مجله کانون وکلای دادگستری استان آذربایجان شرقی
کانون وکلای دادگستری استان آذربایجان شرقی
شماره ۵۱ و ۵۲ پاییز و زمستان ۱۴۰۳

مسئولیت مدنی ناشی از نقض داده‌های شخصی: بررسی تطبیقی حقوق ایران و اتحادیه اروپا

دکتر رحیم وکیل زاده[۱]
علی دیودار[۲]

چکیده

حریم خصوصی داده‌ها یکی از مفاهیم بنیادین در نظام‌های حقوقی معاصر است که با گسترش فناوری‌های اطلاعاتی و ارتباطی، اهمیت روزافزون یافته است. در این پژوهش، مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها بررسی می‌شود و نقش سه رکن اساسی آن، یعنی ضرر، تقصیر و رابطه سببیت، در تحقق مسئولیت مدنی تحلیل می‌گردد. یکی از چالش‌های اساسی در این حوزه، نظریه «نقض حریم خصوصی داده‌ها» است که برخی حقوقدانان غربی مطرح کرده‌اند و بر اساس آن، با توجه به گسترش فناوری‌های پایش و پردازش داده‌ها، دیگر انتظاری معقول برای حفظ حریم خصوصی وجود ندارد. این نظریه ضمن تأثیر بر مبانی مسئولیت مدنی، امکان مطالبه خسارت را نیز محدود می‌سازد. در این پژوهش، این نظریه نقد شده و بر لزوم حمایت حقوقی مؤثر از زیان‌دیدگان تأکید شده است. همچنین، با توجه به تأثیر نقض حریم خصوصی داده‌ها بر حقوق شخصیت، خسارات معنوی ناشی از آن بررسی شده و در نهایت، امکان تلقی حریم خصوصی داده‌ها به‌عنوان یک حق مالی بر اساس نظریه مالکیت فکری مورد تحلیل قرار گرفته است. یافته‌های تحقیق نشان می‌دهد که هرچند فناوری‌های نوین احتمال نقض حریم خصوصی را افزایش داده‌اند، اما این امر نباید به تضعیف حمایت‌های حقوقی از افراد منجر شود، بلکه باید با تقویت سازوکارهای جبران خسارت و توسعه قواعد مسئولیت مدنی، توازن میان منافع عمومی و حقوق فردی حفظ گردد.

کلید واژه: مسئولیت مدنی، حریم خصوصی داده‌ها، ضرر، نظریه نقض حریم خصوصی، حقوق شخصیت

---

[۱] وکیل پایه یک دادگستری، دانشیار گروه فقه و مبانی حقوق اسلامی، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران. (نویسنده مسئول) rahimvakilzadeh@gmail.com

[۲] وکیل پایه یک دادگستری،کارشناسی ارشد حقوق خصوصی، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران. alidivdar10@gmail.com

