فصلنامه پژوهش های نوین در علوم انسانی و حقوق دوره ۱- شماره ۴ – صفحات ۷۱-۴۳
Journal of new Researches in Humanities and Law
ISSN 3060-6101

مسئولیت مدنی ناشی از آسیب به داده‌های شخصی در حقوق ایران و مقایسه با مقررات GDPR اروپا

شبنم پیرحیاتی *

۱- کارشناسی ارشد حقوق بین الملل، دانشگاه آزاد اسلامی، واحد صفادشت، استان تهران، ایران.

(داوطلب دکتری حقوق خصوصی)

چکیده

با گسترش فضای دیجیتال و افزایش ارزش اقتصادی و اجتماعی داده‌های شخصی، بحث حمایت حقوقی و تعیین مسئولیت مدنی در قبال آسیب به داده‌های افراد، به یکی از چالش‌های اساسی نظام‌های حقوقی معاصر تبدیل شده است. در نظام حقوقی ایران، علی‌رغم توسعه چشم‌گیر فناوری و بروز مصادیق نوینی از نقض داده‌های شخصی، خلأ قانون‌گذاری جامع و شفاف در حوزه حمایت از داده‌های شخصی و تعیین مسئولیت مدنی ناشی از آن‌ها همچنان به‌صورت محسوس وجود دارد و قواعد عام مسئولیت مدنی قابلیت پاسخ‌گویی کامل به آسیب‌های پیچیده و چندلایه فضای داده‌محور را ندارند. از سوی دیگر، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) با تبیین چارچوبی دقیق و صریح برای شناسایی داده‌های شخصی، تعیین مسئولیت گسترده (حتی مسئولیت شبه‌محض یا محض)، شناسایی صریح خسارت‌های مادی و غیرمادی، ارکان اثبات دعوا و ضمانت‌اجراهای بازدارنده، الگویی پیشرفته و الهام‌بخش برای سایر کشورها فراهم آورده است. پژوهش پیش‌رو با رویکرد تطبیقی و تحلیلی، در ابتدا به تبیین مفهومی، حقوقی و اقتصادی داده‌های شخصی و جایگاه آن‌ها در حقوق ایران می‌پردازد؛ سپس ساختار سنتی مسئولیت مدنی را با تأکید بر آسیب‌های داده‌ای و چالش‌های ناشی از آن ارزیابی نموده و مبانی، ارکان و ضمانت‌اجراهای ناظر بر آسیب به داده‌های شخصی را تحلیل می‌کند. در ادامه، مقررات GDPR اروپا به‌عنوان نقطه عطف و معیار جهانی در حفاظت هوشمندانه از داده‌های شخصی، در زمینه مبانی مسئولیت مدنی و شیوه‌های جبران خسارت، به‌صورتی تفصیلی مورد واکاوی قرار می‌گیرد و نقاط قوت و یادگیری‌پذیر آن برای ایران استخراج می‌شود. سپس با رویکردی تطبیقی، تفاوت‌ها و تشابهات دو نظام در زمینه ارکان و مبانی مسئولیت، بار اثبات، ضمانت‌اجراها، حمایت از قربانیان داده‌ای و چالش‌های اجرای رأی مقایسه شده و کاستی‌ها و فرصت‌های نظام حقوقی ایران در این زمینه نقد و تحلیل می‌شود. در بخش پایانی، ضمن ارائه راهکارهای تقنینی، اجرایی و سیاستی از جمله تدوین قانون خاص، اصلاح رویه‌های کلی مسئولیت مدنی، تقویت نهادهای تخصصی و الهام‌گیری از مقررات GDPR اروپا، بر ضرورت تحول سریع ساختارهای حقوقی جهت تأمین حقیقی امنیت داده‌ای و صیانت از حقوق بنیادین اشخاص در بستر داده‌محور تأکید شده است.

کلمات کلیدی: داده‌های شخصی، مسئولیت مدنی، آسیب داده‌ای، GDPR، حمایت حقوقی

مقدمه :

در عصر حاضر که به عصر انقلاب دیجیتال، جامعه دانش‌بنیان و اقتصاد داده‌محور موسوم شده است، داده‌های شخصی دیگر صرفاً مجموعه‌ای از اطلاعات بی‌اهمیت یا اسناد جزئی تلقی نمی‌شوند، بلکه به منزله ارزشمندترین سرمایه‌های فردی و اجتماعی، نقشی بنیادین در شکل‌دهی به مناسبات اقتصادی، فرهنگی، سیاسی و حتی اخلاقی اجتماع ایفا می‌کنند. با گسترش فناوری‌های پیشرفته نظیر اینترنت اشیاء، هوش مصنوعی، پایگاه‌های کلان‌داده و شبکه‌های اجتماعی، حجم و سرعت جمع‌آوری، پردازش و انتقال اطلاعات شخصی افراد به طرز بی‌سابقه‌ای افزایش یافته است. امروزه داده‌های شخصی نه‌تنها زمینه‌ساز رشد اقتصادی جوامع و ظرفیت‌آفرین برای نوآوری‌های فناورانه‌اند، بلکه به عنوان بستر اصلی ارتقای رفاه انسانی، توسعه خدمات هوشمند و ارتقای کیفیت تصمیم‌گیری در سطوح کلان و خرد مورد استفاده قرار می‌گیرند. (میرشکاری و دیگران، ۱۴۰۳)

در این میان، مفهوم حریم خصوصی، که تا پیش از این بیشتر منحصر به مرزهای حضور فیزیکی و اسناد سنتی بوده، دچار تحول عمیقی شده و به حریم داده‌ای تغییر یافته است؛ به نحوی که آسیب، دسترسی غیرمجاز، انتشار یا حتی تحلیل و بهره‌برداری بدون رضایت، می‌تواند پیامدهای جبران‌ناپذیر و ممتد مادی (از قبیل سرقت هویت، زیان‌های اقتصادی و ایجاد محدودیت‌های شغلی یا اعتباری) و غیرمادی (نظیر اضطراب روانی، لکه‌دارشدن حیثیت و نقض آزادی‌های بنیادین افراد) به دنبال داشته باشد. این شرایط موجب شده است که حمایت حقوقی از داده‌های شخصی و تعیین چارچوب‌های پاسخگویی و مسئولیت مدنی در قبال آسیب به این داده‌ها، به یکی از مهم‌ترین دغدغه‌های حقوقی معاصر مبدل شود؛ به ویژه در شرایطی که بسیاری از فعالیت‌های روزمره افراد، سازمان‌ها و دولت‌ها به تعامل با داده‌های شخصی متکی و وابسته است. (لطیف‌زاده، ۱۴۰۱)

برخلاف کشورهای پیشرو در عرصه نظام‌مندسازی و حفظ امنیت داده‌های شخصی نظیر اتحادیه اروپا که با وضع مقررات جامعی همچون مقررات عمومی حفاظت از داده‌ها (GDPR)، الگویی دقیق، پیشرفته و پاسخ‌گو برای حمایت از حریم خصوصی اشخاص، پیشگیری، مقابله و جبران خسارت‌های ناشی از آسیب به داده‌های شخصی فراهم ساخته‌اند، در حقوق ایران همچنان با چالش‌های اساسی مواجه هستیم. فقدان قانون جامع و مستقل حمایت از داده‌های شخصی، عدم ارجاع صریح به مفهوم داده در قوانین سنتی مسئولیت مدنی، کافی نبودن شفافیت در تعریف داده، داده‌پرداز و ذیحقان اطلاعات، و نبود سازوکارهای جبران خسارت متناسب با مختصات دنیای داده‌ای – همگی، زمینه‌ساز نوعی بلاتکلیفی و معضل اثبات، تقصیر و ضمانت‌اجرا در آسیب‌های داده‌ای شده است.

تحولات فناورانه نه‌تنها موجب افزایش امکان بروز خسارت‌های داده‌ای و اشکال نوین تجاوز به حریم خصوصی شده‌اند، بلکه ضرورت بازنگری نظریه‌های کلاسیک مسئولیت مدنی، تطبیق قواعد سنتی با شرایط جدید و ابداع راهکارهای نوآورانه در پاسخ به چالش‌های پیش‌روی قربانیان داده‌محور را برجسته ساخته‌اند. نقض داده‌های شخصی، امروز دیگر صرفاً یک رویداد فناورانه یا فنی نیست، بلکه پدیده‌ای عمیقاً اجتماعی، اقتصادی و حقوقی تلقی می‌شود که با ارزش‌های بنیادین کرامت انسانی، امنیت عمومی و اعتماد اجتماعی در هم تنیده است و برای نظام عدالت مدنی، چالش‌برانگیز و پیامدآفرین است. این مقاله با رویکرد تطبیقی ـــ تحلیلی و با تکیه بر روش تحلیلی-توصیفی، در پی آن است تا ضمن تبیین و واکاوی ابعاد نظری و عملی آسیب به داده‌های شخصی، وضعیت و کارآمدی نظام مسئولیت مدنی ایران را در مواجهه با این آسیب‌ها مورد ارزیابی قرار داده و نسبت به مبانی، ارکان و چالش‌های احراز و جبران خسارت ناشی از آسیب به داده‌ها تحلیل ارائه دهد. همچنین با مطالعه و تحلیل دقیق مقررات GDPR اروپا، سعی خواهد

شد تا سازوکارها، ضمانت‌اجراها، حلقه‌های حمایتی و آموزه‌های این نظام پیشرو در عرصه حمایت از داده‌های شخصی، کشف، نقد و برای الهام‌بخشی به مقررات‌گذاری و اصلاحات حقوقی ایران پیشنهاد گردد.

پرسش بنیادینی که این پژوهش درصدد حل آن است، این است که: نظام حقوقی ایران چه ظرفیت‌ها، کمبودها، نقاط قوت و ضعف ساختاری برای تعیین و اجرای مسئولیت مدنی ناشی از آسیب به داده‌های شخصی دارد؛ این چالش‌ها چه تأثیری بر میزان حمایت واقعی از زیان‌دیدگان داده‌ای داشته و چگونه می‌توان از آموزه‌ها و تجربیات نظام GDPR اروپا برای تدوین، اصلاح و ارتقای سازوکارهای داخلی بهره برد؟ همچنین مقاله حاضر در پی تبیین جایگاه اقتصادی، اجتماعی و حقوقی داده‌های شخصی، نقد محدودیت‌های مقررات سنتی، روشن‌سازی چارچوب‌های نوین احراز مسئولیت و ارائه راهکارهایی اجرایی ـــ تقنینی جهت گذار از وضعیت فعلی و همسویی با تحولات جهانی است تا گامی مؤثر در ارتقای نظام حمایت از داده‌های شخصی و توسعه حقوق بنیادین افراد در ایران بردارد.

۱.۱. روش پژوهش

در پژوهش حاضر با هدف بررسی تطبیقی و تحلیلی مسئولیت مدنی ناشی از آسیب به داده‌های شخصی در حقوق ایران و مقایسه با مقررات GDPR اروپا، از روشی چندلایه و ترکیبی بهره گرفته شده که عبارت است از تلفیق روش توصیفی-تحلیلی با رهیافت تطبیقی و انتقادی.

ابتدا با مطالعه نظام‌مند منابع علمی داخلی و خارجی شامل کتاب‌ها، مقالات علمی – پژوهشی، گزارش‌های تخصصی، اسناد سیاستی و متون مقرراتی مرتبط با داده‌های شخصی، ابعاد مفهومی، ماهوی و اقتصادی داده‌های شخصی و جایگاه آن‌ها در حقوق ایران و اتحادیه اروپا احصاء و تبیین شده است. در این زمینه، تحلیل محتوای متون مقررات عمومی، به ویژه قانون مسئولیت مدنی ایران و مقررات GDPR اروپا (خصوصاً ماده ۸۲)، به عنوان بن‌مایه مقایسه تطبیقی مورد بهره‌برداری قرار گرفته است.

در ادامه، با تمرکز بر استفاده از روش تحلیلی ـــ انتقادی، ضمن واکاوی ساختار حقوقی و تقنینی ایران در مواجهه با آسیب به داده‌های شخصی، مؤلفه‌های اصلی مسئولیت مدنی و نقاط قوت و ضعف واکنش‌های قانونی و رویه‌ای کشور در برابر نقض داده‌های شهروندان تحلیل گردیده است. هم‌چنین، با بررسی رویه‌های قضایی موجود و سوابق دادرسی – هرچند محدود – در ایران و مطالعه نظامات جبران خسارت، به شناسایی محدودیت‌های عملی و چالش‌های اثبات دعوا، عناصر رکن تقصیر، اثبات رابطه سببیت و جنبه‌های حمایتی پرداخته شده است.

در بخش تطبیقی، مقررات GDPR اروپا به عنوان الگویی پیشرو مورد تحلیل دقیق قرار گرفته و از طریق مقایسه عناصر و سازوکارهای مسئولیت مدنی داده‌ای، ضمانت‌اجراها و حقوق زیان‌دیدگان، تفاوت‌ها و تشابهات بنیادین دو نظام مورد تأمل نقادانه قرار گرفته تا قابلیت‌های الهام‌بخش این مقررات برای اصلاح ساختارهای حقوقی ایران استخراج گردد. این مقایسه با تاکید بر تحلیل عمیق ماده ۸۲ GDPR، نظریه‌های جبران خسارت (مادی و معنوی) و نظام بار اثبات پیشرفته آن صورت پذیرفته است. در سطح آخر، روش تحلیلی مبتنی بر ارائه راهکارهای تقنینی، سیاستی و اجرایی برای بهبود و توسعه نظام حمایت از داده‌های شخصی و

ارتقای کارآمدی مسئولیت مدنی در ایران به کار رفته است. ترکیب مستمر یافته‌ها با آموزه‌های نظری و نمونه‌های عملی جهانی، به منظور ارائه پیشنهادهای عملیاتی و همسوسازی حقوق داخلی با معیارهای بین‌المللی رعایت شده است. در جمع‌بندی، این پژوهش از طریق ترکیب روش اسنادی (کتابخانه‌ای)، تطبیقی-تحلیلی و انتقادی، تلاش داشته است تا خلأهای نظری و عملی را شناسایی، چالش‌ها را صورت‌بندی و، بر اساس استانداردهای جهانی و تجارب موفق، راهبردها و راهکارهای بومی‌سازی‌شده ارائه دهد.

