار قواعد عمومی مسئولیت مدنی و تعهدات قراردادی به کار آید. بااین‌حال، این ماده نیز عمدتاً پسینی است و پس از وقوع خسارت عمل می‌کند؛ قواعدی مانند امنیت در طراحی، امنیت پیش‌فرض، مدیریت آسیب‌پذیری، به‌روزرسانی امنیتی و نظارت بازار محصولات متصل را ایجاد نمی‌کند؛ بنابراین، نسبت آن با مقرره تاب‌آوری سایبری اتحادیه اروپا روشن است: قانون تجارت الکترونیکی امکان جبران و انتساب مسئولیت را تا حدی تقویت می‌کند، اما چارچوب پیشگیرانه امنیت محصول متصل را نمی‌سازد. بر پایه معیار چهارسطحی اتحادیه اروپا، قانون تجارت الکترونیکی فقط در سطح داده، آن هم به‌صورت محدود و مشروط، قابلیت استفاده دارد. در سطح پلتفرم، تکالیفی مانند شفافیت سامانه‌های توصیه‌گر، محدودیت هدف‌گیری تبلیغاتی، ارزیابی ریسک‌های نظام‌مند، امکان اعتراض کاربر یا دسترسی پژوهشگران به داده‌های پلتفرم را مقرر نمی‌کند؛ در سطح سامانه هوش مصنوعی، از طبقه‌بندی ریسک، حاکمیت داده آموزشی، مستندسازی فنی، نظارت انسانی یا ارزیابی اثر بر حقوق بنیادین سخنی نمی‌گوید؛ و در سطح محصول متصل نیز امنیت در طراحی، مدیریت آسیب‌پذیری، به‌روزرسانی امنیتی و نظارت بازار را به‌عنوان تکلیف مستقل تولیدکننده نمی‌شناسد؛ بنابراین، نسبت این قانون با الگوی اتحادیه اروپا، نسبت جانشینی یا انتقال کامل نیست؛ نسبت امکان‌سنجی محدود در یکی از چهار سطح است. این قانون را نه باید کنار گذاشت و نه بیش از ظرفیت آن توسعه داد: قانون تجارت الکترونیکی نقطه شروعی محدود برای رضایت، هدفمندی، تناسب، صحت، دسترسی، اصلاح و مسئولیت ناشی از ضعف دستگاه فراهم می‌کند، اما اعمال آن بر اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء فقط با سه قید قابل‌دفاع

است: وجود پیوند روشن با خدمت یا مبادله الکترونیکی؛ رعایت حدود تفسیر، به‌ویژه در ماده ۵۸ به سبب ماهیت کیفری آن؛ و تکمیل آن با اصول بالادستی، قواعد مسئولیت مدنی، مسئولیت قراردادی، حمایت مصرف‌کننده و اصلاحات تقنینی خاص.

قانون جرائم رایانه‌ای ۱۳۸۸ را نیز باید در جایگاه یک‌لایه کیفری محدود و پسینی فهم کرد، نه به‌عنوان چارچوب عام حکمرانی داده، پلتفرم، سامانه هوش مصنوعی یا محصول متصل. در الگوی اتحادیه اروپا، مخاطرات در چهار سطح داده، پلتفرم، سامانه و محصول سامان می‌یابند؛ اما قانون جرائم رایانه‌ای با هیچ‌یک از این سطوح به‌صورت کامل منطبق نیست. ظرفیت آن عمدتاً جایی ظاهر می‌شود که تعرضی مشخص و منصوص علیه محرمانگی، تمامیت، صحت یا دسترسی مجاز به داده و سامانه رخ‌داده باشد. ازاین‌رو، این قانون می‌تواند در برابر بخشی از حملات و تعرض‌های رایانه‌ای نقش ایفا کند، اما جایگزین قواعد پیشینی و نهادی الگوی اتحادیه اروپا نیست (زرکلام، ۱۳۸۶، ص. ۱۷۷). نخستین شرط امکان‌سنجی آن، تفکیک سناریوهای ریسک است. همه آسیب‌های هوش مصنوعی و اینترنت اشیاء منشأ کیفری ندارند. اگر شخص ثالث به دوربین خانگی، ابزار پوشیدنی، خودرو متصل یا سامانه ابری نفوذ کند، شنود غیرمجاز انجام دهد، داده را دست‌کاری کند یا تصویر و صدای خصوصی را بدون مجوز منتشر سازد، با سناریوی حمله ثالث و رفتار مجرمانه منصوص مواجهیم و قانون جرائم رایانه‌ای می‌تواند فعال شود. اما اگر زیان ناشی از نقص طراحی یا ضعف امنیت محصول باشد، مانند نبود امنیت پیش‌فرض، فقدان به‌روزرسانی یا ضعف مدیریت آسیب‌پذیری، موضوع به سطح «محصول متصل» و منطق مقرره تاب‌آوری سایبری نزدیک است، نه به حقوق کیفری. در حقوق ایران نیز چنین وضعیتی بیشتر باید از منظر مسئولیت مدنی، قراردادی، حمایت مصرف‌کننده و تنظیم‌گری اداری تحلیل شود. همچنین اگر زیان ناشی از پردازش مشروع اما پرخطر، رضایت صوری، پروفایل‌سازی یا تصمیم الگوریتمی تبعیض‌آمیز باشد، موضوع به سطح داده یا سامانه هوش مصنوعی مربوط است و قانون جرائم رایانه‌ای، جز در فرض تحقق عنوان مجرمانه مستقل، ابزار کافی ندارد.

ماده ۱ قانون جرائم رایانه‌ای با جرم‌انگاری دسترسی غیرمجاز، از محرمانگی داده و سامانه حمایت می‌کند. در محیط اینترنت اشیاء، این ماده می‌تواند نسبت به نفوذ به دوربین خانگی، قفل هوشمند، حساب کاربری ابزار پوشیدنی یا سامانه کنترل خودرو مطرح شود. بااین‌حال، ملاک اعمال ماده، «متصل بودن» دستگاه نیست، بلکه تحقق دسترسی غیرمجاز به داده یا سامانه است. اگر مهاجم از آسیب‌پذیری یک محصول متصل برای ورود به سامانه استفاده کند، رفتار مهاجم ممکن است ذیل ماده ۱ قرار گیرد؛ اما مسئولیت تولیدکننده بابت عرضه محصول ناایمن از همین ماده به دست نمی‌آید. این تفکیک اهمیت اساسی دارد: ماده ۱ فقط با لحظه تعرض کیفری سروکار دارد، درحالی‌که مقرره تاب‌آوری سایبری بر پیشگیری، امنیت در طراحی، مدیریت آسیب‌پذیری و به‌روزرسانی در سراسر چرخه عمر محصول تمرکز می‌کند. ماده ۲ نیز درباره شنود غیرمجاز داده‌های در حال انتقال در محیط‌های متصل ظرفیت مشخصی دارد. شنود ترافیک شبکه خانه هوشمند، رهگیری داده‌های سلامت در مسیر انتقال یا پایش پنهانی ارتباط میان حسگر و سرور ابری، در صورت تحقق ارکان قانونی، می‌تواند ذیل این ماده بررسی شود. بااین‌حال، هر نوع پردازش یا تحلیل جریان داده شنود غیرمجاز نیست. اگر ارائه‌دهنده خدمت داده را در چارچوب قرارداد یا رضایت کاربر پردازش کند، مسئله اصلی ممکن است شفافیت، تناسب، محدودیت هدف یا سوءاستفاده از داده باشد؛ وضعیتی که در الگوی اتحادیه اروپا به سطح داده نزدیک‌تر است، نه به جرم شنود؛ بنابراین، ماده ۲ فقط در برابر رهگیری غیرمجاز ارتباطات کارکرد دارد و نمی‌تواند همه پردازش‌های غیرشفاف یا پرخطر را پوشش دهد.

مواد ۳ تا ۵ درباره داده‌های سری و مسئولیت مرتبط با آن‌ها، از حیث حمایت کیفری از امنیت اطلاعات اهمیت دارند؛ اما نباید به مبنای عام حمایت از همه داده‌های حساس در اینترنت اشیاء تبدیل شوند. «داده سری» در این مواد مفهومی خاص، امنیتی و کیفری دارد و با داده شخصی حساس یا داده حیاتی حاصل از سامانه‌های هوشمند یکی نیست. داده سلامت، مکانی، زیستی یا رفتاری ممکن است از منظر حریم خصوصی مهم باشد، اما تا زمانی که با مفهوم قانونی داده سری منطبق نباشد، نمی‌توان حمایت شدیدتر مواد ۳ تا ۵ را به آن تسری داد. اینجا فاصله حقوق ایران با سطح داده در الگوی اتحادیه اروپا آشکار می‌شود: حقوق ایران در این بخش از شدت حمایت امنیتی سخن می‌گوید، اما میان حساسیت حریم خصوصی، داده‌های استنباطی و داده‌های سری، طبقه‌بندی داده‌محور منسجم ندارد. مواد ۶ و ۷ درباره جعل رایانه‌ای و استفاده از داده مجعول نیز در سناریوهایی مانند دست‌کاری متقلبانه داده حسگر، تغییر داده ثبت‌شده یا تولید ورودی جعلی برای اثرگذاری بر تصمیم سامانه اهمیت دارند. اگر داده حسگر در سامانه بیمه، کنترل صنعتی یا مدیریت دسترسی به‌گونه‌ای تغییر داده شود که حقیقت دیجیتال قلب گردد و ضرر ایجاد شود، تحلیل جعل رایانه‌ای قابل‌طرح است. اما خطای مدل، سوگیری داده آموزشی، ضعف آزمون سامانه یا تصمیم نادرست الگوریتمی را نمی‌توان صرفاً به دلیل زیان‌بار بودن، جعل رایانه‌ای دانست. جعل مستلزم رفتار متقلبانه و انطباق با ارکان قانونی است، درحالی‌که بسیاری از خطاهای هوش مصنوعی به سطح سامانه مربوط‌اند و باید با قواعدی مانند حاکمیت داده، مستندسازی، آزمون، نظارت انسانی و ارزیابی اثر بر حقوق بنیادین کنترل شوند.