مقدمه

در عصر حاضر، داده‌های شخصی به‌مثابه سرمایه‌ای ارزشمند برای افراد و جوامع تلقی می‌شوند. پیشرفت فناوری اطلاعات، گسترش خدمات اینترنتی، و حضور روزافزون افراد در فضای مجازی موجب شده است که حجم قابل توجهی از اطلاعات شخصی در معرض پردازش، ذخیره‌سازی و تبادل قرار گیرد. این تحول تکنولوژیک، اگرچه مزایای فراوانی در تسهیل خدمات، افزایش بهره‌وری و گسترش ارتباطات ایجاد کرده، اما همزمان زمینه‌ساز تهدیدهایی نسبت به حریم خصوصی افراد و نقض اطلاعات شخصی آنان نیز شده است. در چنین شرایطی، حفاظت از داده‌های شخصی نه تنها یک ضرورت اخلاقی و اجتماعی محسوب می‌شود، بلکه به‌عنوان یک تعهد حقوقی برای دولت‌ها، نهادهای عمومی، شرکت‌های خصوصی و حتی اشخاص حقیقی نیز مطرح است. در واقع، داده‌های شخصی از جمله حقوق بنیادین انسان‌ها به شمار می‌آیند که نیازمند تضمین‌های مؤثر قانونی هستند (لطیف زاده و همکاران، ۱۴۰۰: ۲۶). یکی از مهم‌ترین بُعدهای حقوقی مرتبط با داده‌های شخصی، بحث مسئولیت مدنی در صورت نقض این داده‌هاست. در صورتی که اطلاعات شخصی افراد بدون رضایت یا برخلاف موازین قانونی افشاء، پردازش یا مورد سوءاستفاده قرار گیرد، خسارات مادی و معنوی متعددی متوجه صاحب داده خواهد شد. در چنین حالتی، نظام حقوقی موظف است با بهره‌گیری از اصول مسئولیت مدنی، امکان جبران خسارات وارده به قربانی را فراهم آورد. اما ماهیت خاص داده‌های شخصی، از حیث ناملموس بودن، قابلیت تکثیر، و ارزش‌گذاری پیچیده، سبب شده است که اعمال قواعد سنتی مسئولیت مدنی بر این حوزه با چالش‌هایی مواجه گردد. همین امر، ضرورت بازاندیشی در قواعد موجود و بهره‌گیری از تجارب دیگر نظام‌های حقوقی را دوچندان می‌کند (قناد و همکاران، ۱۴۰۰: ۲۲). در حقوق ایران، اگرچه اصول کلی مسئولیت مدنی همچون لزوم جبران ضرر غیرقانونی و حرمت اضرار به غیر در فقه و قانون مدنی وجود دارد، اما در زمینه نقض داده‌های شخصی، با خلأهای قانونی و رویه‌ای جدی مواجه هستیم. قانون‌گذار ایرانی هنوز قانون جامعی در زمینه حفاظت از داده‌های شخصی تصویب نکرده و تنها در برخی مواد قانون جرایم رایانه‌ای یا مقررات پراکنده دیگر به‌صورت ضمنی به آن اشاره شده است. همچنین، رویه قضایی ایران نیز به‌دلیل نو بودن موضوع و فقدان رویه‌های منسجم، نتوانسته است تفسیر و تبیین روشن و اثربخشی از مسئولیت مدنی در این حوزه ارائه دهد. در نتیجه، قربانیان نقض داده‌ها اغلب با دشواری‌های فراوانی برای اثبات خسارت و مطالبه جبران مواجه هستند (محقق داماد، ۱۳۹۵: ۱۸).

در مقابل، اتحادیه اروپا با درک اهمیت موضوع، اقدامات اساسی و بنیادینی در راستای حمایت از داده‌های شخصی و تنظیم مسئولیت‌های مدنی ناشی از نقض آن‌ها انجام داده است. تصویب مقررات عمومی حفاظت از داده‌ها (General Data Protection Regulation - GDPR) در سال ۲۰۱۶

که از سال ۲۰۱۸ لازم‌الاجرا شد، نقطه عطفی در تنظیم رابطه میان صاحبان داده، نهادهای پردازشگر، و دولت‌ها بود. این مقررات به‌طور مفصل به حقوق افراد، الزامات پردازش داده‌ها، ضمانت‌های اجرایی و همچنین نحوه جبران خسارت ناشی از نقض داده‌ها پرداخته و نظام مسئولیت مدنی نسبتاً پیشرفته‌ای را در این حوزه ارائه کرده است. از جمله نوآوری‌های GDPR می‌توان به اصل شفافیت، حق فراموشی، و حق انتقال‌پذیری داده‌ها اشاره کرد (Breen, 2020: 26). مسئولیت مدنی ناشی از نقض داده‌های شخصی در نظام‌های حقوقی مختلف، بسته به مبانی فکری آن‌ها، ممکن است بر پایه تقصیر یا مسئولیت مطلق (بی‌تقصیر) استوار باشد. در برخی نظام‌ها مانند حقوق ایران، اساس مسئولیت مدنی همچنان تقصیرمحور است و اثبات آن بر عهده زیان‌دیده قرار دارد. اما در حقوق اتحادیه اروپا، با توجه به مفاد GDPR، در مواردی مسئولیت ناشی از نقض داده‌ها می‌تواند جنبه غیرتقصیری به خود بگیرد، به‌ویژه در جایی که پردازش‌گر داده نتواند رعایت الزامات قانونی را اثبات کند. چنین تفاوت‌هایی در مبانی مسئولیت، تأثیر مستقیم بر امکان دسترسی زیان‌دیدگان به جبران خسارت دارد و همین امر، مقایسه تطبیقی میان این دو نظام حقوقی را مهم و ضروری می‌سازد (Colcelli,2019: 14).