۲. بررسی مفهومی داده‌های شخصی و حمایت حقوقی از آن‌ها

۲-۱. تعریف و اقسام داده‌های شخصی

داده‌های شخصی (Personal Data) به مجموعه‌ای از اطلاعات اطلاق می‌شود که به طور مستقیم یا غیرمستقیم به یک شخص حقیقی قابل‌شناسایی اختصاص دارد؛ منظور از فرد قابل‌شناسایی شخصی است که بتوان به‌واسطه‌ی یک یا چند مشخصه‌ی شناخته شده—اعم از نام، نام خانوادگی، کد ملی، نشانی محل اقامت، شماره تماس، کدپستی، نشانی الکترونیکی، اطلاعات بانکی، شماره گذرنامه یا اطلاعات هویتی دیگر—او را بازشناسی کرد. اما داده شخصی تنها به این اطلاعات آشکار محدود نیست؛ بلکه داده‌های غیرمستقیم، مانند آدرس IP، داده‌های مکانی جمع‌آوری‌شده توسط دستگاه‌های هوشمند، سابقه جست‌وجو، الگوهای رفتاری، داده‌های حاصل از تراکنش‌های اینترنتی، داده‌های زیستی (biometric data) نظیر اثرانگشت، اسکن عنبیه، DNA و حتی صدا، چهره یا تصاویر ویدئویی نیز می‌تواند، به شرط آنکه به هویت فرد مربوط باشد یا امکان اتصال به هویت او را فراهم آورد، جزء داده‌های شخصی محسوب شود. (لطیف زاده و همکاران، ۱۴۰۲)

به طور کلی، داده‌های شخصی را بر اساس معیار محتوا و شدت حساسیت می‌توان به دو گروه عمده تقسیم کرد:

۱. داده‌های شخصی معمولی شامل اطلاعات شناسایی عمومی (مانند نام و نشانی، شماره شناسنامه، شماره ملی، تاریخ تولد، اطلاعات تحصیلی و شغلی) و داده‌های مربوط به وضعیت عمومی افراد.

۲. داده‌های شخصی خاص یا حساس (Sensitive Data) که ماهیتاً قابلیت ایجاد بیشترین آسیب را دارند و افشای آن‌ها تهدید یا تبعیضی جدی علیه فرد ایجاد می‌کند؛ مانند داده‌های قومیت، نژاد، مذهب، دیدگاه سیاسی، اطلاعات پزشکی، سلامت روان، سوابق کیفری، گرایش‌های جنسی یا داده‌های ژنتیکی و بیومتریک. مقررات GDPR اروپا این گروه از داده‌ها را صراحتاً مشمول حمایت مضاعف قرار داده، پردازش آن‌ها را فقط تحت شرایط محدود و ضوابط سخت‌گیرانه مجاز شمرده است.

در فضای سایبری، محدوده داده شخصی دائماً گسترده‌تر می‌شود و حتی داده‌های رفتاری (مانند اطلاعات مربوط به عادات خرید، مدل استفاده از اپلیکیشن‌ها، یا فعالیت در شبکه‌های اجتماعی)، داده‌های تحلیلی یا داده‌های مرتبط با دستگاه و سخت‌افزار نیز اهمیت یافته و بخشی از حریم داده‌ای فرد به شمار آمده‌اند. در حقوق ایران، هرچند قانون جامع در این زمینه تصویب نشده است، اما در اسناد سیاستی (نظیر سند امنیت فضای تبادل اطلاعات و سند دولت الکترونیک) و برخی مصوبات غیرالزام‌آور، تعاریفی نزدیک به استاندارد بین‌المللی از داده‌ها ارائه شده و حساسیت بالای نسبت به داده‌های خاص مورد تأکید واقع شده است.

۲-۲. ارزش اقتصادی و حقوقی داده‌های شخصی

در جهان پرشتاب امروز، داده‌های شخصی نه تنها واجد حیثیت شخصی و مرتبط با حریم خصوصی تلقی می‌گردند بلکه به منبعی قابل‌مبادله، سرمایه‌ای تجاری و دارایی ملموس مبدل شده‌اند. شرکت‌های بزرگ فناوری و پلتفرم‌های دیجیتالی (مانند گوگل، متا، آمازون و غیره)، چرخه حیات اقتصادی خود را بر گردآوری، تحلیل و پردازش کلان‌داده‌های شخصی کاربران بنیان نهاده‌اند و با استخراج الگوهای رفتاری و ترجیحات کاربران، فضای جدیدی برای بازارسازی، تبلیغات هدفمند و حتی تأثیرگذاری اجتماعی و سیاسی خلق نموده‌اند.

از جهت حقوقی، داده شخصی همزمان واجد دو جنبه آشکار است:

نخست، جنبه شخصی‌بودن که به کرامت انسانی، حفظ حریم خصوصی و آزادی‌های بنیادین فرد مربوط است و نقض آن می‌تواند آسیب معنوی، اضطراب روانی، لکه‌دارشدن اعتبار و محرومیت از فرصت‌های اجتماعی را در پی داشته باشد؛ دوم، ارزش اقتصادی داده که آن را به دارایی انتقال‌پذیر و قابل‌معامله بدل ساخته است. در حقوق مالکیت فکری معاصر و حقوق رقابت، داده‌های شخصی به عنوان دارایی‌های مورد حمایت، دارای ارزش مبادله در بازارها هستند. این ارزش بالا، انگیزه‌های فزاینده برای سوءاستفاده، فروش غیرمجاز، کلاهبرداری، اخاذی، جاسوسی صنعتی یا تحلیل‌های سیاسی را سبب شده و ضرورت برخورداری از نظام حقوقی قدرتمند برای تضمین حفاظت و جبران خسارات را دوچندان می‌سازد.

در سطح اجتماعی نیز، داده‌های شخصی – به سبب نقش‌شان در مدیریت سلامت، امور بانکی، آموزش، روابط اجتماعی و مدیریت هویتی– بخشی از زیرساخت نظام رفاه و حتی امنیت ملی را شکل می‌دهند و نقض، افشا یا انتقال غیرقانونی این اطلاعات، می‌تواند کل جامعه، بازار سرمایه و حاکمیت ملی را با تهدید روبه‌رو کند. (لطیف زاده و همکاران، ۱۴۰۱)

۲-۳. مروری بر مبانی حمایت از داده‌های شخصی

مبانی حمایت از داده‌های شخصی، ریشه در اخلاق، عرف، حقوق بشر و ضرورت حمایت از کرامت انسانی دارد. مستندات بین‌المللی متعددی چون اعلامیه جهانی حقوق بشر (ماده ۱۲)، میثاق بین‌المللی حقوق مدنی و سیاسی (ماده ۱۷) و کنوانسیون اروپایی حقوق بشر (ماده ۸) صراحتاً بر حق افراد بر حفظ حرمت زندگی خصوصی، مکاتبات و اطلاعات‌شان تأکید نموده‌اند و دولت‌ها را ملزم به حمایت عملی و تقنینی از این حقوق ساخته‌اند.

حمایت‌های حقوقی، معمولاً در سه لایه برقرار می‌شود:

۱. لایه ممنوعیت نقض آشکار: هرگونه جمع‌آوری، پردازش یا انتشار داده‌های شخصی بدون رضایت یا مجوز قانونی ممنوع شناخته می‌شود؛

۲. حقوق کنترلی فرد بر داده: هر فردی باید حق داشته باشد به داده‌های خود دسترسی داشته، آن‌ها را اصلاح یا حذف کند و نسبت به استفاده یا انتقال داده‌هایش اعتراض نماید؛

۳. الزامات شفافیت و مسئولیت‌پذیری: شرکت‌ها و نهادهای دارنده داده موظف به اطلاع‌رسانی، گزارش‌دهی و پاسخگویی در برابر سوءاستفاده یا رخنه‌های امنیتی هستند.

در ایران، با وجود فقدان قانون حمایت جامعی چون GDPR، پاره‌ای اسناد از جمله قانون اساسی (اصل ۲۲ و ۲۵)، قانون جرایم رایانه‌ای (مصوب ۱۳۸۸)، قانون تجارت الکترونیکی، قوانین مربوط به افشای اسرار پزشکی و راهنماهای تخصصی دستگاه‌های دولتی، بر لزوم صیانت از اسرار و اطلاعات شخصی و ایجاد مسئولیت مدنی ناشی از افشای غیرمجاز داده‌ها تأکید نموده‌اند. با این وجود، این قواعد به‌صورت پراکنده، غیرنظام‌یافته و عمدتاً ناظر به مصادیق خاص وضع شده‌اند و نظام‌مندی جامع و روزآمد ندارند.

۴-۲. اصول بنیادین حفاظت از داده‌های شخصی

حفاظت اثربخش داده‌های شخصی تنها به ممنوعیت افشا یا تعیین جرم‌انگاری محدود نیست؛ بلکه باید بر اصول بنیادین جامع‌نگری تکیه داشته باشد، اصولی که در اسناد بین‌المللی و به ویژه مقررات GDPR اروپا، ساختارمند و الزام‌آور گردیده است:

۱. اصل شفافیت (Transparency): پردازش داده‌ها باید کاملاً شفاف و برای فرد داده‌گذار، قابل فهم باشد؛ سازمان‌های جمع‌آورنده باید هدف، نوع، مدت نگهداری و نحوه‌ی استفاده از داده‌ها را صریحاً به فرد اعلام کنند.

۲. اصل محدودیت هدف (Purpose Limitation): جمع‌آوری داده باید صرفاً برای اهداف مشروع، مشخص و از پیش اعلام‌شده صورت گیرد و مصرف داده صرفاً در این چارچوب مجاز باشد.

۳. اصل حداقل‌گرایی داده (Data Minimization): داده‌هایی که جمع‌آوری یا نگهداری می‌شوند، باید محدود به مقداری باشد که برای تحقق هدف مذکور ضرورت دارد (جمع‌آوری داده‌ی مازاد ممنوع است).

۴. اصل دقت و صحت (Accuracy): تلاش معقول برای صحت داده‌ها پیش‌بینی شده و افراد حق درخواست اصلاح داده‌های نادرست را دارند.

۵. اصل امنیت (Security): حفظ داده‌های شخصی در برابر دسترسی غیرمجاز، افشا، مفقودی، تخریب یا پردازش غیرقانونی، از طریق انجام تدابیر فنی و سازمانی الزامی است.

۶. اصل قابلیت پاسخگویی (Accountability): نهاد پردازش‌کننده باید همواره قادر به اثبات رعایت اصول حفاظت از داده در برابر مراجع ذی‌صلاح باشد و در صورت کوتاهی پاسخگو است.

۷. اصل محدودیت نگهداری (Storage Limitation): مدت نگهداری داده باید به اندازه‌ای باشد که هدف پردازش محقق شود؛ پس از آن نگهداری داده ممنوع است مگر در موارد استثنایی قانونی.

۸. اصل رعایت حقوق موضوع داده (Data Subject Rights): افراد باید حق دسترسی، اصلاح، حذف (حق فراموش شدن)، و محدود کردن یا اعتراض به پردازش داده‌های خود را داشته باشند. (صحرائیان و زارع، ۱۳۹۸)

جدول ۱. مقایسه مبانی و عناصر مسئولیت مدنی در حقوق ایران و GDPR اروپا

مؤلفه / نظام	حقوق ایران	مقررات GDPR اروپا
مبنای مسئولیت	عموماً مبتنی بر تقصیر	مسئولیت محض و تقصیر، با گرایش به مسئولیت شبه‌محض
عناصر لازم	ورود ضرر، فعل زیان‌بار، رابطه سببیت	ورود ضرر، نقض مقررات داده، رابطه سببیت، احراز جبران خسارت (مادی یا غیرمادی)
تعریف داده شخصی	نبود تعریف قانونی جامع؛ تفسیر از اسناد سیاستی	تعریف دقیق، اعم از مستقیم و غیرمستقیم
اثبات تقصیر	بر عهده زیان‌دیده	اغلب بر عهده متولی داده (معکوس‌شدن بار اثبات)
حمایت از خسارات معنوی	محدود و وابسته به تفسیر قضایی	به رسمیت شناخته‌شده و دارای ضمانت‌اجرا
ضمانت‌اجراهای جبران خسارت	فاقد سازوکارهای تخصصی و مؤثر	ضمانت‌اجراهای مالی، نظارتی و بازدارنده، جبران فوری و متنوع

در مقررات اتحادیه اروپا (GDPR)، این اصول واجد ضمانت‌اجرای تقنینی و جبرانی قوی هستند، در حالی که در حقوق ایران، هنوز نبود قانون مستقل، اعمال غیرواحد و پراکنده‌نگری در این حوزه را باید از مهم‌ترین چالش‌ها دانست. اصول بالا به طور پراکنده در برخی دستورالعمل‌های بانکی و آیین‌نامه‌های داخلی دستگاه‌ها منعکس شده، اما وحدت رویه و قاعده‌گذاری ساختارمند ندارند.

از برآیند مباحث این بخش چنین نتیجه می‌توان گرفت که داده‌های شخصی، علاوه بر ماهیت شخصی و خصوصی‌شان، نقش محوری در مناسبات اجتماعی عصر حاضر یافته‌اند و نبود حمایت جامع، روشن و مبتنی بر اصول بین‌المللی، خطر تهدید حقوق فردی، اعتماد عمومی و امنیت ملی را مضاعف می‌کند. تصویب قانون خاص و استخراج اصول بنیادین لازم‌الاجرا—الهام‌گرفته از تجارب پیشرفته جهانی و به ویژه مقررات GDPR—پایه اصلاح و تحول نظام حقوقی ایران در حمایت اثربخش از داده‌های شخصی خواهد بود.

۳. چارچوب مسئولیت مدنی در حقوق ایران

۱-۳. مبانی و ارکان کلی مسئولیت مدنی

مسئولیت مدنی در حقوق ایران، چه در بستر فقه امامیه و چه با تأثیرپذیری از نظام‌های حقوق نوشته، دارای جایگاهی ریشه‌ای و بنیادین است. قاعده لاضرر، قاعده تسبیب و قاعده اتلاف ستون‌های مسئولیت مدنی را تشکیل می‌دهند. قانون مدنی ایران در ماده ۱ و ۲ قانون مسئولیت مدنی مصوب ۱۳۳۹، سه رکن اصلی را برای تحقق مسئولیت مدنی توصیه می‌کند:

۱. ورود ضرر مسلم به غیر: ضرر باید واقعی، محقق و قابل اثبات باشد و صرف احتمال ورود آسیب، واجد اثر حقوقی نیست.

۲. ارتکاب فعل زیان‌بار یا ترک فعل: خواه به صورت عمدی (با سوءنیت) باشد یا از طریق بی‌احتیاطی، بی‌مبالاتی یا قصور، و حتی گاه ترک فعل نیز اگر موجب ورود آسیب گردد، قابل پیگرد است.

۳. وجود رابطه سببیت مستقیم بین رفتار و زیان: اثبات این رابطه اغلب دشوار و پیچیده بوده و نیازمند ادله متقن است؛ اگر واقعه‌ای، شرایط را برای ورود ضرر مهیا کرده اما رابطه علیت نهایی وجود ندارد، مسئولیت شکل نمی‌گیرد.