مواد ۱۶ و ۱۷ که تغییر، تحریف یا انتشار فیلم، صوت، تصویر یا اسرار خصوصی دیگری را بدون رضایت جرم‌انگاری می‌کنند، نزدیک‌ترین نقطه قانون جرائم رایانه‌ای به حمایت کیفری از حریم خصوصی شخصی‌اند (بابایی، ۱۳۹۸، ص. ۱۳۲). در محیط‌های متصل، این مواد می‌توانند نسبت به انتشار تصویر ضبط‌شده توسط دوربین خانگی، افشای صدای خصوصی یا دست‌کاری و انتشار محتوای منتسب به شخص، از جمله برخی مصادیق دیپ‌فیک، اهمیت یابند. بااین‌حال، کارکرد آن‌ها واکنشی و موردی است. از این مواد قواعدی مانند برچسب‌گذاری محتوای مصنوعی، تشخیص منشأ، حذف نسخه‌های اساساً معادل، مسئولیت پلتفرم برای بازنشر یا ارزیابی ریسک نظام‌مند به دست نمی‌آید. ازاین‌جهت، قانون جرائم رایانه‌ای با سطح پلتفرمی الگوی اتحادیه اروپا فاصله دارد؛ زیرا مقرره خدمات دیجیتال مسئله را فقط در سطح انتشار منفرد نمی‌بیند، بلکه به قدرت پلتفرم در بازنشر، توصیه، دسترس‌پذیری و مدیریت ریسک‌های نظام‌مند توجه می‌کند. بندهای «الف» و «ب» ماده ۲۵ نیز با جرم‌انگاری تولید، انتشار، توزیع، معامله یا در دسترس قراردادن داده‌ها، گذرواژه‌ها یا ابزارهای تسهیل‌کننده دسترسی غیرمجاز، برای مهار بازار ابزارهای نفوذ به سامانه‌های متصل اهمیت دارند (جلالی فراهانی، ۱۳۸۶، ص. ۶۹). این ماده می‌تواند نسبت به فروش گذرواژه‌های سرقت‌شده، انتشار ابزار نفوذ به دوربین‌های خانگی یا توزیع داده‌های دسترسی به سامانه‌های متصل کاربرد داشته باشد؛ اما نباید به ابزار عام کنترل همه نرم‌افزارها یا ابزارهای فنی تبدیل شود. بسیاری از ابزارهای امنیت سایبری دو کاربردی‌اند و ممکن است برای آزمون امنیت، پژوهش آسیب‌پذیری یا ارزیابی مقاومت سامانه استفاده شوند. ازاین‌رو، اعمال ماده ۲۵ باید بر تسهیل دسترسی غیرمجاز و تحقق عناصر مجرمانه متمرکز بماند؛ در غیر این صورت، تفسیر موسع کیفری می‌تواند پژوهش مشروع امنیتی را نیز با خطر کیفری مواجه کند. مواد ۲۸ تا ۳۱ درباره صلاحیت کیفری نیز امکان نظری تعقیب برخی رفتارهای فرامرزی را فراهم می‌کنند، اما ظرفیت صلاحیتی به‌تنهایی معادل کارآمدی اجرایی نیست. بسیاری از تعرض‌های مرتبط با اینترنت اشیاء از طریق زیرساخت ابری، ارائه‌دهندگان خارجی، پلتفرم‌های برون‌مرزی یا زنجیره‌های ناشناس انجام می‌شود. قانون جرائم رایانه‌ای می‌تواند در برخی موارد مبنای صلاحیت کیفری فراهم کند، اما ابزارهایی مانند نگهداری

فوری ادله دیجیتال، دسترسی زمان‌مند به داده، همکاری ساختاریافته با پلتفرم‌ها، حذف نسخه‌های اساساً معادل، ممیزی مستقل یا دسترسی پژوهشگران را پیش‌بینی نمی‌کند؛ بنابراین، این مواد امکان تعقیب را گسترش می‌دهند، اما سازوکار تنظیم‌گری اجرایی یا پلتفرمی برای مدیریت ریسک‌های فرامرزی ایجاد نمی‌کنند.

بر پایه معیار چهارسطحی اتحادیه اروپا، قانون جرائم رایانه‌ای فقط در بخشی از سطح داده و سامانه، آن هم از زاویه تعرض کیفری، قابل‌استفاده است. در سطح داده، نسبت به دسترسی، شنود، افشا، جعل یا تغییر غیرمجاز واکنش نشان می‌دهد، اما مشروعیت پردازش، کمینه‌سازی، شفافیت، حقوق اشخاص و ارزیابی اثر را تنظیم نمی‌کند. در سطح پلتفرم، شفافیت توصیه‌گرها، هدف‌گیری تبلیغاتی، ارزیابی ریسک نظام‌مند، اعتراض کاربر و دسترسی پژوهشگران را نمی‌شناسد. در سطح سامانه هوش مصنوعی، طبقه‌بندی ریسک، حاکمیت داده، مستندسازی، نظارت انسانی و ارزیابی اثر بر حقوق بنیادین را مقرر نمی‌کند. در سطح محصول متصل نیز امنیت در طراحی، مدیریت آسیب‌پذیری، به‌روزرسانی و نظارت بازار را بر تولیدکننده تحمیل نمی‌سازد؛ بنابراین، نسبت این قانون با الگوی اتحادیه اروپا، نسبت امکان‌سنجی کیفری در برابر بخشی از تعرض‌های منصوص به داده و سامانه است. نتیجه آن است که قانون جرائم رایانه‌ای در حمایت از حریم خصوصی داده‌محور نقشی مکمل دارد، اما این نقش به سناریوهای معین محدود است: حمله ثالث، نفوذ، شنود، جعل، دست‌کاری و افشای غیرمجاز. در مقابل، نقص طراحی یا امنیت محصول، خطای کاربر، پردازش مشروع اما پرخطر، تصمیم الگوریتمی آسیب‌زا و ریسک‌های نظام‌مند پلتفرمی را نباید با توسعه عناوین کیفری حل کرد. در سناریوی نقص محصول، مسیر اصلی مسئولیت مدنی، قراردادی، حمایت مصرف‌کننده و تنظیم‌گری اداری است؛ در سناریوی پردازش پرخطر، خلأ قانون جامع داده آشکار می‌شود؛ در سناریوی تصمیم الگوریتمی، نیاز به شفافیت، نظارت انسانی و ارزیابی اثر بر حقوق بنیادین وجود دارد؛ و در سناریوی پلتفرمی، فقدان مقررات هم‌تراز با مقرره خدمات دیجیتال برجسته می‌شود. بدین ترتیب، امکان‌سنجی اعمال قانون جرائم رایانه‌ای فقط با دو قید قابل‌دفاع است: تحقق دقیق عنوان مجرمانه منصوص و تفکیک روشن میان حوزه کیفری، مدنی، قراردادی و اداری.