نظریه تقصیر (Fault)، مبنای سنتی مسئولیت مدنی در ایران است؛ به این معنی که شخص تنها در صورتی مسئول شناخته می‌شود که مرتکب رفتاری خلاف عرف، قانون یا اخلاق شده و این رفتار منشأ آسیب باشد. با این حال در موارد خاص، مانند حوادث ناشی از فعالیت‌های خطرناک یا مالکیت برخی اموال، نظریه مسئولیت محض یا نوعی (Strict Liability) نیز در رویه دادگاه‌ها جاری شده است؛ جایی که اثبات صرف ورود زیان و رابطه سببیت برای احراز مسئولیت کافی است و نیاز به اثبات تقصیر مرتکب نمی‌باشد. مبانی نظری این قواعد از آموزه‌های فقهی (قاعده من أتلف) و نظریه‌های غربی، از جمله نظریه تضمین حق و خطر، تغذیه شده است. (صالحی حمیدرضا و همکاران، ۱۳۹۹)

ورود داده‌های شخصی به این ساختار سنتی در ابتدا امری غریب تلقی شد؛ زیرا بخش عمده دعاوی مسئولیت مدنی ایران، ناظر به آسیب‌های مادی معین (جسمی، مالی، تلف عین و منفعت) بوده و معیار سنجش ضرر عمدتاً خسارت فیزیکی یا معنوی شخصی بود. اما با تحول جایگاه داده‌ها در جامعه اطلاعاتی و تغییر مفهوم حریم خصوصی از حوزه خانوادگی و مکاتبات به قلمرو داده‌ای، ناگزیر پذیرش قلمرو موسع برای تعریف "ضرر" و بازتعریف مبنای مسئولیت ضروری شده است. در دهه‌های اخیر، بخشی از دکترین حقوقی ایران و حتی آرای متأخر دادگاه‌ها بر این نکته تأکید دارند که مسئولیت مدنی صرفاً محدود به ضررهای سنتی و مادی نیست و نسبت به ضررهای نوین از حیث فقدان اعتماد اجتماعی، نقض آزادی اطلاعاتی، سرقت هویت داده‌ای و جبران خسارت‌های غیرمالی، نیز باید پاسخگو باشد. از این‌رو مبنای مسئولیت در قبال داده‌های شخصی، می‌تواند از طرز تفکر فقه سنتی تا پذیرش مبانی مبتنی بر خطر یا تضمین حق، متغیر باشد؛ اگرچه تحقق این تحول در عمل با چالش‌های عمده مواجه است.

۲-۳. مفهوم ضرر، فعل زیان‌بار و رابطه سببیت

در نظام حقوقی ایران، تعریف "ضرر" واجد اصالت است و میان ضرر مادی، معنوی، مسلم و غیرمسلم تمایز گذارده شده است. شرایط احراز ضرر در دعاوی داده‌ای با موانعی جدی روبه‌روست، زیرا اغلب ضررهای ناشی از افشای داده یا رخنه امنیتی، ضمنی، بلندمدت، تراکمی و چندلایه‌اند و مدل ارزیابی خسارت سنتی پاسخگوی این پیچیدگی نیست.

ضرر مادی: مانند خسارت‌های مالی مستقیم (برداشت غیرمجاز از حساب، فروش داده به اشخاص ثالث، تحمیل هزینه‌های بازیابی هویت).

ضرر معنوی: نظیر خدشه به شخصیت اجتماعی، بی‌اعتمادی عمومی، اضطراب روانی یا آسیب به حیثیت و اعتبار.

اغلب دعوای دادهای، نمونه بارز تحقق ضرر غیرمادی است؛ زیرا برای اکثر اشخاص، زیان اصلی ناشی از خدشه به "حق انتخاب" و "کنترل" بر داده تلقی می‌شود. چالش قضایی اینجاست که اثبات ضرر معنوی یا فرهنگی اغلب نیازمند ادله قوی و کارشناسی است و برخی نهادهای قضایی ایران، در غیاب قانون خاص، استناد صریح به آن را نمی‌پذیرند.

در باب "رفتار زیان‌بار"، عمل می‌تواند شامل هر نوع افشای غیرمجاز، انتشار عمدی یا سهوی، پردازش ناامن، جمع‌آوری داده بدون رضایت یا حتی ترک مراقبت فنی لازم در صیانت از داده باشد. مضاف بر این، نحوه تعریف "رفتار قابل سرزنش" یا "تقصیر" در تعامل با داده‌ها غالباً محل مناقشه قرار دارد. آیا صرفاً خروج داده از سامانه، ولو بدون سوءنیت، تقصیر محسوب می‌شود؟ معیار احتیاط متعارف چگونه باید در امور داده‌ای سنجیده شود؟

اما "رابطه سببیت"، یکی از دشوارترین ارکان در دعاوی داده‌ای به‌شمار می‌رود. چرا که داده‌های شخصی عموماً در محیط‌های پیچیده و بین‌سازمانی پردازش و منتقل می‌شود؛ امکان رخداد همزمان چندین واقعه مخرب وجود دارد و تعیین اینکه دقیقاً کدام اقدام یا نارسایی فنی به رخداد ضرر منتهی شده، همواره شفاف نیست. تداخل عوامل ثالث (نظیر حملات سایبری از خارج کشور یا دسترسی غیرمجاز چندگانه)، پیچیدگی چرخه انتقال داده و نبود ثبت دقیق وقایع (logging)، اثبات رابطه علیت مستقیم یا عرفی میان رفتار مرتکب و زیان وارده را بسیار دشوار ساخته است. (شریفی‌کیا و شعبانی‌جهرمی، ۱۴۰۱)

۳-۳. جایگاه داده‌های شخصی در نظام مسئولیت مدنی سنتی

در فقه اسلامی و سنت حقوقی ایران، مفهوم "حریم خصوصی" عمدتاً هم‌ارز با "استتار منزل، مکاتبات، اسرار خانوادگی و اسرار شغلی" تلقی می‌گردد و داده‌های شخصی مدرن، به معنای مبتنی بر فناوری اطلاعات آن، عموماً در شمول مستقیم این مفاهیم سنتی قرار نمی‌گیرد. مسئولیت ناشی از افشای اسرار حرفه‌ای و اطلاعات خصوصی پزشکی یا تجاری، سالهاست با تکیه بر قواعد عام (اتلاف، تسبیب و منع ضرر) یا مقررات خاص (مانند افشای اسرار بیماران) حمایت می‌شود. اما داده به معنای دیجیتال، همچنان خارج از شمول مقررات سنتی باقی مانده است.

در مواردی از جمله افشای اسرار پزشکی، وجهی از داده‌های سنتی در بستر مقررات خاص مانند قانون مجازات اسلامی یا آیین‌نامه‌های بخش سلامت پوشش داده شده است. با این حال فضای مجازی و داده‌های حجیم (Big Data) با ویژگی سیالی، قابلیت تکثیر و ترکیب بی‌انتها، دامنه جدیدی از چالش‌ها را مطرح کرده که نظام سنتی قادر به پاسخگویی کامل به آن نیست. افزون‌براین، مقولات جدیدی چون "حق فراموشی"، "حق انتقال‌پذیری داده"، "حق بر کنترل داده شخصی"، یا "حق اعتراض به پردازش خودکار"، اصولاً جایگاهی در حقوق سنتی ایران ندارند و خلأ چشمگیر تقنینی در این حوزه وجود دارد.

۴-۳. مصادیق و چالش‌های نوین آسیب به داده‌های شخصی در ایران

در سال‌های اخیر، با رشد پایگاه‌های داده دولتی، نیمه‌دولتی و خصوصی، وقوع رخدادهای امنیتی گسترده‌ای نظیر نشت اطلاعات کاربران سامانه‌های شهری، تاکسی‌های اینترنتی، شبکه‌های آموزشی، بانک‌ها و بیمه‌ها، آسیب‌های جدی برای کاربران ایرانی به

همراه داشته است. با وجود این، چارچوب مسئولیت مدنی، نه تنها در شناسایی زیان‌دیده واقعی و تعیین خسارت جامع، بلکه در شناسایی مسئول (اعم از دارنده داده، پردازش‌گر، ثالث یا پیمانکار فناوری اطلاعات) با دشواری عینی روبه‌روست.

برخی از مصادیق رایج آسیب به داده‌های شخصی در ایران عبارتند از:

- نشت گسترده اطلاعات کاربران بانک‌ها یا موسسات اعتباری؛

- انتشار اسامی، نشانی، تصاویر و سوابق سلامت بیماران بدون رضایت؛

- استفاده شرکت‌های تبلیغاتی یا پلتفرم‌های نرم‌افزاری از داده‌های رفتاری مشتریان جهت تبلیغات هدفمند و تحلیل بازار بدون شفافیت و رضایت آگاهانه؛

- فروش بانک‌های شماره تلفن، ایمیل یا سایر داده‌ها به اشخاص ثالث و کلاهبرداران؛

- دستکاری و جعل داده‌های هویتی با هدف دسترسی به امکانات مالی یا سوءاستفاده از هویت افراد.

با وجود این، چالش‌های عملی متعددی در راستای حمایت از حقوق زیان‌دیدگان داده‌ای در نظام حقوقی ایران به چشم می‌خورد که برخی از مهم‌ترین آن‌ها عبارتند از:

۱. اثبات دشوار ضرر و رابطه سببیت: خصوصاً در مواردی که داده در اختیار چند مرجع قرار دارد یا وقوع ضرر به عوامل خارجی نیز وابسته است؛

۲. نادیده‌گیری و دشواری جبران خسارت‌های غیرمالی و معنوی: بسیاری از زیان‌های داده‌ای در قالب آسیب به اعتبار و حیثیت اجتماعی رخ می‌دهد که اثبات و ارزیابی‌یابی اقتصادی آن برای قربانی و دادگاه‌ها سخت و گاه ناممکن است؛

۳. نبود ضوابط روشن درباره سطح احتیاط، تکالیف پردازش‌گر داده و مفهوم تقصیر در فرآیندهای پیچیده داده‌ای:

۴. نبود ضمانت‌اجراهای منسجم و بازدارنده: چه از حیث ضعف ضمانت اجراهای کیفری در قوانین فعلی، چه عدم پیش‌بینی صریح مسئولیت تضامنی یا مجازات منع فعالیت حرفه‌ای یا جبران فوری خسارت؛

۵. ابهام در شناسایی مخاطب دعوا (data subject، data controller، data processor) و حدود صلاحیت مراجع رسیدگی: که گاه منجر به اطاله دادرسی یا بی‌پناه ماندن قربانی داده می‌شود؛

۶. فقدان رویه قضایی منسجم به دلیل نبود قانون خاص و تکیه بر تفسیرهای پراکنده و غیرقابل پیش‌بینی؛

۷. ضعف آگاهی حقوقی عمومی و حتی تخصصی نهادهای مقررات‌گذار و رسیدگی‌کننده: که گاه منجر به بی‌توجهی به ماهیت داده و آثار برجسته آسیب به آن می‌شود؛

۸. عدم شناسایی حقوق نوین موضوع داده نظیر حق فراموشی، محدودسازی پردازش یا حق دسترسی به داده در نظام حقوقی ایران که موجب شده است فضای دعاوی و راهکارهای عملی نیز برای زیان‌دیدگان تنگ و ناکارآمد باشد.

در تحلیل نهایی، می‌توان گفت که چارچوب فعلی مسئولیت مدنی ایران که بر مبنای قواعد عام و سنتی استوار شده، نه تنها نسبت به خصایص ذاتاً فناورانه داده‌های شخصی و پیامدهای عمیق آسیب به آن‌ها پاسخگو نیست، بلکه التزام کارآمد به صیانت از حقوق بنیادین داده‌ای و توسعه‌یافته را نیز دشوار ساخته است. این وضعیت، ضرورت بازنگری بنیادین در مبانی، ارکان و ضمانت‌اجراهای مسئولیت مدنی و الگوگیری هدفمند از نظام‌های پیشرفته ـــ به ویژه مقررات GDPR اروپا ـــ را اجتناب‌ناپذیر می‌سازد و به‌عنوان ضرورتی ملی و حقوقی باید مورد توجه تصمیم‌گیرندگان تقنینی و دادرسان قرار گیرد. (رهبری و مسعودی تفرشی ۱۴۰۳)

جدول ۲. انواع داده‌های شخصی و سطح حمایت قانونی

نوع داده شخصی	مثال‌ها	سطح حمایت در ایران	سطح حمایت در GDPR اروپا
داده‌های شناسایی عمومی	نام، نشانی، کد ملی، شماره تماس	حمایت محدود و غیرصریح	حمایت جامع و کامل
داده‌های خاص/حساس	سلامت، گرایش سیاسی یا مذهبی، داده ژنتیکی	فاقد قانون مستقل و ضمانت‌اجرا	حمایت ویژه و مضاعف
داده‌های رفتاری	سوابق جست‌وجو، تراکنش مالی، عادات خرید	تقریباً بی‌ضابطه	صراحتاً تحت شمول حمایت
داده‌های بیومتریک	اثر انگشت، عنبیه، چهره، صدا، DNA	بدون چارچوب الزام‌آور	محرمانگی و ممنوعیت جدی
داده‌های تحلیلی	تحلیل رفتار مصرف‌کننده، رتبه اعتباری	فاقد مقررات مشخص	پوشش کامل

۴. تحول مسئولیت مدنی در مواجهه با آسیب به داده‌های شخصی

۴-۱. ضرورت بازاندیشی در ارکان مسئولیت مدنی

ظهور و گسترش فناوری‌های نوین ارتباطی، به ویژه اینترنت، کلان‌داده‌ها، رایانش ابری و اینترنت اشیاء، مفهوم «ضرر»، «تقصیر» و «رابطه سببیت» را در مسئولیت مدنی بنیاداً دچار تحول کرده است. در جهان سنتی، این مفاهیم عموماً با رویدادهای مشهود و ملموس سر و کار داشتند: ورود آسیب به جسم، مال یا شهرت فرد با رفتار مستقیم و قابل مشاهده‌ی عامل زیان. اما امروز با جهانی شدن ارتباطات مجازی، آسیب به داده‌های شخصی نه تنها واجد ابعاد پنهان، تدریجی و شبکه‌ای است، بلکه اغلب بدون حضور مستقیم اشخاص، در فضای غیرمادی، و گاه توسط سامانه‌های خودکار داده‌ای پدید می‌آید.

همین ویژگی‌ها، تفسیر سنتی ارکان مسئولیت مدنی را با چالش جدی مواجه ساخته است. به عنوان نمونه، عنصر تقصیر که تکیه بر وجود عامدلنه‌بودن یا لااقل قصور فاحش دارد، ظرفیتی محدود در مواجهه با انواع جدید مخاطرات داده‌ای دارد. رخدادهایی نظیر

حملات هکری، آسیب رخ داده از طریق نقص نرم‌افزاری، یا پردازش ناآگاهانه داده توسط اپلیکیشن‌های فراگیر، اغلب نه با سوءنیت آشکار که با ضعف سیستماتیک یا فقدان تدابیر احتیاطی رخ می‌دهد. بنابراین، سنجش تقصیر باید بر اساس استانداردهای تخصصی امنیت اطلاعات، سطح هشدارپذیری، و ماهیت داده‌های پرداش‌شده بازتعریف شود.

در همین راستا، شاخص رابطه سببیت نیز نیازمند بازنگری است. ساختار شبکه‌ای و توزیع‌شده داده‌ها موجب شده که نشانه‌گذاری یک عامل بعنوان "سبب اصلی" ورود زیان دشوار گردد؛ در برخی موارد، چندین حلقه از تأمین‌کنندگان داده، پیمانکاران فنی، و واسطه‌های پردازشی به‌طور غیرمستقیم یا مشترک در پیدایش آسیب نقش دارند. از این رو، برخی حقوق تطبیقی، الگوهایی چون مسئولیت جمعی، شراکت در مسئولیت یا مسئولیت تضامنی زنجیره‌ای را برای مقابله با این وضعیت توصیه می‌کنند. چنین رویکردهایی، کارآمدی ارکان سنتی را عملاً به چالش می‌کشد و به خوبی نشان می‌دهد که دور شدن از صورت‌بندی‌های کلاسیک الزام‌آور و اجتناب‌ناپذیر شده است.

۲-۴. بررسی خسارت‌های مادی و معنوی ناشی از آسیب به داده‌های شخصی

آسیب به داده‌های شخصی دارای ماهیتی خاص و به مراتب پیچیده‌تر از زیان‌های کلاسیک است. داده‌های شخصی می‌توانند بستری برای اعمال مجرمانه نظیر سرقت هویت، جعل سند، اخاذی الکترونیک، نفوذ به حریم خصوصی یا حتی ارتکاب کلاهبرداری‌های مبتنی بر کلان‌داده مهیا کنند که آثار مالی مستقیم برای زیان‌دیده دارد؛ اما مهم‌تر از آن، بعد معنوی و فرهنگی آسیب به داده‌های شخصی است که در گذشته عمدتاً نادیده گرفته می‌شد. امروزه هرگونه افشای غیرمجاز، فروش، پردازش یا انتشار غیرمجاز داده‌های هویتی، رفتاری یا سلامت افراد می‌تواند منجر به هتک شخصیت، برهم خوردن امنیت روانی، لطمه به وجهه و اعتبار اجتماعی افراد شود و حتی به بحران‌های شغلی یا خانوادگی دامن بزند. ضرر معنوی در این حوزه اغلب به صورت اضطراب دائمی، کاهش اعتماد به نهادها، فقدان حس امنیت شخصی و زخم‌های روانی دیرپا نمایان می‌شود، که سنجش، اثبات و جبران آن‌ها بر خلاف خسارت‌های مالی، بسیار دشوارتر است.

در حقوق ایران نیز علی‌رغم پذیرش کلی مسئولیت مدنی بابت ضرر معنوی در برخی آرای محدود و مواد قانونی پراکنده (نظیر ماده ۱ و ۲ قانون مسئولیت مدنی)، هنوز ضابطه روشنی برای احراز و ارزیابی این نوع زیان‌ها در حوزه داده‌های شخصی وجود ندارد. تفاوت چالش‌ها در این است که گاه زیان‌دیده از افشای یک داده صرفاً متحمل احساس تهدید یا تحقیر شده ولی هیچ فایده مالی مستقیمی عاید عامل زیان نشده است. حال آنکه، جبران کامل و متناسب چنین آسیب‌هایی مستلزم پذیرش مفهوم گسترده‌تر خسارت معنوی و اتخاذ رویه‌های نوگرا در تحلیل، اثبات و ارزیابی ضرر است.

۳-۴. موضوع جبران خسارت و شیوه‌های جبران

مسئولیت مدنی در مواجهه با آسیب به داده‌های شخصی، صرفاً ناظر به جبران نقدی یا پرداخت وجوه مالی به زیان‌دیده نیست. انواع نوین زیان و گستردگی آثار آسیب داده‌ای، ضرورت پذیرش و توسعه مدل‌های جبران غیرنقدی را ایجاب می‌کند. در ساختارهای حقوقی پیشرفته، سه شیوه عمده جبران قابل شناسایی است:

۱. جبران عینی (Restitution): الزام عامل زیان یا دارنده داده به حذف داده‌های منتشرشده، اصلاح یا بازگرداندن داده به حالت اولیه، توقف پردازش غیرمجاز و تلاش برای اعاده وضعیت پیشین (Injunctive Relief).

۲. جبران نمادین یا معنوی (Moral/Symbolic Compensation): الزام به عذرخواهی رسمی، بیانیه عمومی به منظور احیای اعتبار فرد، یا ترتیبات ویژه برای اعاده حیثیت از دست رفته.

۳. جبران مالی (Pecuniary Compensation): پرداخت وجه نقد به عنوان خسارت مادی و معنوی با احتساب دشواری‌های ارزیابی در حوزه داده.

در نظام‌های نسبتاً پیشرفته مانند اتحادیه اروپا، ترکیب این راهکارها برای جبران خسارت متداول است و هر دعوا بر اساس نیازهای زیان‌دیده و نوع خسارت، ممکن است منتج به صدور چند حکم جبرانی توأمان گردد؛ حال آنکه، در نظام حقوق ایران عملاً تمرکز اصلی بر پرداخت وجه نقد یا دیه است و در موارد اندک، احکام تکمیلی مانند حذف داده یا عذرخواهی علنی صادر شده است. همین محدودیت، موجب انعکاس ناکافی آثار معنوی، روانی و اجتماعی آسیب به داده‌ها در فرآیند جبران خسارت شده و مانع تحقق عدالت جبرانی می‌گردد. مسئله مهم دیگر، امکان جبران فوری و دسترسی‌پذیر به جبران متناسب با زیان داده‌ای است: در حوزه داده، تأخیر در جبران ممکن است موجب تزاید ضرر یا انتشار وسیع‌تر داده گردد، از این رو، حقوق تطبیقی، جبران آنی، تضمین شده و قابل نظارت را لازم می‌داند، در حالی که در رویه حقوقی داخلی ایران، نه تنها ضمانت اجراهای فوری بلکه حتی سامانه اجرایی مؤثری برای حذف/اصلاح داده وجود ندارد. (حسین پور و همکاران، ۱۳۹۸)

۴-۴. مسئولیت تقصیری و مسئولیت محض؛ امکان‌سنجی تطبیقی و دروس آموزنده

حقوق سنتی ایران و بسیاری نظام‌های کلاسیک بر مبنای تقصیر، مسئولیت مدنی را ساز و ترتیب می‌دهند: اثبات ورود ضرر و رکن تقصیر شرط تحقق مسئولیت است. اما آسیب داده‌ای، به‌ویژه در محیط‌هایی با تعاملات گسترده و پیچیده مثل بانکداری، بیمه و سلامت، اغلب نتیجه ضعف فرایندها، خطاهای فنی یا حتی حملات غیرقابل پیش‌بینی است که احراز تقصیر عمدی را دشوار یا ناممکن می‌سازد.

بر همین اساس، الگوهای پیشرفته‌تر همچون GDPR اروپا، در موارد بسیاری، اصل را بر مسئولیت محض (Strict Liability) قرار داده، یعنی آستانه مسئولیت را از صرف اثبات تقصیر به کارایی اقدامات احتیاطی و قابلیت کنترل خطر منتقل کرده‌اند. در این‌جا پردازش‌گر داده موظف است فعالانه، سطحی متعارف از حفاظت و مراقبت فنی را رعایت کند و در صورت بروز آسیب، حتی اگر

حسن‌نیت خود را اثبات کند، مسئولیت جبران بر عهده او قرار می‌گیرد مگر آن‌که اثبات کند کلیه تمهیدات لازم را اتخاذ کرده است و زیان ناشی از شرایط "فوق‌العاده" یا عوامل خارجی بوده است.

تحلیل تطبیقی نشان دهنده خروجی‌های زیر است:

- پذیرش مسئولیت محض یا شبه‌محض، نه تنها مؤید حمایت پیشگیرانه و فعالانه از زیان‌دیده است، بلکه با منطق اقتصادی حقوق نیز همخوان است؛ زیرا هزینه وقایع آسیب‌بخش بر کسی بار می‌شود که قدرت کنترل بیش‌تری بر فرآیند دارد.

- الگوبرداری از این رویکرد می‌تواند شکاف ناکارآمد در حمایت از داده‌های شخصی در حقوق ایران را پر کند، مخصوصاً در حوزه‌هایی که ویژگی‌های فنی و مدیریتی داده بر رفتار عامل زیان غلبه دارد.

- در نهایت، مسئولیت محض نه تنها انگیزه ارتقاء استانداردهای فنی و رعایت مقررات محافظتی را تقویت می‌کند، بلکه آسیب‌پذیری قربانیان داده‌ای را تا حدود قابل ملاحظه‌ای کاهش می‌دهد و موجب ایفای بهتر عدالت جبرانی در حوزه زیان‌های نوین می‌گردد.

در مجموع، تحول نگرش از مسئولیت صرفاً تقصیری به مسئولیت محض یا شبه‌محض و تدوین ضمانت اجراهای متنوع و کارآمد، ضرورتی اجتناب‌ناپذیر در نظام حقوقی ایران برای صیانت از حقوق داده‌ای شهروندان و مقاربت مؤثر با چالش‌های عصر فناوری اطلاعات تلقی می‌شود. (حاج نجفی ۱۴۰۳)

۵. مسئولیت مدنی ناشی از آسیب به داده‌های شخصی در حقوق ایران

۵-۱. تحلیل ماهیت آسیب به داده‌های شخصی به‌عنوان ضرر

در منظومه فقهی و حقوقی ایران، مفهوم ضرر تنها منحصر به آسیب‌های مادی قابل لمس نیست، بلکه طیفی از خسارات معنوی، حیثیتی، روانی و اجتماعی نیز باید مورد شناسایی و حمایت قرار گیرد. داده‌های شخصی در بستر تحول جامعه اطلاعاتی، ورودی جدید به مقوله ضرر و آسیب به حیثیت فردی هستند و موجب گسترش قلمرو مسئولیت مدنی شده‌اند. گونه‌شناسی آسیب‌های داده‌ای نشان می‌دهد که نقض داده‌های شخصی غالباً منجر به ورود زیان‌هایی می‌شود که هرچند مستقیماً ارزیابی مالی آن‌ها آسان نیست، اما تأثیرات عمیق و پایداری بر جایگاه اجتماعی، آبرو، آسایش روانی، اعتماد عمومی و حتی فرصت‌های شغلی فرد بر جا می‌گذارند.

در رویه فقهی معتبر، زیان‌هایی همچون هتک حرمت، انتشار اسرار، افشای راز و لطمه به حسن شهرت از مصادیق خسارت معنوی به شمار آمده و قابل جبران شناخته شده‌اند. داده‌های شخصی، امروز جایگزین یا بسط مفهومی همان اسرار شخصی و حیثیتی هستند که فقهاء در قالب حق الناس نسبت به آن‌ها حساسیت جدی داشته‌اند. امروزه با توجه به گسترش روابط الکترونیکی، آسیب به داده‌های فردی، چه از طریق نفوذ، نشت و سوءاستفاده غیرمجاز و چه از طریق قصور متولیان فنی، مصداق جدیدی از ضرر تلقی می‌شود که علاوه بر آثار مالی، بر حقوق اساسی افراد در امنیت روانی و کرامت انسانی، خدشه وارد می‌سازد.

از منظر نظری، آسیب داده‌ای صرفاً به معنای ضرر نیست بلکه با تضعیف سرمایه اجتماعی، کاهش اعتبار هویتی، بی‌آبرویی و تحقیر در جامعه همراه است. در یک پرونده فرضی، اگر داده سلامت فردی بدون رضایت افشا شود و حتی نتیجه مادی بلافاصله نداشته باشد، می‌تواند آینده شغلی، موقعیت اجتماعی یا وضعیت خانوادگی وی را دگرگون ساخته و نقض حریم شخصی و آرامش فرد را در پی داشته باشد. این تلقی اقتضا دارد که مفهوم سنتی ضرر در مسئولیت مدنی توسعه یابد و مبانی فقهی ـــ حقوقی کشور با شرایط جدید منطبق گردد تا هیچ آسیبی بدون جبران مؤثر باقی نماند.

۲-۵. مصادیق مسئولیت مدنی

دامنه اشخاصی که ممکن است مسئولیت مدنی ناشی از آسیب به داده‌های شخصی متوجه آنان گردد، بسیار گسترده و متکثر است. نخست، متولیان مستقیم داده شامل اشخاص حقیقی نظیر مدیران سامانه‌ها، کارمندان امور فناوری اطلاعات، توسعه‌دهندگان اپلیکیشن‌ها یا مشاوران امنیت داده، که با سهل‌انگاری یا تخلف از تدابیر حفاظتی، موجبات آسیب را فراهم می‌آورند. افزون بر این، اشخاص حقوقی اعم از شرکت‌ها، نهادهای مالی، بیمه‌ای، بانکی، درمانی، پلتفرم‌های داده‌محور و حتی اپراتورهای ارتباطی، به سبب ایفای نقش کلیدی در گردآوری، پردازش و نگهداری اطلاعات اشخاص، در معرض طرح دعوای مسئولیت قرار دارند.