آیین‌نامه‌های ناظر بر دفاتر خدمات حضوری اینترنت و واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت را نیز نباید «ستون سوم» حکمرانی داده تلقی کرد. این مقررات، از حیث مرتبه هنجاری و قلمرو موضوعی، نه جای قانون جامع حمایت از داده‌های شخصی را می‌گیرند، نه با مقررات پلتفرمی اتحادیه اروپا هم‌سنخ‌اند، نه الزامات سامانه‌های هوش مصنوعی را مقرر می‌کنند و نه چارچوبی برای امنیت چرخه عمر محصولات متصل می‌سازند. جایگاه دقیق آن‌ها، تنظیم اداری رفتار برخی بازیگران زیرساختی است؛ یعنی اشخاص و واحدهایی که به سبب موقعیت فنی خود، در نقطه تماس کاربر با شبکه قرار می‌گیرند و امکان دسترسی، مشاهده، انتقال یا اثرگذاری بر جریان داده را دارند. ارزش این مقررات در آن است که برای بخشی از قدرت زیرساختیِ دسترسی به داده، حداقل‌هایی از منع اداری و انتظامی پیش‌بینی شده است (نکونام، ۱۴۰۳، ص. ۲۹). هسته هنجاری آن‌ها را می‌توان در تبدیل «دسترسی فنی» به «تعهد حقوقی خودداری» خلاصه کرد: بازیگر زیرساختی ممکن است توانایی مشاهده بسته‌های اطلاعاتی، دسترسی به رمزها، شناسایی روابط ارتباطی یا بهره‌برداری از ترافیک را داشته باشد، اما همین توان فنی نباید به مجوز بهره‌برداری از داده تبدیل شود. ممنوعیت افشای روابط خصوصی، تعرض به حریم اطلاعات شخصی، انتشار کلیدهای رمز، ارائه روش‌های شکستن رمز، نفوذ غیرمجاز و شنود یا بررسی بسته‌های اطلاعاتی دیگران، صورت‌بندی اداری این اصل است که ارائه‌دهنده خدمت اینترنتی باید از تبدیل امکان فنی مشاهده و عبور داده به قدرت نامحدود بر داده‌های کاربران منع شود (نکونام، ۱۴۰۳، ص. ۳۰). اهمیت این قاعده در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء بیشتر می‌شود؛ زیرا داده‌های ابزارهای متصل، غالباً عادی و منفرد به نظر می‌رسند، اما از رهگذر عبور مستمر از شبکه می‌توانند به الگوهای رفتاری، مکانی، خانگی، زیستی یا مصرفی تبدیل شوند. مشاهده ترافیک خانه هوشمند ممکن است بدون دسترسی مستقیم به محتوای مکالمات، زمان حضوروغیاب، الگوی خواب، استفاده از وسایل خانگی یا حتی وضعیت سلامت کاربر را آشکار کند؛ بنابراین، ممنوعیت شنود، بررسی بسته‌های اطلاعاتی و افشای روابط خصوصی، در سطح زیرساخت ارتباطی نقشی پیشگیرانه دارد؛ اما این پیشگیری فقط ناظر به سوءاستفاده از موقعیت ارتباطی است و درباره مشروعیت پردازش،

محدودیت هدف، کمینه‌سازی، ارزیابی اثر، حقوق اشخاص و پاسخ‌گویی قابل ممیزی نظام مستقلی ایجاد نمی‌کند.

آیین‌نامه ناظر بر واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت نیز با تأکید بر مصونیت حریم خصوصی کاربران، شنود، افشا یا بررسی بسته‌های اطلاعاتی بدون مجوز قانونی، تلاش برای شکستن قفل رمز دستگاه‌ها و نفوذ غیرمجاز به مراکز داده را تخلف اداری می‌داند و ضمانت اجراهایی از تذکر تا لغو پروانه و ارجاع به مرجع قضایی پیش‌بینی می‌کند (قاسم‌زاده لیاسی و رئیسی، ۱۳۹۹، ص. ۶۰۵). این ضمانت اجراها نشان می‌دهد که حمایت از حریم خصوصی در این سطح نه از طریق اعطای حقوق تفصیلی به کاربر، بلکه از مسیر کنترل مجوز، صلاحیت حرفه‌ای و استمرار فعالیت ارائه‌دهنده خدمت دنبال می‌شود. بااین‌حال، همین نقطه قوت، حدّ این مقررات را نیز آشکار می‌کند: ضمانت اجرای اداری برای مهار شنود، افشا یا نفوذ اهمیت دارد، اما برای مدیریت ریسک‌های پیچیده هوش مصنوعی و اینترنت اشیاء کافی نیست. بسیاری از مخاطرات این حوزه نه از شنود مستقیم یا افشای صریح، بلکه از پردازش تدریجی، ترکیب داده‌ها، انتقال به سرویس‌های ابری، پروفایل‌سازی رفتاری، طراحی نامتقارن رابط کاربر، نبود امنیت پیش‌فرض یا استفاده از داده در تصمیم‌های الگوریتمی پدید می‌آیند. این وضعیت‌ها الزاماً در قالب تخلف اداریِ شنود یا افشا نمی‌گنجند؛ بنابراین، آیین‌نامه‌ها نسبت به «سوءاستفاده زیرساختی از دسترسی» واکنش دارند، اما نسبت به «طراحی داده‌محور پرخطر» یا «حکمرانی الگوریتمی» ابزار کافی ندارند. در نسبت با الگوی اتحادیه اروپا، جایگاه این مقررات محدود و سطحی است. در سطح داده، فقط بخشی از محرمانگی و امنیت ارتباطات را از مسیر منع شنود، افشا، بررسی یا نفوذ غیرمجاز پشتیبانی می‌کنند، اما مشروعیت پردازش، شفافیت، محدودیت هدف، کمینه‌سازی، حقوق اشخاص، ارزیابی تأثیر و پاسخ‌گویی نهادی را مقرر نمی‌سازند. در سطح پلتفرم، تعهدی درباره شفافیت توصیه‌گرها، هدف‌گیری تبلیغاتی، ارزیابی ریسک‌های نظام‌مند، اعتراض کاربران یا دسترسی پژوهشگران دیده نمی‌شود. در سطح سامانه هوش مصنوعی، از طبقه‌بندی ریسک، مستندسازی فنی، نظارت انسانی، دقت و استحکام یا ارزیابی اثر بر حقوق بنیادین سخنی نیست؛ و در سطح محصول متصل نیز امنیت در طراحی، امنیت پیش‌فرض، مدیریت آسیب‌پذیری، به‌روزرسانی امنیتی و نظارت بازار بر تولیدکننده تحمیل نشده است. در مقام امکان‌سنجی، اگر ارائه‌دهنده خدمات اینترنتی یا کارمند آن بسته‌های

اطلاعاتی کاربر را بدون مجوز بررسی کند، روابط خصوصی را افشا کند یا از دسترسی خود برای نفوذ یا همکاری غیرقانونی استفاده کند، آیین‌نامه‌ها می‌توانند مبنای مداخله اداری و انتظامی باشند و اگر رفتار واجد عنوان مجرمانه باشد، مسیر کیفری نیز فعال می‌شود. اما اگر مسئله استفاده پلتفرم از داده‌های رفتاری برای توصیه‌گری یا تبلیغات هدفمند باشد، این آیین‌نامه‌ها ابزار مناسبی برای ارزیابی ریسک پلتفرمی نیستند؛ اگر مسئله ضعف امنیتی یک دستگاه متصل یا نبود به‌روزرسانی باشد، موضوع به مسئولیت تولیدکننده، حمایت مصرف‌کننده و تنظیم‌گری امنیت محصول نزدیک‌تر است؛ و اگر مسئله تصمیم‌گیری الگوریتمی بر پایه داده‌های اینترنت اشیاء باشد، قواعد خاص سامانه هوش مصنوعی، شفافیت، نظارت انسانی و ارزیابی اثر بر حقوق بنیادین لازم است؛ بنابراین، کارکرد آیین‌نامه‌ها فقط در حلقه دسترسی و رفتار زیرساختی قرار دارد. این آیین‌نامه‌ها باید در کنار اصول بالادستی و قواعد مسئولیت خوانده شوند، نه به‌جای آن‌ها: اصول مربوط به حیثیت، حریم خصوصی و مصونیت ارتباطات جهت بنیادین حمایت را فراهم می‌کنند؛ قواعد مسئولیت مدنی و قراردادی جبران زیان ناشی از نقص اطلاع‌رسانی، ضعف امنیت یا نقض تعهد مراقبت را امکان‌پذیر می‌سازند؛ قانون تجارت الکترونیکی بخشی از کارکرد داده‌ای را در قلمرو خدمات و مبادلات الکترونیکی پوشش می‌دهد؛ قانون جرائم رایانه‌ای نسبت به تعرض‌های منصوص کیفری واکنش نشان می‌دهد؛ و آیین‌نامه‌ها رفتار برخی بازیگران زیرساختی را از مسیر مجوز، تخلف اداری و ضمانت اجرای انتظامی کنترل می‌کنند؛ بنابراین، هیچ‌یک از این منابع به‌تنهایی مدل حکمرانی داده را نمی‌سازد؛ هرکدام فقط بخشی از منظومه‌ای پراکنده و ناتمام‌اند.