در موارد متعددی مسئولیت متوجه دستگاه‌ها و نهادهای دولتی نیز هست، به‌ویژه آنجا که داده‌های فراوانی اعم از سجلی، هویتی، تحصیلی یا پزشکی در اختیار ارگان‌های عمومی باشد و به علت ضعف سامانه‌های امنیتی، اطلاعات شخصیت حقیقی یا حقوقی در معرض افشا یا سوءاستفاده قرار گیرد. نقش پردازش‌گران داده (Data Processors) که به وکالت یا پیمانکاری از طرف متولیان اصلی دسترسی به اطلاعات دارند، از مصادیق نوین مسئولیت محسوب می‌شود. رفتار زیان‌بار ممکن است در قالب افشای عمدی داده، ترک فعل مثل عدم رفع آسیب‌پذیری سیستم، ارائه ناقص اطلاعات به صاحب داده یا حتی استفاده غیرمجاز و گسترده از داده‌ها به اغراض اقتصادی، سیاسی یا تبلیغاتی ظاهر شود. خلأ مهم دیگر، فقدان نظام جامع در تعیین استانداردهای فنی و رویه‌های عرفی برای رفتار متعارف در نگهداری داده است که موجب ناهمگنی در تشخیص مصادیق مسئولیت و تشتت آراء قضایی شده است. مسئولیت مدنی گاه متوجه یک شخص خاص و گاه به صورت مسئولیت جمعی میان عوامل متعدد و مشارکت‌کنندگان در زنجیره پردازش داده قابل طرح است. (پیشنماز و همکاران، ۱۴۰۲)

۳-۵. الزامات و حدود تقصیر در نقض داده‌های شخصی

در وضعیت فعلی قانون‌گذاری ایران، با فقدان قانون خاص حمایت از داده‌های شخصی مواجه هستیم، از این رو الزامات رفتاری متولیان داده عمدتاً مبتنی بر معیار عرف، ضوابط قراردادی، آیین‌نامه‌های موردی و اصول عام مسئولیت مدنی تحلیل می‌گردد. اصولاً از هر دارنده یا پردازش‌گر داده (اعم از حقیقی و حقوقی) توقع می‌رود که مراقبت متعارف فنی، به‌روزرسانی مستمر سامانه‌ها، آموزش کافی نیروی انسانی و اتخاذ تدابیر امنیتی را رعایت نماید تا مانع از نقض داده‌ها گردد؛ این معیار عرفی، با الزامات مقرر در دستورالعمل‌ها و دستورهای اجرایی خاص برخی نهادها تکمیل می‌گردد، اما نبود وحدت رویه سبب شده است ماهیت و دامنه تقصیر، نسبی و بسته به هر پرونده باشد.

از حیث مصداق‌یابی تقصیر، هرگونه سهل‌انگاری، بی‌توجهی به هشدارهای امنیتی، استفاده از رمزهای ضعیف، ناتوانی در مانیتورینگ رویدادهای غیرمجاز، عدم تعیین سطح دسترسی کاربر و تحصیل یا انتقال اطلاعات بدون رضایت تصریحی، می‌تواند به عنوان فعل یا ترک فعل زیان‌بار تلقی گردد. مع‌الوصف، کمبود مقررات الزام‌آور و پراکندگی استانداردها، اثبات و تعیین میزان تقصیر را دشوار ساخته است. در رویه کنونی، دادگاه‌ها با ارجاع به عرف متخصصان فناوری اطلاعات، نظرات کارشناسان امنیت داده و استانداردهای جهانی، تلاش دارند معیار ارزیابی رفتار متعارف را کشف کنند، اما فاصله جدی میان انتظارات متعارف بین‌المللی (مانند GDPR) و واقعیت قابلیت فنی داخلی ملموس است. همین ضعف و ابهام، بزرگ‌ترین چالش حقوق ایران در تعیین حدود تقصیر و تدوین ضوابط الزام‌آور تلقی می‌گردد.

۴-۵. آثار، ضمانت‌اجراها و دعاوی قابل طرح

آسیب به داده‌های شخصی، آثار و پیامدهای کوتاه‌مدت و بلندمدتی بر افراد و جامعه دارد. نخست، امکان طرح دعوی مدنی برای جبران خسارت به اشکال گوناگون فراهم است. زیان‌دیده می‌تواند از مرجع صالح تقاضای جبران هزینه‌های مالی (مانند خسارت ناشی از سرقت هویت، سوءاستفاده بانکی یا کلاهبرداری اینترنتی)، حذف داده‌های منتشرشده، توقف پردازش غیرمجاز، اعاده حیثیت از دست رفته و حتی صدور رأی عذرخواهی رسمی و جبران معنوی را نماید. علاوه بر این، مواد محدود قانون مجازات رایانه‌ای برخی ضمانت‌اجراهای کیفری همچون حبس، جزای نقدی یا محرومیت از فعالیت را برای برخی مصادیق افشای داده مقرر کرده است، اما این ضمانت‌ها پراکنده، غیرجامع و در عمل ناکافی است. در برخی دعاوی خاص، صدور دستور موقت برای جلوگیری از ادامه آسیب و الزام فوری به حذف یا اصلاح داده‌های آسیب‌دیده از محاکم خواسته می‌شود، هرچند اجرای مؤثر این دستورات به کمبود ظرفیت‌های فنی و اجرایی برخورد می‌کند.

برخی مواد قانون مسئولیت مدنی و اصول عام جبران خسارت در فقه امامیه از دیگر مبانی طرح دعوی و مطالبه حقوق زیان‌دیده محسوب می‌شود. با این وجود، فقدان یک نظام اختصاصی برای جبران خسارت ناشی از آسیب داده‌ای و محدود بودن ضمانت‌اجراها به ابزارهای مالی یا جزایی کلاسیک، پاسخگوی مخاطرات گسترده و پیچیده آسیب داده‌ای در عصر دیجیتال نیست و زمینه گسترش صدمه‌های جبران‌ناپذیر را فراهم می‌آورد.

۵-۵. چالش‌های اثبات و رسیدگی قضایی

یکی از مهم‌ترین موانع مؤثر بر دستیابی به جبران حق زیان‌دیدگان داده‌ای در ایران، دشواری‌های مربوط به اثبات وقوع آسیب، تعیین مسئول واقعی و مدیریت روند رسیدگی است. از یک سو، پیچیدگی فنی سامانه‌های داده‌محور سبب می‌شود تشخیص منشأ آسیب، نحوه و مسیر نشت داده و شناسایی عامل اصلی زیان بسیار دشوار باشد. آسیب داده‌ای معمولاً در بسترهای چندلایه و با حضور کارگزاران متعدد رخ می‌دهد، بنابراین تعیین سهم تقصیر و رابطه سببیت میان رفتار هر بازیگر فنی و زیان وارده، مستلزم دانش پیشرفته فنی و همکاری مؤسسات تخصصی است. از سوی دیگر، نهاد مرجع رسیدگی معمولاً فاقد تخصص کافی در حوزه داده و فناوری اطلاعات است و نمی‌تواند با سهولت لازم، جنبه‌های بیشتری از مقصر بودن یا نبودن متولی داده را تحلیل کند. ضعف

جدی در بدنه کارشناسان رسمی دادگستری با تخصص فناوری اطلاعات و محدودیت امکانات فنی مراکز قضایی سبب شده زیان‌دیدگان نتوانند سهل و سریع به احقاق حق دست یابند.

افزون بر این، نبود سازوکار پیگیری گروهی (Class Action)، ناتوانی از اثبات سهولت وقوع آسیب برای گروهی وسیع از افراد و هزینه‌های گزاف مطالبه حقوق داده‌ای در عرصه‌های قضایی و شبه‌قضایی، از عواملی است که عملاً سبب کاهش انگیزه زیان‌دیدگان برای طرح و پیگیری دعاوی مربوط به نقض داده‌های شخصی گردیده است. همین وضعیت، مطالبه تدوین آئین دادرسی خاص، ایجاد شعب متخصص رسیدگی و ارتقای سطح دانش قضایی را بیش از پیش مطرح می‌سازد. (باقری و همکاران، ۱۴۰۱)

۶. تحلیل مقررات و رویه مسئولیت مدنی در GDPR اروپا

۱-۶. معرفی کلی مقررات GDPR

مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (General Data Protection Regulation - GDPR) نقطه عطفی در تاریخ تحولات حقوق داده در عرصه بین‌الملل و الگوی اصلی برای توسعه قوانین ملی در کشورهای مختلف به شمار می‌آید. این مقررات در ۲۵ مه ۲۰۱۸ اجرایی شده و از آن تاریخ، کلیه اشخاص حقیقی و حقوقی که به هر نحو در پردازش داده‌های شخصی شهروندان اتحادیه اروپا مشارکت دارند را مکلف به رعایت ضوابط سخت‌گیرانه در جمع‌آوری، ذخیره، پردازش، انتقال و حذف داده‌های شخصی نموده است.

یکی از بزرگ‌ترین تمایزات GDPR با نظام‌های سنتی، نگاه مبتنی بر محوریت «کنترل آگاهانه و اختیاری فرد» بر داده‌های خود است؛ یعنی هرگونه عملیات داده‌ای بدون رضایت مشخص و شفاف فرد یا بدون مبنا و ضرورتی مندرج در قانون، غیرمجاز تلقی می‌شود. نظام رضایت در GDPR نه‌تنها به‌معنای اخذ رضایت‌نامه‌ای کلی و نامشخص نیست، بلکه باید با اطلاع‌رسانی کامل، شفاف و قابل فهم همراه باشد؛ انصراف از رضایت (حق بازپس‌گیری Consent) نیز در هر مرحله امکان‌پذیر است.

GDPR اصول متعددی را بر فرآیند پردازش داده حاکم نموده است، از جمله اصل محدودیت هدف (Data Minimisation)، اصل صحت داده‌ها (Accuracy)، اصل شفافیت (Transparency)، اصل امنیت و محرمانگی (Security and Confidentiality) و اصل پاسخگویی (Accountability). هر متولی داده ملزم به اثبات رعایت این اصول می‌باشد (اصل معکوس بار اثبات)، و هرگونه تخلف از الزامات، مشمول شدیدترین ضمانت‌اجراهای اداری، مدنی و کیفری اتحادیه اروپا می‌شود.

از سوی دیگر، قلمرو اجرایی مقررات فراتر از مرزهای جغرافیایی اتحادیه اروپا بوده و اصطلاحاً مفهوم «برون‌اقلیمی بودن» (Extraterritoriality) دارد؛ به این معنا که هر شخصیت حقوقی ولو خارج از اتحادیه، اگر داده شهروندان اروپایی را پردازش کند، ملزم به رعایت مقررات GDPR خواهد بود. همین خصیصه، این مقررات را تبدیل به یک معیار جهانی برای مسئولیت مدنی و انتظام‌بخشی رفتار فنی سازمان‌ها در حوزه داده‌های شخصی کرده است.

۲-۶. مبانی مسئولیت مدنی در GDPR

ماهیت مسئولیت مدنی در ساختار GDPR، با ترکیبی از «مسئولیت مبتنی بر تقصیر» و «مسئولیت شبه‌محض» تقنین یافته است؛ هدف این بوده که بیشترین سطح حمایت برای اشخاص داده‌دار ایجاد شود و قربانی نقض داده با موانع اثباتی مواجه نگردد. ماده ۸۲ این مقررات مقرر می‌دارد که هر شخصی که در نتیجه نقض این مقررات دچار زیان مادی یا معنوی شود، حق دارد در دادگاه‌های ملی اتحادیه اروپا یا محاکم محل وقوع حادثه، علیه کنترل‌کننده یا پردازش‌گر داده (Data Controller/Data Processor) دعوی اقامه کند و مطالب جبران خسارت نماید.

نکته مهم و تفاوت آشکار با مسئولیت مدنی سنتی و حتی با نظام حقوق ایران، آن است که در اینجا کنترل‌کنندگان و پردازش‌گران داده باید اثبات نمایند که در تحقق آسیب داده‌ای مرتکب هیچ‌گونه تخلف از الزامات قانونی نشده‌اند؛ به عبارت دیگر «مفروض بودن تقصیر» بر سود صاحب داده عمل می‌کند. در حالی که در حقوق سنتی اثبات عنصر تقصیر و causal link عمدتاً بر عهده زیان‌دیده است، در GDPR این روند معکوس شده تا حمایت حداکثری تضمین گردد.

در راستای ارتقاء استانداردهای رفتاری، مقررات GDPR علاوه بر پیش‌بینی جبران زیان‌های وارده، متولی داده را مکلف به اطلاع‌رسانی سریع به مقام ناظر و نیز فرد آسیب‌دیده می‌کند (Notification Obligation)، که نوعی مسئولیت پیشینی و پیشگیرانه است. همچنین هرگونه بی‌مبالاتی، عدم پیش‌بینی، اجرای ناقص استانداردهای فنی یا عدم تطبیق رویه‌های سازمانی با الزامات GDPR موجبات مسئولیت را فراهم می‌آورد. فلسفه چنین تدابیری، پیشبرد فرهنگ پاسخگویی، شفافیت و اعتماد عمومی به محیط فناوری اطلاعات است. (اسماعیلی و نریمان پور، ۱۴۰۳)

۳-۶. ارکان و شرایط تحقق مسئولیت مدنی در GDPR

تحقق مسئولیت مدنی در چارچوب GDPR، تابع شرایط مضیق اما شفاف است. اولاً باید اثبات گردد که پردازش داده، ناقض یکی از اصول یا ضوابط مندرج در مقررات بوده و این نقض اعم از فعل (اقدام به پردازش غیرمجاز) یا ترک فعل (خودداری از اجرای تدابیر امنیتی یا اطلاع‌رسانی لازم) مصداق دارد. ثانیاً اثبات وقوع ضرر برای داده‌دار (اعم از ضرر مادی یا غیرمادی) الزامی است؛ به این معنی که حتی صرف نگرانی، اضطراب، یا تجربه آسیب روانی نیز می‌تواند مبنای طرح دعوی قرار گیرد و لازم نیست زیان محدود به خسارت مالی صِرف باشد.

رکن سوم، رابطه سببیت میان نقض و زیان واردشده است؛ اما در این میان، بار اثبات فقط به صورت جزئی بر عهده زیان‌دیده باقی می‌ماند و کنترل‌کننده یا پردازش‌گر صرفاً در صورتی از مسئولیت معاف خواهد شد که به وضوح اثبات کند کلیه اقدامات معقول و متعارف مطابق با استانداردهای فنی، سازمانی و قانونی را رعایت کرده و حتی‌الامکان مانع تحقق آسیب شده است. این رویکرد، ایجاد توازن میان حمایت از داده‌دار و رعایت حقوق بنگاه‌های اقتصادی را مد نظر قرار داده است. در مجموع، مقررات GDPR با تفسیر موسّع از عناصر تحقق مسئولیت، سعی در کاستن از موانع اثباتی و بارز ساختن اصل حمایت حداکثری (Pro Data Subject) داشته و حتی در موارد مشکوک به نفع صاحب داده حکم می‌دهد. همچنین مسئولیت مدنی در GDPR به هیچ‌وجه محدود یا حصری نبوده و طیفی از ضمانت‌اجراها اعم از مدنی، کیفری و انتظامی را شامل می‌شود.

۴-۶. خسارات قابل مطالبه و شیوه‌های جبران

در سیاست‌گذاری GDPR، دامنه جبران خسارت بسیار وسیع و نوآورانه تعریف شده است. علاوه بر جبران سنتی مالی، زیان‌دیدگان می‌توانند جبران خسارات غیرمادی را نیز خواستار شوند؛ دادگاه‌های اروپایی سابقه دارند که نه‌تنها ضررهای مالی، بلکه خسارات حیثیتی، اضطراب، آسیب روانی، کاهش اعتماد، هتک آبرو، سختی در ادامه زندگی عادی و حتی نگرانی از سوءاستفاده‌های آتی را نیز مصداق خسارت قابل مطالبه شناسایی کرده‌اند. از منظر رویه عملی، جبران خسارت ممکن است به اشکال زیر تحقق یابد:

- بازیابی یا بازگرداندن وضعیت پیشین (Restitution): بازگرداندن داده‌ها به صاحب آن یا عودت وضعیت به پیش از وقوع آسیب؛

- حذف یا نابودی داده به دستور مقام قضایی؛

- الزام به توقف پردازش یا انتقال داده؛

- تهدید یا الزام به اطلاع‌رسانی عمومی و عذرخواهی رسمی نسبت به جمعیت آسیب‌دیده؛

- محکومیت به پرداخت غرامت مالی (Compensation)، که گاه در پرونده‌های مشهور به میلیون‌ها یورو بالغ شده است؛

- جبران جمعی یا شکایت گروهی، که امکان دستیابی جمعی آسیب‌دیدگان به جبران را تسهیل می‌کند.

سهولت دسترسی به دادگستری، تسهیل شیوه‌های اقامه دعوی از راه‌های برخط و حمایت نهادی از داده‌داران در کشورهای عضو اتحادیه اروپا، از عوامل کلیدی تحقق جبران عینی و مؤثر خسارات در قالب مقررات GDPR است. (احمدوند و همکاران، ۱۴۰۲)

۵-۶. نمونه‌کاوی‌های پرچالش و رویه‌های قضایی

در دهه اخیر، تطبیق عملی مقررات GDPR در نظام قضایی اتحادیه اروپا موجبات شکل‌گیری رویه‌های قضایی ارزشمند و بعضاً انقلابی شده است؛ از جمله:

- پرونده Google Spain SL v. Agencia Española de Protección de Datos (AEPD): حق «فراموش‌شدن» (Right to be Forgotten) به عنوان یک حق مسلم داده‌دار به رسمیت شناخته شد که شخص می‌تواند خواستار حذف اطلاعات قدیمی یا نادرست خود از پایگاه‌های اینترنتی شود، حتی در مواجهه با منافع عمومی یا آزادی بیان؛ این حکم گشاینده پرونده‌های فراوان مشابه و تقویت‌کننده استقلال فردی و جایگاه حقوقی اطلاعات شخصی بود.

- پرونده Schrems I II: احکام دیوان عدالت اروپا مبنی بر غیرقانونی بودن انتقال داده شهروندان اروپایی به ایالات متحده بدون تضمین‌های کافی حفاظتی، نمونه بارز سخت‌گیری در اعمال استانداردهای GDPR حتی در سطح بین‌المللی بود.

- جریمه‌های فزاینده علیه شرکت‌های بزرگ فناوری مانند Meta (Facebook)، Google، British Airways و سایر غول‌های داده‌ای که به دلیل نقص ساختاری امنیت داده، دیده‌بان‌های اتحادیه، آنان را به پرداخت جریمه‌های میلیون‌ها یورویی محکوم کردند، بیانگر اراده جدی در اجرای دامنه‌دار مقررات GDPR و پیشبرد عدالت تقسیم اطلاعات است.

در کنار این رویه‌ها، اتحادیه اروپا با ایجاد آژانس‌های نظارتی تخصصی (Data Protection Authorities)، سامانه‌های آنلاین اعلام تخلف و گزارش‌دهی مردمی، بستر اجرایی قوی و پشتیبان برای دفاع از حقوق داده‌داران فراهم نموده است.

۶-۶. حمایت ویژه از داده‌های گروه‌های آسیب‌پذیر

یکی از نوآوری‌های شایان توجه در مقررات GDPR، اهتمام جدی به حمایت مضاعف از داده‌های گروه‌های آسیب‌پذیر، به‌ویژه کودکان، اشخاص دارای معلولیت یا کسانی که از لحاظ فرهنگی یا اقتصادی ظرفیت کمتری برای دفاع از حقوق خود دارند، است. برای مثال:

- پرداختن به داده‌های کودکان: جمع‌آوری یا پردازش هرگونه داده مرتبط با اشخاص زیر سن قانونی، تنها با رضایت والدین یا سرپرست قانونی مجاز است و شرکت‌ها الزام دارند روش اطلاع‌رسانی را متناسب با سن و سطح درک کودک انجام دهند.

- داده‌های حساس (Sensitive Data): داده‌هایی نظیر اطلاعات سلامتی، تاریخچه ژنتیک، تمایلات سیاسی، مذهبی یا گرایشات جنسی، مشمول بالاترین سطح حفاظت قرار می‌گیرند و پردازش آن‌ها به جز در شرایط استثنایی امکان‌پذیر نیست.

- حمایت‌های فنی و سازمانی: ایجاد استانداردهای بالاتر امنیتی (مانند رمزنگاری سراسری، ممیزی‌های فنی مستمر، ممیزی‌های سالیانه)، الزام به حضور مسئول حفاظت داده (Data Protection Officer) و ارائه آموزش‌های فراگیر.

این سازوکارها، الگویی الهام‌بخش برای دیگر کشورها بوده و حتی برخی از اسناد بین‌المللی (مانند کنوانسیون ۱۰۸ شورای اروپا) تلاش دارند این الگوی موفق را ترویج دهند.

در مجموع، مقررات GDPR الگویی است برای مسئولیت مدنی فراتر از سنت‌های ملی، با محوریت ایجاد توازن بین توسعه فناوری و حمایت همزمان از حیثیت و کرامت انسانی. این مقرره با شفاف‌سازی ارکان تحقق مسئولیت، تقویت ضمانت اجراها، ارائه ابزارهای متعدد جبران و به‌ویژه حمایت ویژه از گروه‌های آسیب‌پذیر، نقطه عطفی در ادبیات حقوق داده در مقیاس جهانی ایجاد نموده است. نهادینه‌سازی چنین رویکردی در نظام‌های غیراروپایی ـ از جمله ایران ـ مستلزم بازنگری جدی در مبانی، رویه‌ها، ساختار اجرایی و توسعه زیرساخت‌های حقوقی داده‌های شخصی است. (میرشکاری و دیگران، ۱۴۰۳)

جدول ۳. چالش‌های کلیدی اجرای مسئولیت مدنی داده‌ای در ایران

چالش	شرح	پیامدها	وضعیت فعلی مقررات

فقدان قانون خاص داده‌های شخصی	نبود قانونی مستقل و جامع	ناتوانی در حمایت عملی، سردرگمی قضات	جدی
ضعف اثبات دعوا	بار اثبات بالا برای زیان‌دیده	محرومیت از جبران خسارت	شایع
نبود نهاد نظارت تخصصی	فاقد سازمان مستقل برای رسیدگی	ضعف در اجرای آراء و تضمین حقوق	شدید
کمبود ضمانت‌اجراهای بازدارنده	نبود جرایم و مقررات ویژه	نبود ضمان کافی علیه متخلفان	جدی
حمایت ضعیف از خسارات معنوی	تردید در جبران زیان غیرمادی	تحدید دامنه جبران، تبعیض	بسیار محدود

۷. مقایسه تطبیقی مسئولیت مدنی: ایران و مقررات GDPR

۷-۱. مقایسه مفهومی و ارکان مسئولیت

مسئولیت مدنی در ایران بر سه رکن سنتی خسارت، تقصیر و رابطه‌ی سببیت بنا نهاده شده و این ارکان به‌عنوان ستون‌های اصلی دعاوی مدنی تلقی می‌شوند. از دیدگاه مفهومی، نقض الزام‌های قانونی صرفاً زمانی موجب مسئولیت می‌گردد که ضرر مسلم، تقصیر معین و رابطه علیت میان آن‌ها احراز شود و بار اثبات عمدتاً بر عهده‌ی متضرر است. بدین معنا که اثبات وقوع ضرر، احراز وجود فعل یا ترک فعل زیان‌بار (با معیار فرد متعارف) و در نهایت، ارائه دلیل متقن بر این‌که ضرر مستقیماً ناشی از رفتار عامل است، ضرورت دارد. به‌ویژه در حوزه داده‌های شخصی، این روند سنتی با انواع پیچیدگی‌های اثباتی، فنی و تفسیر مبهم از مفاهیم مواجه است؛ به‌خصوص در جایی که آسیب غیرمادی (از جمله هتک حرمت، اضطراب، خدشه بر اعتماد یا آسیب به آبرو) رخ می‌دهد و سازوکار نظری روشنی برای سنجش کیفیت و کمیت چنین خساراتی وجود ندارد.

در مقابل، مقررات GDPR رویکردی متحول و متناسب با تحولات فناوری اطلاعات اتخاذ کرده است. در این الگو، مسئولیت مدنی ناشی از آسیب به داده‌های شخصی، عمدتاً بر مبنای مسئولیت محض یا شبه‌محض (strict liability) تعریف شده است؛ به این معنا که صرف وقوع آسیب به واسطه نقض تکالیف مقرر در پردازش داده، فارغ از اثبات سنتی تقصیر، می‌تواند سبب مسئولیت مدنی گردد. بر این اساس، مسئولیت متولیان داده شخصی (چه کنترل‌کننده و چه پردازشگر) نه با استناد به اثبات تقصیر بلکه با اصل مفروض بودن رعایت‌نشدن الزامات قانونی و معکوس شدن بار اثبات شکل می‌گیرد — بدین ترتیب که مدعی کافی است نشان دهد داده‌ی او بر خلاف تکالیف GDPR آسیب دیده و اینک متولی داده باید با اسناد و مدارک قابل قبول نشان دهد تمامی اقدامات احتیاطی لازم را رعایت نموده است.

تفاوت بنیادی دیگر در شمول و تنوع ضررهاست؛ در نظام ایران، خسارت معنوی و غیرمادی گرچه در برخی رویه‌های دادگاه‌ها پذیرفته شده اما وحدت‌رویه‌ای نداشته و جبران آن غالباً در هاله‌ای از ابهام قرار دارد. در حالی‌که GDPR با رسمیت و تأکید بسیار،

خسارات واقعا متنوع از آسیب‌های مالی تا رنج روانی، تضعیف جایگاه اجتماعی، اضطراب، احساس ناامنی، خسارت شخصیتی و سایر لطمه‌های غیرمادی را واجد اعتبار مدنی و قابل جبران می‌داند. (شریفی‌کیا و شعبانی‌جهرمی، ۱۴۰۱)

۲-۷. تفاوت و تشابه مبنای مسئولیت

از حیث مبنا، حقوق ایران عمدتاً متاثر از نظریه تقصیر و آموزه‌های فقهی است. در نتیجه صِرف نقض قاعده رفتاری (مانند افشای اشتباه یا ناایمن داده‌ها) الزاماً به مسئولیت نمی‌انجامد، مگر آنکه عملکرد پردازشگر داده معیاری از قصور یا تعدی را نشان دهد. بار اثبات بر عهده زیان‌دیده است و دادگاه تنها در فروض استثنایی مسئولیت شبه‌محض (همانند مواد معدودی از قانون مسئولیت مدنی یا مواد قانون مدنی در رابطه با ضمان قهری) را اعمال می‌کند. این امر موجب سختی فراوان برای بزه‌دیده، پیچیدگی‌های قضایی، افزایش احتمال نقض و ناکارآمدی رویه‌های حمایتی شده است.

در روش اروپایی و بر اساس GDPR، با پذیرش مسئولیت شبه‌محض، تمرکز بر «نتیجه» و «فراهم‌آوردن بالاترین سطح حمایت» است. این شاخصه موجب می‌شود که به محض وقوع آسیب داده‌ای و اثبات نقض الزامات تعیین‌شده (برای نمونه، پردازش غیرقانونی یا امنیت ناکافی)، مسئولیت مدنی بدون توجه به اثبات قصور یا تقصیر شخصی الزام‌آور گردد. تنها راه رهایی برای متولی داده آن است که اثبات کند تمامی اقدامات معقول و مقتضی را برای پیشگیری از آسیب انجام داده یا حادثه ناشی از قوه قهریه یا تقصیر شخص ثالث بوده است. این رویکرد در عمل، مکانیسم حمایت از حقوق داده‌دار را تاحدود زیادی مطمئن، سریع و کم هزینه کرده است و نقش عدالت جبرانی را تقویت می‌نماید.

در هر دو نظام، اشتراک در آن است که نقض الزام‌های قانونی در زمینه داده شخصی، می‌تواند آبستن مسئولیت‌های مدنی باشد؛ اما رویکرد اثباتی و دامنه‌ی حمایت، اساسا متفاوت و در اروپا کارآمدتر و حمایتی‌تر است. (رهبری و مسعودی تفرشی ۱۴۰۳)

۳-۷. مقایسه ضمانت‌اجراها و شیوه‌های جبران

در نظام سنتی حقوق ایران، ضمانت‌اجراها شدیداً محدود و در اغلب موارد به پرداخت وجه نقد یا بعضا دیه منتهی می‌شود؛ هرچند قانون جرایم رایانه‌ای برای برخی مصادیق نقض داده، ضمانت‌های کیفری مثل حبس یا جزای نقدی در نظر گرفته، اما چارچوب روشن و سازمان‌یافته‌ای برای جبران مجموعه‌ای از خسارات اعم از مادی و معنوی وجود ندارد. مکانیسم‌های جبران غیرمالی ـ مانند الزام به حذف داده، توقف پردازش غیرقانونی، عذرخواهی رسمی یا بازگرداندن وضعیت پیشین ـــ یا پیش‌بینی نشده یا فاقد قابلیت اجرایی قابل اتکا هستند. حتی در مواردی که دادگاه خسارت معنوی را شناسایی کرده، نحوه ارزیابی و میزان آن اغلب دلبخواهی و غیرشفاف است.

در مقابل، GDPR مجموعه‌ای گسترده از ضمانت‌اجراها را پیش‌بینی کرده است که ترکیبی از ابزارهای مدنی، کیفری، انتظامی و حتی اداری را در بر می‌گیرد. جریمه‌های مالی، عموماً با توجه به گردش مالی سالانه شرکت‌ها یا سازمان‌ها تا سقف ۴ درصد یا ۲۰ میلیون یورو (هرکدام بالاتر باشد) وضع می‌شود. افزون بر آن، دستور توقف فعالیت‌های پردازشی، حذف داده‌ها، اطلاع‌رسانی عمومی

به آسیب‌دیدگان، الزام به بازگرداندن اطلاعات، تعلیق یا لغو پروانه فعالیت و ثبت تخلف در سوابق شرکت‌ها از مصادیقی است که اجرای آن‌ها حجم سنگینی از آثار مثبت جبرانی و بازدارندگی را به همراه دارد. حمایت از اقامه دعوای گروهی یا Class Action و تسهیل اقامه دعوا در بستر آنلاین نیز امکان جبران دسته‌جمعی و دسترسی همگانی به عدالت داده‌ای را فراهم می‌کند.