کاربست مقررات موجود ایران در حوزه هوش مصنوعی و اینترنت اشیاء زمانی از توصیف پراکنده قواعد عبور می‌کند که در نسبت با کارکردهای مشخص الگوی ریسک‌محور اتحادیه اروپا سنجیده شود. در این الگو، حمایت از حریم خصوصی فقط در سطح داده متوقف نمی‌ماند؛ بلکه در چهار سطح به‌هم‌پیوسته توزیع می‌شود: داده، پلتفرم، سامانه هوش مصنوعی و محصول متصل؛ بنابراین، پرسش اصلی در حقوق ایران این نیست که آیا مفاهیمی مانند «داده‌پیام»، «داده رایانه‌ای» یا «سامانه رایانه‌ای» از نظر لفظی به هوش مصنوعی و اینترنت اشیاء قابل تسری‌اند؛ بلکه پرسش این است که هر متن ایرانی دقیقاً کدام کارکرد از این چهار سطح را، در حدود قلمرو خود، پشتیبانی می‌کند و در کجا متوقف می‌شود. در سطح داده، مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی فقط در نسبتی محدود با کارکردهای مقرره عمومی حفاظت از داده‌ها قابل امکان‌سنجی‌اند. این مواد، در فرض وجود رابطه الکترونیکی میان کاربر و ارائه‌دهنده خدمت، می‌توانند حداقلی از پرسش‌های داده‌محور را فعال کنند: آیا رضایت معتبر وجود دارد؟ هدف پردازش روشن است؟ داده گردآوری‌شده برای آن هدف ضرورت دارد؟ آیا کاربر امکان دسترسی، اصلاح یا حذف داده را دارد؟ از این منظر، اگر ابزار پایش سلامت، سامانه خانه هوشمند، خدمت مدیریت انرژی یا خودرو متصل در قالب رابطه‌ای مستمر با ارائه‌دهنده خدمت، داده‌های شخصی را پردازش کند، مواد ۵۸ و ۵۹ نقطه آغاز تحلیل‌اند. بااین‌حال، این ظرفیت به معنای تحقق منطق کامل مقرره عمومی حفاظت از داده‌ها نیست؛ زیرا قانون تجارت الکترونیکی ارزیابی تأثیر بر حفاظت از داده، پاسخ‌گویی قابل ممیزی، نهاد مستقل ناظر، قواعد روشن انتقال داده، پردازش ابری، پروفایل‌سازی رفتاری و استنباط الگوریتمی را نظام‌مند تنظیم نمی‌کند. ازاین‌رو، نسبت آن با مقرره عمومی حفاظت از داده‌ها، نسبت پوشش ناقص برخی کارکردهای اولیه سطح داده است (حیدری و جعفری، ۱۳۸۹، ص. ۹۴). همین محدودیت در داده‌های اینترنت اشیاء برجسته‌تر می‌شود؛ زیرا داده‌های حاصل از ابزارهای متصل، غالباً در لحظه گردآوری عادی و کم‌خطر به نظر می‌رسند، اما در مرحله تحلیل می‌توانند معنای حساس پیدا کنند. الگوی خواب، مصرف انرژی، رفت‌وآمد، ضربان قلب، استفاده از وسایل خانگی یا موقعیت مکانی ممکن است در ابتدا داده رفتاری یا فنی تلقی شود، اما از طریق ترکیب و تحلیل الگوریتمی، وضعیت سلامت، الگوی

زندگی، وضعیت روانی یا آسیب‌پذیری شخص را آشکار کند. در الگوی اتحادیه اروپا، چنین وضعیتی با محدودیت هدف، کمینه‌سازی، ارزیابی اثر و پاسخ‌گویی مستمر کنترل می‌شود؛ در حقوق ایران، مواد ۵۸ و ۵۹ چنین سازوکار پیوسته‌ای ندارند و هرجا ماده‌ای ماهیت کیفری پیدا می‌کند، نمی‌توان با تفسیر موسع، هر استنباط الگوریتمی را به داده حساس منصوص ملحق کرد؛ بنابراین، قانون تجارت الکترونیکی برای پردازش اولیه داده در روابط الکترونیکی ظرفیت دارد، اما برای داده‌های استنباطی و حساسیت پسینی ناشی از تحلیل الگوریتمی کافی نیست.

در سطح کیفری، قانون جرائم رایانه‌ای فقط هنگامی قابل‌اعمال است که رفتار زیان‌بار با عنوان مجرمانه منصوص انطباق داشته باشد. دسترسی غیرمجاز به حافظه ابزار پوشیدنی، نفوذ به پنل خانه هوشمند، شنود ارتباط میان حسگر و سرور ابری، دست‌کاری متقلبانه داده‌های ثبت‌شده یا انتشار غیرمجاز تصویر خصوصی، در صورت تحقق ارکان قانونی، می‌تواند ذیل موادی مانند دسترسی غیرمجاز، شنود غیرمجاز، جعل رایانه‌ای یا انتشار محتوای خصوصی تحلیل شود (قاسم‌زاده لیاسی و رئیسی، ۱۳۹۹، ص. ۶۰۹). اما این حمایت با منطق قانون هوش مصنوعی و مقرره تاب‌آوری سایبری تفاوت بنیادین دارد؛ زیرا قانون جرائم رایانه‌ای عمدتاً پس از وقوع تعرض وارد عمل می‌شود، درحالی‌که قانون هوش مصنوعی و مقرره تاب‌آوری سایبری، خطر را در مرحله طراحی، عرضه، استقرار و چرخه عمر سامانه یا محصول مدیریت می‌کنند. ازاین‌رو، ضعف طراحی محصول، نبود امنیت پیش‌فرض، فقدان به‌روزرسانی امنیتی، خطای کاربر، رضایت صوری یا پردازش قراردادی اما پرخطر، به‌خودی‌خود جرم رایانه‌ای نیستند و باید از مسیر مسئولیت مدنی، قراردادی، حمایت مصرف‌کننده یا تنظیم‌گری اداری تحلیل شوند. رویه قضایی منتشرشده نیز همین مرز را تأیید می‌کند. در دادنامه قطعی شماره ۹۱۰۹۹۷۰۲۲۳۸۰۱۴۵۲ مورخ ۳۰/۱۰/۱۳۹۱، موضوع دسترسی غیرمجاز به ایمیل اشخاص توسط کارکنان دولت در چارچوب ماده ۱ قانون جرائم رایانه‌ای تحلیل شده است. اهمیت این رأی برای محیط‌های متصل آن است که معیار مسئولیت کیفری را «تحقق دسترسی غیرمجاز به داده یا سامانه» می‌داند، نه صرف حساسیت داده یا نوظهور بودن ابزار؛ بنابراین، منطق این رأی می‌تواند در مواردی مانند نفوذ به‌حساب کاربری ابزار پوشیدنی، سامانه خانه هوشمند یا پنل ابری یک خدمت متصل راهنما باشد؛ اما همین منطق مجوزی برای جرم‌انگاری نقص طراحی، ضعف امنیت پیش‌فرض یا پردازش پرخطر فراهم نمی‌کند (دادگاه تجدیدنظر استان تهران، شعبه ۴۳، ۱۳۹۱). در حوزه صوت، تصویر و اسرار خصوصی نیز تحلیل باید بر تفکیک دقیق عناصر قانونی استوار باشد. دادنامه قطعی شماره ۹۲۰۹۹۷۰۲۲۲۳۰۰۳۶۲ مورخ ۲۵/۰۳/۱۳۹۲، در موضوع انتشار تصاویر خصوصی و تغییر تصویر دیگری از طریق سامانه‌های رایانه‌ای، تمایز میان «انتشار تصویر خصوصی بدون رضایت» و «تغییر یا تحریف تصویر» را برجسته می‌کند. اهمیت این تمایز

برای فناوری‌هایی مانند دیپ‌فیک آن است که مواد ۱۶ و ۱۷ قانون جرائم رایانه‌ای را نمی‌توان یکپارچه به همه مصادیق محتوای مصنوعی تسری داد. اگر محتوا واقعاً تغییر یا تحریف شده و به شخص قابل‌شناسایی منتسب باشد، تحلیل ماده ۱۶ قابل‌طرح است؛ اما اگر تصویر واقعی بدون رضایت منتشر شده باشد، محور بحث به ماده ۱۷ نزدیک می‌شود. در هر دو فرض، خصوصی‌بودن محتوا، فقدان رضایت، انتساب عرفی و ورود ضرر یا هتک حیثیت باید جداگانه بررسی شود. بااین‌حال، این تحلیل کیفری با منطق مقرره خدمات دیجیتال فاصله دارد؛ زیرا حقوق ایران در این قسمت ابزارهایی مانند برچسب‌گذاری محتوای مصنوعی، تشخیص منشأ، حذف نسخه‌های اساساً معادل، مسئولیت پلتفرم برای بازنشر یا ارزیابی ریسک نظام‌مند را پیش‌بینی نمی‌کند (دادگاه تجدیدنظر استان تهران، شعبه ۶، ۱۳۹۲). از این منظر، قانون جرائم رایانه‌ای فقط نسبت به «انتشار یا تحریف زیان‌بار» واکنش موردی نشان می‌دهد، درحالی‌که مقرره خدمات دیجیتال مسئله را در مقیاس پلتفرمی می‌بیند؛ یعنی نه‌فقط اینکه چه محتوایی منتشر شده، بلکه اینکه پلتفرم چگونه آن را توصیه، بازنشر، تقویت، حذف یا قابل‌اعتراض می‌کند؛ بنابراین، اگر تصویر خصوصی یا دیپ‌فیک زیان‌بار منتشر شود، ممکن است مسیر کیفری فعال شود؛ اما اگر همان محتوا در چرخه الگوریتمی بازنشر شود، بارها تغییر قالب دهد، در چند سکو تکثیر شود یا از سوی سامانه توصیه‌گر تقویت گردد، مقررات موجود ابزار پلتفرمی هم‌سنگ با مقرره خدمات دیجیتال در اختیار نمی‌گذارد.