۴-۷. تحلیل چالش‌های اجرایی و اثبات دعوا

هرچند در سطح نظری، تفاوت ساختاری میان نظام ایران و GDPR در زمینه اثبات و اجرای مسئولیت آشکار است، اما در عمل هر دو نظام با چالش‌هایی مواجه‌اند. در ایران، نبود نهاد مستقل ناظر بر داده‌ها (نظیر Supervisory Authorities اروپایی)، ضعف آموزش قضایی و تخصص فنی، نبود بانک‌های اطلاعاتی و ردیابی دقیق عاملین آسیب داده‌ای و چندوجهی بودن زنجیره پردازش داده، عمده‌ترین موانع هستند. ساختار غیرمتمرکز پردازش و پیچیدگی‌های فناوری مانند استفاده از بسترهای ابری، داده‌های توزیع‌شده و چندکاربره و حتی اجرای پردازش توسط الگوریتم‌ها و سامانه‌های بی‌نام و نشان، شناسایی دقیق عامل زیان و تعیین مسبب نهایی را دشوار ساخته‌اند.

در مقایسه، گرچه GDPR بواسطه حضور مستمر نهادهای ناظر (اعم از آژانس‌های ملی و کمیسیون اروپا)، همکاری فرامرزی و سازوکارهای پیشرفته گزارش‌دهی، اغلب مشکلات فوق را تا حد زیادی مدیریت کرده، اما در مواردی مانند تقاطع مرزهای ملی یا انتقال داده به خارج از اتحادیه اروپا، هم‌چنان چالش‌های فنی، حقوقی و اجرایی قابل اعتنایی باقی است. افزون بر آن، اتخاذ رویکرد «بار اثبات معکوس» در GDPR، اگرچه به نفع قربانی است اما گاه برای کسب‌وکارهای کوچک هزینه بالایی ایجاد می‌کند و می‌تواند مورد سوءاستفاده‌های احتمالی نیز واقع شود. (حسین پور و همکاران، ۱۳۹۸)

۵-۷. انتقال تجربیات مقررات اروپایی به نظام ایران

در پرتوی نقاط ضعف و قوت دو نظام، انتقال تجربیات مقررات اروپا به نظام حقوقی ایران می‌تواند زمینه‌ساز تحول بنیادین در حوزه حمایت از داده‌های شخصی باشد. نخستین و شاید مهم‌ترین راهکار، تدوین قانون جامع و شفاف در زمینه حفاظت و جبران آسیب داده‌های شخصی است؛ قانونی که علاوه بر تعریف دقیق داده شخصی و انواع خسارت، ساختار منسجم برای ارزیابی و جبران انواع خسارت‌های مادی و غیرمادی داشته باشد. گام دوم، واگذاری بار اثبات عدم تقصیر به عامل پردازش داده، در راستای رفع موانع اثباتی در نظام کنونی و تقویت ضمانت اجرایی حمایت از زیان‌دیدگان داده‌ای است.

همچنین، تاسیس یک نهاد مستقل و تخصصی ناظر بر حفاظت داده‌ها شبیه به Supervisory Authorityهای اروپا، ضرورت دارد؛ نهادی که همزمان بر سیاست‌گذاری، آموزش و ارتقاء دانش فنی و نیز رسیدگی به شکایات و گزارش‌ها نظارت کند. توسعه ضمانت‌اجراهای غیرمالی ـــ نظیر الزام به توقف پردازش، عذرخواهی عمومی، بازگردانی اطلاعات یا محدودسازی فعالیت ـــ می‌تواند بسته حقوقی جبران را به استانداردهای جهانی نزدیک‌تر نماید. علاوه بر این، ترویج فرهنگ مطالبه‌گری و ارتقاء آگاهی عمومی در خصوص هشدارهای نقض داده، داشتن حق اطلاع‌رسانی و حذف اطلاعات از پایگاه‌های آنلاین ـــــ همانند گذاره‌ی «حق

فراموش‌شدن» اروپایی ـــــ از دیگر مقولاتی است که می‌بایست مورد توجه قانونگذار ایرانی قرار گیرد. نهایتاً، همگرایی حقوقی با مقررات بین‌المللی، پیوستن به کنوانسیون‌های جهانی (مانند کنوانسیون ۱۰۸ شورای اروپا)، و تبادل اطلاعات نهادی و دادگاهی میان ایران و سایر کشورها، می‌تواند فصلی نو در حمایت مؤثر از داده‌های شخصی ایرانیان رقم بزند و با فراهم شدن زیرساخت‌های حقوقی، فنی و اجرایی، زمینه عدالت داده‌ای را در کشورمان تقویت نماید. (پیشنماز و همکاران، ۱۴۰۲)

۸. آینده‌پژوهی و راهکارهای پیشنهادی

۸-۱. ضرورت تدوین قانون خاص حفاظت از داده‌های شخصی

در جهان معاصر که داده‌های شخصی نقش غیرقابل‌انکاری در روابط اجتماعی، اقتصادی و حتی هویتی شهروندان ایفا می‌کند، ضعف قانونگذاری و فقدان چارچوب منسجم و جامع در عرصه حمایت از داده‌های شخصی در ایران، یکی از چالش‌های اساسی نظام حقوقی و تقنینی به شمار می‌رود. با تحول فضای سایبر و ظهور فناوری‌های نوین همچون اینترنت اشیا، هوش مصنوعی، کلان‌داده و خدمات فناوری ابری، تهدیدات متنوعی متوجه امنیت داده‌ها، محرمانگی و حریم خصوصی افراد شده است که هیچ‌یک از مقررات جزئی پراکنده کنونی (اعم از قانون جرایم رایانه‌ای و برخی آیین‌نامه‌های بخشی) قادر به تأمین حمایت کافی و ضمانت‌بخش برای حفاظت از این سرمایه‌های معنوی و شخصی نیستند.

آنچه بیش از پیش اهمیت دارد، طراحی و تصویب قانونی مستقل و جامع، با رویکردی حمایت‌محور مبتنی بر حقوق بنیادین بشری و معیارهای بین‌المللی، به ویژه استانداردهای مستقر در مقررات GDPR اروپا است. چنین قانونی می‌باید ضمن تعریف شفاف داده‌های شخصی و تعیین مصادیق آن، الزامات و حدود جمع‌آوری، پردازش، ذخیره‌سازی، افشا و انتقال داده‌ها را با دقیق‌ترین رویکرد ممکن تدوین کند. بارزترین عنصر این قانون، شناسایی مسئولیت محض متولیان داده نسبت به هرگونه آسیب، تعریف انواع ضمانت‌اجراهای متنوع اعم از مدنی، کیفری، انتظامی و حتی جبران معنوی، و برقراری اصول اساسی همچون حق دسترسی، حق اصلاح، حق حذف (حق فراموش شدن)، اطلاع‌رسانی شفاف و امکان اعتراض به پردازش‌های غیرمجاز است.

ضروری است که در این قانون، حق مالکیت معنوی و کنترل شخص بر داده‌های خود به عنوان حقی ذاتی و غیرقابل‌سلب شناخته شود؛ همچنین راهکارهایی برای جبران خسارات گروهی، پیش‌بینی رژیم خاص خسارت‌های غیرمادی (مانند اضطراب، خدشه به حیثیت، کاهش اعتماد و آسیب به آبرو) و طراحی سازوکارهای نظارتی قوی توسط نهاد یا مرجع تخصصی و مستقل لحاظ گردد. بدون چنین تحولی، نظام فعلی ایران در برابر گسترش فناوری و ضرورت حفظ حقوق فردی آسیب‌پذیر و ناکارآمد خواهد بود.

۸-۲. الگوبرداری عالمانه از مقررات GDPR

مقررات GDPR اروپا به‌مثابه‌ی یک مدل موفق، جامع و فراملی در عرصه حمایت از داده‌های شخصی، می‌تولند الهام‌بخش قانونگذاری در ایران باشد. تحلیل تطبیقی نشان می‌دهد که GDPR فراتر از صرف مقررات فنی، یک نظام حمایتی عدالت‌محور است که بر اصل کرامت انسانی و حق بنیادین بر داده استوار گردیده است. در این چارچوب، مواردی نظیر شناسایی خسارت معنوی و

غیرمالی و ضـــرورت جبران واقعی آن، الزام به انتقال بار اثبات تقصـــیر و رعایت الزامات قانونی به متولی داده (و نه قربانی)، تعیین جایگاه نهادی مسـتقل و مقتدر برای نظارت و رسـیدگی بر دعاوی داده‌ای، طراحی سـازوکارهای بازدارنده چون جریمه‌های سـنگین مالی، ممنوعیت یا محدودیت پردازش، الزام به اطلاع‌رسانی فوری در صورت بروز رخداد داده‌ای، و حقوق شـناخته‌شده‌ای چون حق دسترسی، اصلاح، حذف و حتی انتقال داده، همگی می‌تواند در فرایند قانونگذاری ملی ایران بومی‌سازی و الگوبرداری شود.

افزون بر این، شـفافیت در فرایند جمع‌آوری و پردازش، تصـریح در مورد رضـایت آگاهانه و قابل بازپس‌گیری، حق تعیین سـرنوشـت داده‌ها بعد از قطع همکاری با سازمان، الزام به پاسخگویی سریع و موثر متولیان، توسعه ابزارهای کنترل و رصد رفتار داده‌ای توسط اشخاص ثالث، و حمایت ویژه از گروه‌های آسیب‌پذیر چون کودکان و سالمندان از مؤلفه‌هایی است که در طراحی حقوقی آینده باید به آنها پرداخته شـود. اتکای صـرف به مقررات کیفری یا تحدیدگرایانه، نه تنها پاسـخگوی مؤثر خدشـه به داده‌های شـخصـی نیسـت بلکه در عمل موجب پیچیدگی، اطاله دادرسی و افزایش احتمال فرار از مسئولیت متولیان داده نیز خواهد بود.

۸-۳. اصلاح بنیادین رویه‌های دادرسی و بار اثبات دعوا

یکی از مهم‌ترین کاستی‌های نظام کنونی ایران، فقدان رویه‌های تخصصی، بروز و سازگار با ویژگی‌های فنی و پیچیده دعاوی داده‌ای است. در شرایط فعلی اثبات دعوا به ویژه بار اثبات وقوع خسارت و رابطه سببیت، چالشی بزرگ برای زیان‌دیدگان محسوب می‌شود و بسیاری از جبران‌های مورد نیاز، به سبب عدم وجود ساختارهای فنی و قضایی، ناکام می‌ماند. آینده تقنین و اجرا در این حوزه در گرو ایجاد شعب تخصصی در دادگاه‌ها و تمرکز بر توانمندسازی قضات و کارکنان دستگاه قضایی در حوزه فناوری اطلاعات و حقوق داده است.

همچنین، ضـروری اسـت نظام کارشـناسـی دعاوی داده‌ای تغییر یابد؛ بدین معنا که به جای کارگروه‌های سـنتی، ارکان کارشـناسـی مرکب از متخصصان حقوقی و فنی داده و امنیت سایبری ایجاد شود تا گره کور پرونده‌های داده‌ای زودتر و با دقت بالاتری باز شود. هسـته مرکزی تحول، معکوس‌سازی بار اثبات تقصـیر اسـت؛ یعنی بر خلاف شـیوه سـنتی نظام مدنی ایران (که زیان‌دیده را به اثبات تقصـیر مکلف می‌کند)، بر اسـاس رویکرد GDPR عامل داده ملزم اسـت اثبات نماید اقدامات لازم برای پیشـگیری از هرگونه آسـیب احتمالی را انجام داده و تمامی استانداردهای امنیتی و مراقبتی را رعایت نموده است. تحقق این تحول دادرسی، موجب کاهش اطاله رویه؛ سهولت جبران خسارت واقعی و ارتقاء سطح اعتماد به نظام قضایی خواهد شد.

۸-۴. توسعه نظریه حقوق بنیادین داده و تضمین جبران مؤثر و واقعی خسارت

در دهه‌های اخیر، روند حقوق بشر و آزادی‌های شـهروندی به سـمت شـناسـایی «حق بر داده» (Right to Data) گام برداشـته اسـت و از صـــرف یک مفهوم تکنولوژیک فراتر رفته و جنبه‌ای هویتی، شـــخصـــیتی و نهادی یافته اســـت. آینده نظام حقوقی ایران برای پاسـخ‌گویی موثر به آسـیب‌های داده‌ای، مسـتلزم آن اسـت که حق بر داده را همچون سـایر حقوق بنیادین (حیات، حیثیت، آزادی، مالکیت و آبرو) شناسایی کرده و جبران همه‌جانبه و مؤثر آسیب به این حق را تضمین کند.

این جبران بایستی شامل همه ابعاد مادی، معنوی، روحی و حوزه‌های غیرقابل سنجش باشد؛ برای نمونه، تعیین ضابطه شفاف برای جبران آسیب‌های ناشی از افشای داده‌های محرمانه خانوادگی، تجاری و سلامت روانی، درج امکان دادخواهی جمعی، پیش‌بینی بیمه‌های ویژه و صندوق‌های عمومی جبران خسارت، و اعطای صلاحیت‌های خاص برای حمایت از قربانیان داده‌ای از پایه‌های این تحول نظری است. همچنین توسعه تجهیزات و سامانه‌های گزارش‌دهی خودکار، بسترهای دیجیتال برای تسهیل ثبت شکایت و بهره‌مندی از مشاوره فوری حقوقی داده‌ای، باید به عنوان مکمل مقررات قانونی پیش‌بینی گردد. ابزارهای نوین جبران نظیر الزام به اصلاح و حذف داده، عذرخواهی عمومی، بازگرداندن وضعیت پیشین فناورانه و سایر ضمانت‌اجراهای غیرنقدی نیز باید به طور مستمر توسعه یابد.