در سطح مسئولیت مدنی نیز باید میان وقوع جرم و قابلیت جبران خسارت تفکیک کرد. در دادنامه قطعی شماره ۹۲۰۹۹۸۰۲۷۹۲۰۰۰۳۳ مورخ ۲۱/۰۲/۱۳۹۴، در دعوای مطالبه ضرر و زیان ناشی از سرقت داده‌های رایانه‌ای، دادگاه تصریح کرده است که صرف ربایش اطلاعات و داده‌های رایانه‌ای به‌تنهایی به معنای ورود خسارت نیست و ضرر باید احراز شود. ارزش این رأی آن است که نشان می‌دهد تعقیب کیفری و جبران مدنی دو منطق مستقل دارند. ممکن است دسترسی غیرمجاز یا سرقت داده از حیث کیفری قابل‌تعقیب باشد، اما مطالبه خسارت ناشی از افشای داده، لطمه اعتباری، اختلال خدمت، زیان اقتصادی یا نقض انتظار مشروع کاربر، نیازمند اثبات ضرر، رابطه سببیت و میزان خسارت است. این تفکیک برای امکان‌سنجی مهم است؛ زیرا در الگوی اتحادیه اروپا، سازوکارهای پیشینیِ ارزیابی ریسک و پاسخ‌گویی، بار مدیریت آسیب را تا حدی ساختارمند می‌کنند، درحالی‌که در حقوق ایران، بخش مهمی از موضوع پس از وقوع زیان و در قالب اثبات قضایی باقی می‌ماند (دادگاه تجدیدنظر استان تهران، شعبه ۲۳، ۱۳۹۴). در سطح اداری و زیرساختی نیز آیین‌نامه‌های ناظر بر دفاتر خدمات اینترنتی و واحدهای ارائه‌کننده خدمات اطلاع‌رسانی فقط بخشی از رفتار بازیگران واسطه را کنترل می‌کنند. ممنوعیت افشای روابط خصوصی، تعرض به حریم اطلاعات شخصی، انتشار کلیدهای رمز، ارائه روش‌های شکستن رمز، نفوذ غیرمجاز و شنود یا بررسی بسته‌های اطلاعاتی، از حیث کارکردی مانع آن می‌شود که موقعیت فنی ارائه‌دهنده خدمت به قدرت بی‌ضابطه بر داده‌های کاربران تبدیل شود (نکونام، ۱۴۰۳، ص. ۲۹–۳۰). ضمانت اجراهایی مانند تذکر، تعلیق، لغو پروانه یا ارجاع به مرجع قضایی نیز حمایت از حریم خصوصی را با استمرار صلاحیت حرفه‌ای و مجوز فعالیت پیوند می‌زند (قاسم‌زاده لیاسی و رئیسی، ۱۳۹۹، ص. ۶۰۵). بااین‌حال، این مقررات فقط در حلقه «دسترسی زیرساختی» قابل امکان‌سنجی‌اند و با هیچ‌یک از چهار مقرره اتحادیه اروپا هم‌سنگ نیستند: نه نظام عمومی داده شبیه مقرره عمومی حفاظت از داده‌ها ایجاد می‌کنند، نه تکالیف پلتفرمی مقرره خدمات دیجیتال را دارند، نه سامانه هوش مصنوعی را مانند قانون هوش مصنوعی اتحادیه اروپا طبقه‌بندی و کنترل می‌کنند، و نه امنیت چرخه عمر محصول متصل را مانند مقرره تاب‌آوری سایبری بر تولیدکننده تحمیل می‌سازند. اگر ارائه‌دهنده خدمات

اینترنتی یا کارکنان آن بسته‌های اطلاعاتی کاربر را بدون مجوز بررسی کنند، روابط خصوصی را افشا کنند یا از موقعیت فنی خود برای نفوذ یا همکاری غیرقانونی استفاده کنند، آیین‌نامه‌ها می‌توانند مبنای مداخله اداری باشند و در صورت تحقق عنوان مجرمانه، مسیر کیفری نیز فعال شود. اما اگر مسئله، استفاده پلتفرم از داده‌های رفتاری برای توصیه‌گری، تبلیغات هدفمند یا تقویت الگوریتمی محتوا باشد، این مقررات ابزار مناسبی برای مدیریت ریسک پلتفرمی نیستند؛ اگر مسئله، ضعف امنیتی یک محصول متصل یا نبود به‌روزرسانی باشد، موضوع به قلمرو امنیت محصول و مسئولیت تولیدکننده نزدیک‌تر است؛ و اگر مسئله، تصمیم‌گیری الگوریتمی بر پایه داده‌های اینترنت اشیاء باشد، به قواعدی مانند شفافیت، نظارت انسانی، مستندسازی و ارزیابی اثر نیاز دارد؛ بنابراین، کارکرد آیین‌نامه‌ها در امکان‌سنجی محدود به کنترل رفتار زیرساختی است، نه مدیریت کامل زنجیره ریسک.

برآیند کاربست تقنینی آن است که حقوق ایران در برابر حریم خصوصی هوش مصنوعی و اینترنت اشیاء با «فقدان مطلق حمایت» مواجه نیست، اما هنوز به نظام ریسک‌محور در معنای اتحادیه اروپا نیز نرسیده است. قانون تجارت الکترونیکی بخشی از کارکرد سطح داده را در روابط الکترونیکی پشتیبانی می‌کند؛ قانون جرائم رایانه‌ای نسبت به تعرض‌های کیفری به داده و سامانه واکنش نشان می‌دهد؛ آیین‌نامه‌ها رفتار برخی بازیگران زیرساختی را از مسیر ضمانت اجراهای اداری کنترل می‌کنند؛ و قواعد مسئولیت مدنی و قراردادی می‌توانند در جبران خسارت و سنجش تعهدات مراقبتی نقش داشته باشند. بااین‌حال، این مجموعه، برخلاف مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی اتحادیه اروپا و مقرره تاب‌آوری سایبری، به زنجیره‌ای منسجم از پیشگیری، ارزیابی اثر، شفافیت، نظارت، پاسخ‌گویی، امنیت در طراحی و مدیریت چرخه عمر تبدیل نشده است. نتیجه امکان‌سنجی آن است که حقوق ایران ظرفیت‌هایی واقعی اما پراکنده و سناریو محور دارد؛ ظرفیت‌هایی که برای حمله، افشا، دسترسی غیرمجاز یا برخی روابط الکترونیکی قابل استفاده‌اند، اما برای ریسک‌های ترکیبی و زنجیره‌ایِ ناشی از پلتفرم‌ها، سامانه‌های هوش مصنوعی و محصولات متصل کافی نیستند (رفیعی و همکاران، ۱۴۰۱، ص. ۲۱۳). حاصل این ارزیابی آن است که مسئله اصلی، نبود مطلق حمایت از حریم خصوصی نیست؛ بلکه ناتوانی قواعد موجود در تبدیل «ریسک‌های متنوع» به «تکالیف حقوقی متناسب» است. در نظام اتحادیه اروپا، مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی و مقرره تاب‌آوری سایبری هر یک سطح خاصی از ریسک را هدف می‌گیرند: ریسک داده‌ای، ریسک پلتفرمی، ریسک سامانه‌ای و ریسک محصول متصل. ارزش تحلیلی این الگو آن است که هر خطر را در محل پیدایش خود مهار می‌کند: داده را از حیث مشروعیت و شفافیت پردازش، پلتفرم را از حیث قدرت توصیه و بازنشر، سامانه هوش مصنوعی را از حیث اثر خروجی بر اشخاص، و محصول متصل را از حیث امنیت چرخه عمر. در حقوق ایران، قواعد موجود چنین تقسیم کاری را ایجاد نکرده‌اند. قانون تجارت الکترونیکی بخشی از مسئله داده را در روابط الکترونیکی می‌بیند؛ قانون جرائم رایانه‌ای به تعرض‌های منصوص و پسینی واکنش نشان می‌دهد؛ آیین‌نامه‌های خدمات اینترنتی رفتار برخی

بازیگران زیرساختی را محدود می‌کنند؛ و مسئولیت مدنی و قراردادی، پس از وقوع زیان، امکان جبران را فراهم می‌سازد. این مجموعه ظرفیت دارد، اما هنوز به نظامی هماهنگ و سطحی تبدیل نشده است.

از حیث انتقادی، نخستین ظرفیت حقوق ایران در سطح داده ظاهر می‌شود. مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی می‌توانند در قلمرو خدمات و مبادلات الکترونیکی، پرسش‌هایی بنیادین درباره رضایت، هدف پردازش، تناسب داده، صحت، دسترسی و امکان اصلاح یا حذف داده ایجاد کنند. بااین‌حال، نسبت این مواد با مقرره عمومی حفاظت از داده‌ها، نسبت هم‌ارزی نیست؛ زیرا مقرره عمومی حفاظت از داده‌ها فقط بر رضایت یا حق دسترسی متکی نیست، بلکه از طریق پاسخ‌گویی، ارزیابی اثر، امنیت پردازش، نهاد ناظر، ضمانت اجرای اداری و کنترل مستمر پردازش، یک نظام کامل حاکمیت داده ایجاد می‌کند. قانون تجارت الکترونیکی چنین نظامی ندارد و افزون بر آن، اعمال آن به وجود رابطه الکترونیکی مشخص وابسته است. محدودیت مهم‌تر، ظهور «حساسیت پسینی» است: بسیاری از داده‌های اینترنت اشیاء در لحظه گردآوری عادی به نظر می‌رسند، اما با ترکیب و تحلیل الگوریتمی می‌توانند وضعیت سلامت، عادت‌های خصوصی، وضعیت روانی یا آسیب‌پذیری رفتاری شخص را آشکار کنند. الگوی اتحادیه اروپا این مسئله را از طریق محدودیت هدف، کمینه‌سازی، ارزیابی اثر و پاسخ‌گویی مستمر مهار می‌کند؛ در حقوق ایران، چنین سازوکاری به‌صورت صریح و عمومی وجود ندارد؛ بنابراین، قانون تجارت الکترونیکی برای پردازش اولیه داده در روابط الکترونیکی مفید است، اما برای داده‌های استنباطی و تحلیل‌های ثانویه هوش مصنوعی کفایت ندارد. در سطح پلتفرم، شکاف حقوق ایران عمیق‌تر است. مقرره خدمات دیجیتال، مسئله را صرفاً انتشار یک محتوای زیان‌بار نمی‌داند؛ بلکه به این می‌پردازد که پلتفرم چگونه محتوا را توصیه، رتبه‌بندی، بازنشر، تقویت، حذف یا قابل‌اعتراض می‌کند. در حقوق ایران، مواد ۱۶ و ۱۷ قانون جرائم رایانه‌ای می‌توانند در برابر انتشار یا تحریف تصویر، صوت یا اسرار خصوصی واکنش نشان دهند، اما این واکنش موردی جایگزین تنظیم‌گری پلتفرمی نمی‌شود. اگر تصویر خصوصی یا دیپ‌فیک زیان‌بار یک‌بار منتشر شود، امکان تحلیل کیفری وجود دارد؛ اما اگر همان محتوا در چرخه الگوریتمی بازنشر شود، نسخه‌های مشابه پیدا کند، از طریق سامانه توصیه‌گر تقویت شود یا در چند بستر تکثیر گردد، حقوق ایران ابزار هم‌سنگ مقرره خدمات دیجیتال ندارد. در این سطح، کاستی اصلی نه نبود جرم‌انگاری، بلکه نبود تکالیف پلتفرمی درباره شفافیت توصیه‌گرها، تبلیغات هدفمند، سازوکار

اعتراض، حفظ ادله، حذف نسخه‌های اساساً معادل، دسترسی پژوهشگران و ارزیابی ریسک‌های نظام‌مند است. در سطح سامانه هوش مصنوعی نیز قواعد موجود ایران کارکرد محدودی دارند. قانون هوش مصنوعی اتحادیه اروپا، ریسک را بر اساس اثر سامانه بر سلامت، ایمنی و حقوق اشخاص می‌سنجد و برای سامانه‌های پرخطر الزاماتی مانند حاکمیت داده، مستندسازی، نظارت انسانی، آزمون، ثبت خطا و ارزیابی اثر مقرر می‌کند. در حقوق ایران، قانون تجارت الکترونیکی داده را می‌بیند و قانون جرائم رایانه‌ای تعرض مجرمانه را؛ اما خود «خروجی سامانه هوش مصنوعی» هنوز موضوع تنظیم مستقل نیست. سوگیری داده آموزشی، خطای مدل، تصمیم خودکار نامتناسب، نبود نظارت انسانی یا استفاده از داده‌های اینترنت اشیاء برای رتبه‌بندی رفتاری را نمی‌توان با توسعه عناوینی مانند جعل، شنود یا دسترسی غیرمجاز حل کرد. این موارد نه لزوماً جرم‌اند و نه صرفاً مسئله قراردادی؛ بلکه به سطح سامانه مربوط‌اند. ازاین‌رو، حقوق ایران برای کنترل ریسک خود سامانه هوش مصنوعی ابزار اختصاصی ندارد. در سطح محصول متصل نیز فاصله حقوق ایران با مقرره تاب‌آوری سایبری آشکار است .مقرره تاب‌آوری سایبری امنیت محصول را از مرحله طراحی تا عرضه، پشتیبانی، به‌روزرسانی و مدیریت آسیب‌پذیری دنبال می‌کند. در حقوق ایران، اگر دوربین خانگی، خودرو متصل، قفل هوشمند یا ابزار پوشیدنی به دلیل ضعف امنیتی موجب افشای داده شود، می‌توان درباره مسئولیت مدنی، قراردادی یا رفتار کیفری مهاجم بحث کرد؛ اما قاعده عامی وجود ندارد که تولیدکننده را پیشاپیش به امنیت در طراحی، امنیت پیش‌فرض، اعلام آسیب‌پذیری، دوره پشتیبانی امنیتی یا به‌روزرسانی ملزم کند؛ بنابراین، حقوق ایران غالباً پس از حادثه وارد عمل می‌شود، درحالی‌که منطق مقرره تاب‌آوری سایبری بر پیشگیری از حادثه از طریق مسئولیت چرخه عمر محصول استوار است.

این ارزیابی نشان می‌دهد که انتقال منطق ریسک‌محور اتحادیه اروپا به حقوق ایران فقط در صورتی معتبر است که «سطح ریسک» با «ابزار حقوقی» خلط نشود. ریسک داده‌ای را نباید با حقوق کیفری حل کرد؛ ریسک پلتفرمی را نباید به انتشار منفرد تقلیل داد؛ ریسک سامانه‌ای را نباید با صرف کنترل داده ورودی یکی دانست؛ و ریسک محصول متصل را نباید فقط پس از نفوذ مهاجم تحلیل کرد. از اینجا به بعد، پیشنهادهای تفسیری و تقنینی باید دقیقاً از همین شکاف‌ها استخراج شوند. در سطح تفسیری، نخستین پیشنهاد آن است که مراجع قضایی و اداری در پرونده‌های مرتبط با هوش مصنوعی و اینترنت اشیاء، روش «تعیین سطح ریسک» را مبنا قرار دهند. ابتدا باید روشن شود مسئله در سطح داده، پلتفرم، سامانه یا محصول قرار دارد. اگر موضوع، رضایت و هدف پردازش در یک خدمت الکترونیکی است، مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی می‌توانند با رعایت قلمرو خود به کار روند. اگر موضوع، نفوذ، شنود، جعل یا انتشار غیرمجاز است، قانون جرائم رایانه‌ای فقط در حدود عنوان منصوص قابل‌اعمال است. اگر موضوع، سوءاستفاده زیرساختی ارائه‌دهنده خدمات اینترنتی از دسترسی فنی است، آیین‌نامه‌ها می‌توانند مبنای مداخله اداری باشند. اما اگر مسئله، توصیه‌گری پلتفرمی، تصمیم الگوریتمی یا امنیت چرخه عمر محصول است، باید خلأ تقنینی شناسایی شود، نه اینکه با تفسیر موسع منابع موجود پوشانده شود. پیشنهاد تفسیری دوم، تقویت محدود اما مؤثر کارکرد داده‌ای قانون تجارت الکترونیکی است. این قانون نباید به منشور عام همه داده‌های اینترنت اشیاء تبدیل شود؛ اما در قلمرو خدمات الکترونیکی باید جدی گرفته شود. رضایت در خدمات متصل زمانی معتبر است که کاربر بداند چه داده‌ای، برای چه هدفی، تا چه مدت، توسط چه اشخاصی و با چه امکان تحلیل ثانویه پردازش می‌شود؛ بنابراین، مواد ۵۸ و ۵۹ باید به سمت شفافیت واقعی، هدفمندی، تناسب و پرهیز از پردازش زائد تفسیر شوند، نه به سمت مشروع‌سازی شروط طولانی و غیرقابل‌مذاکره. این تفسیر با منطق مقرره عمومی حفاظت از داده‌ها همسو است، اما ادعای جانشینی آن را ندارد. پیشنهاد تفسیری سوم، حفظ مرز حقوق کیفری است. منطق ریسک‌محور اتحادیه اروپا نمی‌تواند مجوز توسعه عناوین مجرمانه در حقوق ایران باشد. دسترسی غیرمجاز، شنود، جعل یا انتشار محتوای خصوصی فقط زمانی قابل تعقیب‌اند که ارکان قانونی همان

جرم محقق باشد. نقص طراحی محصول، نبود به‌روزرسانی، خطای مدل، سوگیری داده یا تصمیم خودکار زیان‌بار را نباید با تفسیر موسع به قلمرو کیفری کشاند. این موارد باید در مسیر مسئولیت مدنی، قراردادی، حمایت مصرف‌کننده، تنظیم‌گری اداری یا اصلاح تقنینی بررسی شوند. این پیشنهاد، هم مانع بی حمایت ماندن اشخاص می‌شود و هم اصل قانونی‌بودن جرم و مجازات را حفظ می‌کند.