جدول ۴. راهکارهای پیشنهادی برای اصلاح نظام حمایت از داده‌های شخصی در ایران

محور راهکار	مصداق عملی	توضیح مختصر
تدوین قانون جامع داده‌های شخصی	تهیه لایحه مستقل، تبیین حق بر داده	تعریف روشن، توجه به تمام مراحل پردازش داده‌ها
الگوبرداری هوشمند از GDPR	معکوس‌سازی بار اثبات، شمول خسارت معنوی	اقتباس سازوکارهای مؤثر، بومی‌سازی مقررات
تشکیل نهاد مستقل ناظر داده‌ای	نهاد نظارتی با قدرت اجرایی و رسیدگی تخصصی	افزایش شفافیت و ضمانت اجرای احکام
آموزش تخصصی قضات و کارشناسان	دوره‌های آموزشی، شعب تخصصی	توانمندسازی برای تحلیل پرونده‌های داده‌محور
پیش‌بینی جبران دسته‌جمعی خسارت	اجازه طرح دعاوی جمعی و گروهی	ارتقای سطح حمایت اجتماعی و کاهش هزینه‌ها
تقویت همکاری‌های بین‌المللی	عضویت در معاهدات، انتقال تجارب	ارتقا و همسویی با استانداردهای جهانی

۵-۸. تقویت همکاری‌ها، هماهنگی‌های بین‌المللی و انتقال تجربه

ارتباط میان کشورها، نهادهای ملی، منطقه‌ای و جهانی در عرصه حکمرانی داده ـ به ویژه با توجه به ماهیت فراسرزمینی، توزیع‌شده و دیجیتال داده‌های امروز ـ حیاتی‌تر از هر زمان دیگری است. آینده راهبردی ایران در حوزه مسئولیت مدنی داده، مستلزم پیوستن فعالانه به کنوانسیون‌ها و معاهدات بین‌المللی (نظیر کنوانسیون شماره ۱۰۸ شورای اروپا)، ایجاد نهادهای ملی هماهنگ با مجامع معتبر جهانی و ایجاد کانال‌های تبادل فوری اطلاعات میان مراجع ذی‌صلاح است.

الگوبرداری و همکاری با نمونه‌های موفق جهانی، بهره‌مندی از تجارب کشورهای پیشرفته (اعم از اروپا، آمریکا و آسیای شرقی)، تبادل حقوقی و فنی میان نهادهای دولتی و خصوصی، مشارکت در فرایندهای استانداردگذاری، آموزش و تربیت نیروی انسانی

متخصص، همه و همه باید بخشی جداناپذیر از سیاست‌گذاری داده‌ای آینده کشور قرار گیرد. به علاوه، سرمایه‌گذاری در پژوهش‌های بین‌رشته‌ای، حمایت از ایده‌های نوآورلنه داده‌ای، همگرایی هویتی دیجیتال و همچنین تأسیس رایزنان داده‌ای در سفارتخانه‌ها و مجامع جهانی، می‌تواند سطح اثربخشی، نفوذ و اعتبار بین‌المللی ایران را در عرصه حمایت از داده‌های شخصی ارتقاء بخشد.

این مسیر آینده‌نگر و راهکارهای پیشنهادی، نه تنها موجب انطباق تدریجی حقوق ایران با استانداردهای جهانی و پاسخگویی به اقتضائات فنی و هویتی فضای نوین داده خواهد شد، بلکه در ارتقاء کرامت انسانی، افزایش اعتماد عمومی و اثربخشی حقوق خصوصی در عصر دیجیتال نقشی بی‌بدیل ایفا می‌نماید.

۹. نتیجه‌گیری جامع

دگرگونی‌های بنیادین عصر دیجیتال و انقلاب اطلاعاتی، ساختارهای سنتی حقوق خصوصی را با چالش‌هایی کم‌سابقه در زمینه حمایت از داده‌های شخصی و مدیریت مسئولیت مدنی ناشی از آسیب به داده‌ها مواجه ساخته است. آنچه تا دیروز صرفاً مقوله‌ای فناوری‌محور تلقی می‌شد، اکنون در متن هستی حقوق فردی، اقتصادی و حتی هویت اجتماعی جای گرفته و ضرورت بازتعریف رهیافت‌های نظری و هنجاری کلاسیک حقوق مسئولیت مدنی را گوشزد می‌کند. در این میان، داده‌های شخصی نه‌تنها المانی اطلاعاتی بلکه دارایی معنوی، حق بنیادین بشری و ابزار قدرت‌آفرین اقتصادی محسوب می‌شوند؛ ضرورتی که مسئولیت مدنی ناشی از هرگونه آسیب یا تعرض به این داده‌ها را به موضوعی کلان در سطح نظام حکمرانی حقوقی بدل کرده است.

مطالعه تطبیقی رهیافت‌های ایران و مقررات GDPR اروپا، خلأهای جدی نظام حقوقی ایران را در زمینه موضوع‌شناسی، فقدان معیارهای دقیق تقصیر یا مسئولیت محض داده‌ای، ضعف قوانین حمایتی، نارسایی تضمین جبران خسارات معنوی و تأخیر در انطباق با تحولات فنی نمایان می‌سازد. نظام فعلی ایران عمدتاً به مقررات جزئی، پراکنده، مجازات‌محور و بدون تبیین قواعد روشن ارجاع دارد که نه تنها پاسخگوی اقتضائات عصر فرااطلاعاتی نیست، بلکه عملاً راه را برای نقض حقوق داده‌داران، تضییع حق دسترسی، ضربه به حیثیت شخصی و کاهش اعتماد عمومی هموار می‌سازد.

در نقطه مقابل، مقررات GDPR با تأسیس قواعد شفاف، جامع و مبتنی بر محوریت کرامت انسانی، بار اثبات را از زیان‌دیده به متولی داده منتقل نموده، استانداردهای سختگیرانه‌ای برای امنیت و شفافیت داده‌ها برقرار ساخته و ضمانت‌اجراهای متنوع و مؤثری وضع کرده است که کارآمدی این مدل را تاحدود زیادی تضمین می‌کند. نگاه اروپایی بر پذیرش حقی ذاتی برای داده‌های شخصی و ایجاد حق مطالبه، اعتراض و حتی حذف داده‌ها توسط افراد متکی است و با مرجعیت نهاد نظارتی مستقل، ظرفیت اعمال فشار بر متولیان داده را فراهم نموده است.

در مقام مقایسه، جایگاه ایران از سه منظر نیازمند تحول بنیادین است: نخست، ضرورت تصویب قانون جامع، مستقل و تخصصی برای حمایت از داده‌های شخصی که ضمن شناسایی داده به مثابه حق بنیادین، تمامی مراحل چرخه عمر داده (جمع‌آوری، پردازش، نگهداری، انتقال و نابودی) را تحت چهارچوب پاسخگو و قابل اجرا هدایت کند؛ دوم، اصلاح رویه‌های دادرسی و

معکوس‌سازی بار اثبات تقصیر، ایجاد شعب و رویه‌های تخصصی و توانمندسازی بدنه قضایی ـــ فنی کشور در شناسایی مصادیق و جبران علمی خسارت‌های داده‌ای؛ و سوم، جلب همکاری‌های بین‌المللی، پیوستن به معاهدات مرتبط، همسویی با استانداردهای جهانی و ارتقاء ساختاری زیرساخت‌های فناوری حقوقی و آموزش عمومی.

افزون بر موارد فوق، جبران واقعی و مؤثر خسارت‌های مادی و معنوی، به رسمیت شناختن دعاوی گروهی و جمعی، پیش‌بینی امکان اقامه دعوی برای انجمن‌ها و حمایت از زیان‌دیدگان گروه‌های آسیب‌پذیر باید به‌صورت صریح و عملیاتی در ساختار جدید لحاظ گردد. توجه به جنبه‌های کیفی و معنوی آسیب، حوزه‌هایی نظیر خدشه به حریم خانوادگی، ضربه به آبرو و ایجاد اضطراب و بی‌اعتمادی اجتماعی را نیز باید جزو خسارت‌هایی دانست که نظام سنتی فعلی فاقد سازوکار جبران متناسب برای آنان است.

به این‌ترتیب می‌توان نتیجه گرفت که نظام حقوقی ایران ناگزیر از عبور از مدل‌های محافظه‌کارانه سنتی، تدوین قانونی با هویت بومی و الگوبرداری هوشمندانه از مقررات پیشرفته بین‌المللی است؛ مسیری که تنها در سایه رویکرد جامع‌نگر، بازنگری شجاعانه سیاست‌های حمایتی، ارتقاء ظرفیت علمی و فنی بدنه حقوقی و بهره‌گیری از تجربیات جهانی محقق خواهد شد. تحقق این هدف، سیمای نظام حقوقی و اجتماعی ایران را در مواجهه با موج آینده‌نگر فناوری‌های نوین دگرگون و صیانت واقعی، همه‌جانبه و پایدار از کرامت، امنیت و هویت داده‌ای شهروندان را تضمین خواهد کرد. بدین معنا، نظام حقوق خصوصی کشور باید بر مبنای مقتضیات انقلاب اطلاعاتی، تغییر پارادایم حمایت از داده‌های شخصی و پذیرش کارکرد آن در رشد توسعه اقتصادی، اجتماعی و انسانی را به‌عنوان بخش جدایی‌ناپذیر عدالت مدرن به رسمیت شناسد.

۱۱. فهرست منابع

- احمدوند, جهانشاهی, آرتین. (۱۴۰۲). بررسی تطبیقی مفهوم داده‌های شخصی در نظام حقوقی اتحادیه اروپا و ایران. پژوهش های حقوق تطبیقی, ۲۷(۱), ۱۰۵-۱۳۲.
- اسماعیلی, نریمان پور. (۱۴۰۳). مبانی حقوقی تبادل داده‌های شخصی (مطالعه تطبیقی در مقررات عمومی حفاظت از داده اتحادیه اروپا و حقوق ایران). حقوق اسلامی, ۲۱(۸۲), ۱۲۳-۱۶۵.
- باقری, نظریان, رافیک, هادی نژاد, دامن کشیده. (۱۴۰۱). تاثیر شاخص های کلان بانکی، مالی، اقتصادی و بحران های اقتصادی بر ادوار تجاری ایران و کشورهای منتخب در حال توسعه اسلامی و توسعه یافته. اقتصاد مالی, ۱۶(۵۹), ۳۰۳-۳۲۴.
- پیشنماز, سید امین, رکنی, امیر عباس. (۱۴۰۲). تعطیلی پلتفرم‌های مجازی؛ ضرورت تحلیل نظام حاکم بر داده‌های شخصی از منظر حقوق اموال. پژوهشهای حقوقی, ۲۲(۵۳), ۴۶۹-۵۰۶.
- حاج نجفی, حسنا. (۱۴۰۳). اثر بروکسل در حقوق حفاظت از داده های شخصی: معیارهای اروپایی و نظم بندی جهانی. دوفصلنامه تحقیق و توسعه در حقوق عمومی.
- حسین پور, هژبر کیانی, زندی, دهقانی, سعیدی. (۱۳۹۸). برآورد ضرایب فزاینده مالی ایران در مقایسه تطبیقی با کشورهای منتخب منا. اقتصاد مالی, ۱۳(۴۸), ۱۱۱-۱۴۶.
- رهبری, مسعودی تفرشی, آرین. (۱۴۰۳). جایگاه و کاربرد حق انتقال داده‌های شخصی در حقوق رقابت پلتفرم‌های دیجیتال. مطالعات حقوقی.
- شریفی‌کیا, شعبانی‌جهرمی. (۱۴۰۱). شرط شخصی تلقی شدن داده‌ها در فضای سایبر بررسی تطبیقی مقررات عمومی اروپایی حفاظت از داده و حقوق ایران. حقوق خصوصی (دانشگاه تهران), ۴۰(۱۹), ۲۲۱-۲۴۵.

- صالحی حمیدرضا, رضوی سیدمحمد, رفیعی رسول, کاووسی یونس. (۱۳۹۹). جبران خسارت معنوی ناشی از معالجات پزشکی در حقوق ایران و آمریکا.
- صحرائیان, زارع. (۱۳۹۸). قرادادهای منعقده در محیط اینترنت در حقوق ایران و فرانسه. تحقیقات حقوقی بین المللی, ۱۲(۴۶), ۱۱۳-۱۳۱.
- لطیف زاده, مهدیه, قبولی درافشان, سیدمحمدمهدی, محسنی, عابدی. (۱۴۰۲). بررسی تطبیقی ضمانت اجرای نقض حق بر داده در حقوق اتحادیه اروپا و نظام حقوقی ایران. مجلس و راهبرد, ۳۰(۱۱۶), ۳۴۱-۳۷۴.
- لطیف زاده, مهدیه, قبولی درافشان, سیدمحمدمهدی, محسنی, عابدی. (۱۴۰۲). تعهدات پردازش‌کنندهٔ داده شخصی در اتحادیه اروپا و امکان‌سنجی پذیرش آن در حقوق ایران. آموزه های فقه مدنی, ۱۵(۲۷), ۲۴۵-۲۸۶.
- لطیف زاده, مهدیه, قبولی درافشان, محسنی, عابدی. (۱۴۰۱). تبیین اسباب مشروعیت پردازش داده‌ی شخصی از منظر حقوق اتحادیه اروپا و ایران. مطالعات حقوقی, ۱۴(۳), ۳۲۵-۳۶۴.
- لطیف زاده, مهدیه, قبولی درافشان, محسنی, عابدی. (۱۴۰۲). چگونگی پردازش داده‌ی شخصی خاص در حقوق اتحادیه اروپا و بررسی آن در نظام حقوقی ایران. پژوهشنامه پردازش و مدیریت اطلاعات, ۳۹(۱), ۱۵۷-۱۹۹.
- لطیف زاده, مهدیه, قبولی درافشان, محسنی, عابدی. (۱۴۰۲). حمایت از دادهٔ شخصی در حقوق اتحادیهٔ اروپا و امکان‌سنجی آن در نظام حقوقی ایران. فصلنامه مطالعات حقوق عمومی دانشگاه تهران, ۵۳(۲), ۹۸۱-۱۰۰۵.
- لطیف زاده, مهدیه, قبولی درافشان. (۱۴۰۱). چگونگی انتقال بین‌المللی داده‌های شخصی (مطالعه تطبیقی در حقوق اتحادیه اروپا و نظام حقوقی ایران). پژوهشنامه حقوق تطبیقی, ۶(۱), ۲۰۷-۲۳۰.
- لطیف‌زاده, مهدیه. (۱۴۰۱). رفع تقابل بین حق آزادی بیان و اطلاعات با حق بر داده‌های شخصی در رسانه‌ها از منظر حقوق اتحادیه اروپا و نظام حقوقی ایران. پژوهش‌های ارتباطی, ۲۹(۱۱۱), ۱۵۳-۱۷۳.
- میرشکاری, پیشنماز, سید امین, رکنی, امیر عباس. (۱۴۰۳). تراست داده، سازوکاری برای مدیریت منافع ذی‌نفعان داده؛ رهنمودهایی برای نظام داده در حقوق ایران. مطالعات حقوق تطبیقی معاصر, ۱۵(۳۴), ۲۷۹-۳۲۰.