در سطح تقنینی، پیشنهادها باید از شکاف چهارسطحی استخراج شوند. در سطح داده، حقوق ایران نیازمند قانون جامع حمایت از داده‌های شخصی است؛ قانونی که داده شخصی، داده حساس، داده زیست‌سنجی، داده مکانی، داده استنباطی، پردازش، کنترل‌کننده، پردازشگر، پروفایل‌سازی و تصمیم‌گیری خودکار را تعریف کند و اصول مشروعیت، شفافیت، محدودیت هدف، کمینه‌سازی، امنیت، محدودیت نگهداری، پاسخ‌گویی و حقوق اشخاص را فرابخشی سازد. در سطح پلتفرم، باید قواعدی درباره شفافیت توصیه‌گرها، تبلیغات هدفمند، اعتراض کاربر، حفظ ادله، حذف محتوای غیرقانونی و نسخه‌های اساساً معادل، و ارزیابی ریسک‌های نظام‌مند پلتفرم‌های اثرگذار پیش‌بینی شود. در سطح سامانه، قانون‌گذار باید میان کاربردهای کم‌خطر، محدود و پرخطر هوش مصنوعی تمایز بگذارد و برای سامانه‌های پرخطر الزاماتی مانند حاکمیت داده، مستندسازی، آزمون پیش از استقرار، نظارت انسانی، ثبت خطا و ارزیابی اثر مقرر کند. در سطح محصول متصل نیز باید چارچوبی برای امنیت در طراحی، امنیت پیش‌فرض، پشتیبانی امنیتی، مدیریت آسیب‌پذیری، به‌روزرسانی و نظارت بازار ایجاد شود. جمع‌بندی آن است که امکان‌سنجی اعمال الگوی ریسک‌محور اتحادیه اروپا در حقوق ایران به پذیرش یا رد کامل آن الگو منتهی نمی‌شود. نتیجه دقیق‌تر این است که حقوق ایران در سطح داده ظرفیت محدود دارد؛ در سطح کیفری، واکنش پسینی نسبت به تعرض‌های منصوص دارد؛ در سطح زیرساخت، کنترل اداری محدودی فراهم می‌کند؛ و در سطح مسئولیت مدنی و قراردادی، امکان جبران برخی زیان‌ها را فراهم می‌سازد. اما در برابر ریسک‌های پلتفرمی، سامانه‌ای و محصول‌محور، هنوز ابزارهای اختصاصی ندارد؛ بنابراین، مسیر اصلاح نه انتقال مکانیکی مقرره عمومی حفاظت از داده‌ها، مقرره خدمات دیجیتال، قانون هوش مصنوعی اتحادیه اروپا و مقرره تاب‌آوری سایبری است و نه اتکای خوش‌بینانه به تفسیر موسع قوانین موجود؛ بلکه بازسازی کارکردی چهار منطق اتحادیه اروپا در حقوق ایران است: داده باید با قانون جامع حمایت شود، پلتفرم باید پاسخ‌گو شود، سامانه هوش مصنوعی باید بر اساس ریسک کنترل شود، و محصول متصل باید از مرحله طراحی ایمن باشد.

بحث و نتیجه‌گیری

برآیند این پژوهش نشان می‌دهد که حمایت از حریم خصوصی در اکوسیستم‌های هوش مصنوعی و اینترنت اشیاء، دیگر با اتکا به یک قاعده منفرد یا صرف شناسایی «داده شخصی» قابل‌تأمین نیست؛ زیرا ریسک‌های این زیست‌بوم در یک نقطه واحد شکل نمی‌گیرند. داده‌های تولیدشده از ابزارهای متصل، قدرت پلتفرم‌ها در توصیه، رتبه‌بندی و بازنشر محتوا، خروجی سامانه‌های هوش مصنوعی و امنیت محصولات دارای عناصر دیجیتال، هر یک می‌توانند به‌گونه‌ای متفاوت بر حریم خصوصی، آزادی انتخاب، عدم تبعیض، امنیت شخصی و امکان اعتراض مؤثر اثر بگذارند. ازاین‌رو، اهمیت الگوی اتحادیه اروپا در آن است که ریسک را در چهار سطح داده، پلتفرم، سامانه هوش مصنوعی و محصول متصل صورت‌بندی کرده و برای هر سطح، تکالیفی متناسب با ماهیت همان خطر پیش‌بینی می‌کند. مقرره عمومی حفاظت از داده‌ها، مشروعیت و کیفیت پردازش داده را کنترل می‌کند؛ مقرره خدمات دیجیتال، قدرت پلتفرم در سازمان‌دهی محیط برخط را محدود می‌سازد؛ قانون هوش مصنوعی، خروجی سامانه و آثار آن بر سلامت، ایمنی و حقوق بنیادین را موضوع نظارت قرار می‌دهد؛ و مقرره تاب‌آوری سایبری، امنیت محصول متصل را در چرخه طراحی، عرضه، پشتیبانی و مدیریت آسیب‌پذیری دنبال می‌کند.

امکان‌سنجی این منطق در حقوق ایران نشان می‌دهد که نظام موجود با خلأ مطلق حمایت مواجه نیست، اما حمایت‌های آن پراکنده، محدود و غالباً پسینی است. قانون تجارت الکترونیکی تنها در سطح داده و در قلمرو روابط یا خدمات الکترونیکی، ظرفیت محدودی برای تحلیل رضایت، هدفمندی، تناسب، دسترسی و اصلاح داده فراهم می‌آورد. قانون جرائم رایانه‌ای نیز صرفاً نسبت به تعرض‌های منصوص، مانند دسترسی، شنود، جعل، دست‌کاری و انتشار غیرمجاز، قابل‌اعمال است و به سبب اصل قانونی‌بودن و منع تفسیر موسع، نمی‌تواند به نقص طراحی محصول، تصمیم الگوریتمی پرخطر یا ریسک‌های نظام‌مند پلتفرمی تسری یابد. آیین‌نامه‌های خدمات اینترنتی نیز فقط بخشی از رفتار بازیگران زیرساختی را کنترل می‌کنند و جایگزین تنظیم‌گری داده، پلتفرم، سامانه یا محصول متصل نمی‌شوند.

از این منظر، اقتباس از الگوی اتحادیه اروپا برای حقوق ایران تنها زمانی قابل‌دفاع است که به انتقال لفظی مقررات یا توسعه تفسیری قوانین موجود فروکاسته نشود، بلکه به بازآرایی کارکردهای حقوقی در چهار سطح مشخص بینجامد. در سطح داده، نیاز اصلی تدوین نظام عام حمایت از داده‌های شخصی با تأکید بر مشروعیت پردازش، شفافیت، کمینه‌سازی، حقوق اشخاص و پاسخ‌گویی نهادی است. در سطح پلتفرم، خلأ اصلی به فقدان تکالیف شفافیت، اعتراض، حفظ ادله، مدیریت بازنشر و ارزیابی ریسک‌های نظام‌مند بازمی‌گردد. در سطح سامانه هوش مصنوعی، مسئله‌محوری نبود نظام طبقه‌بندی ریسک، مستندسازی، نظارت انسانی و ارزیابی اثر بر حقوق بنیادین است. در سطح محصول متصل نیز حقوق ایران فاقد الزامات روشن درباره امنیت در طراحی، پشتیبانی امنیتی، به‌روزرسانی و مدیریت آسیب‌پذیری است؛ بنابراین، دستاورد اصلی این امکان‌سنجی آن است که حقوق ایران برای حمایت مؤثر از حریم خصوصی در محیط‌های هوشمند متصل، بیش از هر چیز به تفکیک دقیق محل پیدایش ریسک و تعیین ضمانت اجرای متناسب با هر سطح نیاز دارد؛ امری که می‌تواند حمایت از حریم خصوصی را از واکنش موردی پس از نقض، به نظامی پیشینی، قابل‌ارزیابی و پاسخ‌گو نزدیک سازد.

منابع

بابایی، جواد (۱۳۹۸). جرایم رایانه‌ای و آیین دادرسی حاکم بر آن. تهران: قوه قضاییه، مرکز مطبوعات و انتشارات.

بابایی، حسین، و احمدی ناطور، زهرا. (۱۳۹۵). مطالعه تطبیقی جرایم علیه حریم خصوصی در فضای سایبری ایران و آلمان. مطالعات بین‌رشته‌ای در رسانه و فرهنگ، دوره ۶، شماره ۱، ۱-۲۴.

جلالی فراهانی، امیرحسین (۱۳۸۶). مزیت‌ها و محدودیت‌های فضای سایبر در حوزه‌های آزادی بیان، آزادی اطلاعات و حریم خصوصی. مجله حقوقی دادگستری، دوره ۷۱، شماره ۵۹، ۱۰۰–۶۱.

حیدری، علی‌مراد، جعفری، علی (۱۳۸۹). حمایت کیفری از رسانه‌های دیداری و شنیداری. نشریه رسانه، دوره ۲۱، شماره ۲، ۱۰۹–۸۷.

دادگاه تجدیدنظر استان تهران. (۱۳۹۲، ۲۵ خرداد) .انتشار تصاویر خصوصی و تغییر تصویر دیگری از طریق سامانه‌های رایانه‌ای، دادنامه قطعی شماره ۹۲۰۹۹۷۰۲۲۲۳۰۰۳۶۲. سامانه ملی آرای قضایی، پژوهشگاه قوه قضاییه.

دادگاه تجدیدنظر استان. (۱۳۹۱، ۳۰ دی) .دسترسی غیرمجاز به داده‌های رایانه‌ای، دادنامه قطعی شماره ۹۱۰۹۹۷۰۲۲۳۸۰۱۴۵۲. سامانه ملی آرای قضایی، پژوهشگاه قوه قضاییه.

دادگاه تجدیدنظر استان. (۱۳۹۴، ۲۱ اردیبهشت) .مطالبه ضرر و زیان ناشی از سرقت داده‌های رایانه‌ای، دادنامه قطعی شماره ۹۲۰۹۹۸۰۲۷۹۲۰۰۰۳۳. سامانه ملی آرای قضایی، پژوهشگاه قوه قضاییه.

رفیعی، علی، عباسلو، بختیار، و امینی، عیسی. (۱۴۰۱). پاسخ‌های غیرکیفری به مسائل نقض حریم خصوصی در سیاست جنایی ایران و کانادا. فصلنامه پژوهش حقوق کیفری، دوره ۱۱، شماره ۴۱، ۲۰۳-۲۲۸. https://doi.org/10.22054/jclr.2023.62002.2365

رئیسی دزکی، لیلا، و قاسم‌زاده لیاسی، فلور. (۱۳۹۹). چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر. مجله حقوقی دادگستری، دوره ۸۴، شماره ۱۱۰، ۹۷-۱۲۰.

زرکلام، ستار. (۱۳۸۶). حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا). پژوهش‌نامه حقوق اسلامی (معارف اسلامی و حقوق)، دوره ۸، شماره ۱، ۱۷۳-۱۹۶.

صفری، مریم، داداشی چکان، محمدمهدی، و یوسفی ایدلو، علی. (۱۳۹۸). حدود و اختیارات پلیس فتا در مواجهه با حریم خصوصی اشخاص در فضای سایبر. در دومین کنفرانس ملی پدافند سایبری، مراغه، ایران.

عامل نجف‌آبادی، محمد. (۱۳۸۷). جرم‌انگاری در فضای مجازی، پایان‌نامه کارشناسی‌ارشد، دانشگاه شهید بهشتی، دانشکده حقوق.

عبدی، فاطمه، و خوش‌صورت موفق، اعظم. (۱۴۰۲). تحلیلی بر رویه قضایی در خصوص حق بر تصویر زنان در فضای مجازی. پژوهش‌نامه زنان، دوره ۱۴، شماره ۴۶، ۹۱-۱۲۳.

عبدی، فاطمه، و غنی‌زاده بافقی، مریم. (۱۴۰۴). تحلیل حقوقی عوامل نقض حق بر تصویر در فضای مجازی: با تمرکز بر آرای قضایی محاکم ایران. مجله حقوق خصوصی، دوره ۲۲، شماره ۱، ۶۹-۸۳. https://doi.org/10.22059/jolt.2025.394951.100738

فرحزادی، علی‌اکبر، و ناصر، مهدی. (۱۴۰۰). حق بر تبادل داده‌های خصوصی و راهکارهای رفع چالش‌های آن در سازوکار عملکرد ابزارهای اینترنت اشیا. دوفصلنامه بررسی‌های بازرگانی، دوره ۱۹، شماره ۱۰۹، ۱۱۵-۱۲۹.

قاسم‌زاده لیاسی، فلور، و رئیسی، لیلا. (۱۳۹۹). کاربست قوانین و مقررات ارتباطی در صیانت از حریم خصوصی شهروندان در فضای سایبر. فصلنامه مطالعات حقوق عمومی، دوره ۵۰، شماره ۲، ۵۹۷-۶۱۶. https://doi.org/10.22059/jplsq.2018.261128.1778

نکونام، وحید. (۱۴۰۳). بایسته‌های تحقیق از حریم خصوصی داده‌های ارتباطاتی و اطلاعاتی در فضای سایبر. فصلنامه حقوق فناوری‌های نوین، دوره ۵، شماره ۹، ۲۷-۴۰.

نیسی، جمیل، و مدحج، نضال. (۱۳۹۰). بررسی حریم خصوصی و حمایت داده‌های محیط سایبری در مقررات کیفری ایران با نگاهی تطبیقی به مقررات کیفری کشورهای آلمان، انگلستان و ایتالیا. در همایش ملی شهر الکترونیک، همدان، ایران.

References

Balcioğlu, Y. S., Çelik, A. A., & Altındağ, E. (2025). A turning point in AI: Europe's human-centric approach to technology regulation. Journal of Responsible Technology, 23, 100128. https://doi.org/10.1016/j.jrt.2025.100128

Baldini, D. (2025). Legislative intersection perspectives on regulatory sandboxes: Navigating the interplay between the AI Act and the GDPR. In Regulatory sandboxes for AI and cybersecurity: Questions and answers for stakeholders (pp. 70–84). Cybersecurity National Lab.

Beltrán, M. (2025). AI algorithms under scrutiny: GDPR, DSA, AI Act and CRA as pillars for algorithmic security and privacy in the European Union. Computers & Security, 158, 104628. https://doi.org/10.1016/j.cose.2025.104628

Big Brother Watch and Others v. the United Kingdom, Apps. Nos. 58170/13, 62322/14, 24960/15, Grand Chamber Judgment (Eur. Ct. H.R., 25 May 2021).

Chamberlain, J. (2023). The risk-based approach of the European Union's proposed Artificial Intelligence regulation: Some comments from a tort law perspective. European Journal of Risk Regulation, 14(1), 1–13. https://doi.org/10.1017/err.2022.38

Colonna, L. (2025). The end of open source? Regulating open source under the cyber resilience act and the new product liability directive. Computer Law & Security Review, 56, 106105.

Ebers, M., Hoch, V. R. S., Rosenkranz, F., Ruschemeier, H., & Steinrötter, B. (2021). The European Commission's proposal for an Artificial Intelligence Act—A critical assessment by members of the Robotics and AI Law Society (RAILS). J, 4(4), 589–603. https://doi.org/10.3390/j4040043

Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law & Technology Review, 16(1), 18–84.

Floridi, L. (2019). Establishing the rules for building trustworthy AI. Nature Machine Intelligence, 1(6), 261–262.

Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. Computer Law & Security Review, 34(2), 279–288. https://doi.org/10.1016/j.clsr.2017.12.003

Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. Computer Law & Security Review, 34(2), 279–288. https://doi.org/10.1016/j.clsr.2017.12.003

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. Big Data & Society, 7(1), 1–15. https://doi.org/10.1177/2053951719897945

Graux, H., Garstka, K., Murali, N., Cave, J., & Botterman, M. (2025). Interplay between the AI Act and the EU digital legislative framework. European Parliament, Policy Department for Transformation, Innovation and Health. https://doi.org/10.2861/4863883

Griffin, R. (2025). Governing platforms through corporate risk management: The politics of systemic risk in the Digital Services Act. European Law Open, 4(2), 223–253. https://doi.org/10.1017/elo.2025.17

Iliopoulou-Penot, A. (2025). Governing the 'governors' of online speech: A review of the Digital Services Act's first steps in regulating social media platforms. Yearbook of European Law. Advance online publication.

Lynskey, O. (2015). The foundations of EU data protection law. Oxford University Press.

Naudts, L., Helberger, N., Veale, M., & Sax, M. (2025). A right to constructive optimization: A public interest approach to recommender systems in the Digital Services Act. Journal of Consumer Policy, 48(3), 269–296. https://doi.org/10.1007/s10603-025-09586-1

Novelli, C., Hacker, P., Morley, J., Trondal, J., & Floridi, L. (2025). A robust governance for the AI Act: AI Office, AI Board, Scientific Panel, and national authorities. European Journal of Risk Regulation, 16(2), 566–590.

Palmieri, A., Kollnig, K., & Tamo-Larrieux, A. (2024). Systemic risks of dominant online platforms: A scoping review (Preprint). Maastricht University. https://doi.org/10.2139/ssrn.5002743

Piasecki, S., & Chen, J. (2022). Complying with the GDPR when vulnerable people use smart devices. International Data Privacy Law, 12(2), 113–131. https://doi.org/10.1093/idpl/ipac001

Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1), 40–81. https://doi.org/10.1080/17579961.2018.1452176

Quelle, C. (2018). Enhancing compliance under the General Data Protection Regulation: The risky upshot of the accountability- and risk-based approach. European Journal of Risk Regulation, 9(3), 502–526. https://doi.org/10.1017/err.2018.47

Smuha, N. A. (2021). Beyond the individual: Governing AI's societal harm. Internet Policy Review, 10(3).

Söderlund, K., Engström, E., Haresamudram, K., Larsson, S., & Strimling, P. (2024). Regulating high-reach AI: On transparency directions in the Digital Services Act. Internet Policy Review, 13(1). https://doi.org/10.14763/2024.1.1746

Strowel, A., & De Meyere, J. (2023). The Digital Services Act: Transparency as an efficient tool to curb the spread of disinformation on online platforms? Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 14, 66–83.

van Mil, J., & Quintais, J. P. (2022). A matter of (joint) control? Virtual assistants and

the General Data Protection Regulation. Computer Law & Security Review, 45, 105689. https://doi.org/10.1016/j.clsr.2022.105689

Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act. Computer Law Review International, 22(4), 97–112. https://doi.org/10.9785/CRI-2021-220402

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Wachter, S., Mittelstadt, B., & Russell, C. (2018). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. Harvard Journal of Law & Technology, 31(2), 842–887.

Wolters, P., & Zuiderveen Borgesius, F. (2025). The EU Digital Services Act: What does it mean for online advertising and adtech? International Journal of Law and Information Technology, 33, eaaf00