در تحلیل مسئولیت مدنی ناشی از نقض داده‌های شخصی، باید به انواع خسارات قابل مطالبه نیز توجه داشت. علاوه بر خسارات مادی نظیر سرقت هویت، سوءاستفاده مالی، یا افشای اطلاعات محرمانه، خسارات معنوی همچون خدشه به حیثیت، سلب آرامش روانی و تعرض به حریم خصوصی نیز اهمیت دارند. با این حال، اثبات و برآورد خسارات معنوی در نظام‌های حقوقی مختلف با چالش‌های متفاوتی همراه است. در ایران، مبنای قانونی روشنی برای پذیرش و ارزیابی خسارات معنوی ناشی از نقض داده‌ها وجود ندارد، در حالی‌که در GDPR تصریح شده است که خسارات معنوی نیز مشمول جبران خواهند بود. این تفاوت نگرش‌ها، پرسش‌هایی اساسی در خصوص عدالت جبرانی و حمایت از کرامت انسانی در پی دارد (منصوریان، ۱۳۹۵: ۱۷). در خصوص شخص یا اشخاص مسئول، نیز تفاوت‌هایی میان نظام‌های حقوقی مشاهده می‌شود. در GDPR مسئولیت ممکن است متوجه «کنترل‌کننده داده» یا «پردازشگر داده» باشد، بسته به نقش و میزان تقصیر آن‌ها در فرآیند نقض. این تقسیم‌بندی حقوقی موجب شفافیت بیشتر و تسهیل در پیگیری‌های قضایی و حقوقی شده است. در حقوق ایران اما به‌دلیل نبود چارچوب قانونی جامع، شناسایی شخص مسئول دشوارتر است، به‌ویژه در مواردی که چندین نهاد درگیر پردازش داده‌ها هستند. همین فقدان تبیین دقیق مفاهیم پایه‌ای مانند کنترل‌گر داده و مسئول پردازش، روند احقاق حق را با مانع مواجه می‌کند (بیات کمیتکی، ۱۳۹۶: ۲۹). از منظر نهادی نیز حمایت از داده‌های شخصی در ایران با ضعف ساختاری همراه است. نهاد مستقلی برای نظارت و رسیدگی به نقض داده‌های شخصی وجود ندارد و افراد معمولاً ناچارند از مسیرهای عمومی مانند دادگاه‌های کیفری یا دادگاه‌های حقوقی برای مطالبه خسارت استفاده کنند. در مقابل، اتحادیه اروپا «مقام ناظر حفاظت از داده‌ها (DPA)

را در هر کشور عضو پیش‌بینی کرده است که وظیفه نظارت، رسیدگی و اعمال ضمانت اجراها را بر عهده دارد. این تفاوت نهادی، تأثیر چشمگیری در میزان اثربخشی مقررات و حمایت عملی از افراد دارد. پیشرفت فناوری‌های نوظهور مانند هوش مصنوعی، اینترنت اشیاء، و کلان‌داده‌ها (Big Data) نیز ابعاد جدیدی به چالش‌های مسئولیت مدنی افزوده است. داده‌های شخصی نه‌تنها از طریق فعالیت مستقیم افراد، بلکه از طریق تحلیل الگوریتمی، ترکیب داده‌ها و داده‌کاوی نیز قابل استخراج و نقض هستند. در چنین فضایی، مسئولیت‌پذیری نهادهای پردازشگر، شفافیت الگوریتم‌ها، و امکان نظارت بر تصمیمات ماشینی به مسائل محوری تبدیل شده‌اند. این وضعیت، نیازمند توسعه مفهوم «مسئولیت مدنی فناورانه» است که باید در حقوق ایران نیز مورد توجه جدی قرار گیرد (محقق داماد، ۱۳۹۳: ۲۷).

با توجه به اهمیت حریم خصوصی و ارتباط آن با کرامت انسانی، بسیاری از حقوقدانان معتقدند که نقض داده‌های شخصی نه‌تنها یک مسئله قراردادی یا تقصیری صرف، بلکه نوعی تعرض به حقوق بشر تلقی می‌شود. در اسناد بین‌المللی مانند میثاق بین‌المللی حقوق مدنی و سیاسی، به صراحت بر منع مداخله خودسرانه در حریم خصوصی تأکید شده است. همچنین در نظام اروپایی، داده‌های شخصی بخشی از حق بر حریم خصوصی شناخته شده‌اند و نقض آن‌ها ممکن است موجبات مسئولیت دولت‌ها نزد نهادهایی مانند دیوان حقوق بشر اروپا را نیز فراهم آورد. این پیوند میان داده‌ها و حقوق بشر، مسئولیت مدنی را از سطح خصوصی فراتر می‌برد. با این حال، پرسش اصلی در این زمینه آن است که نظام حقوقی ایران تا چه اندازه می‌تواند از تجربه اتحادیه اروپا بهره گیرد؟ آیا انتقال مفاهیم، ساختارها و مقرراتی مانند GDPR به‌صورت مستقیم امکان‌پذیر است یا نیازمند بومی‌سازی و انطباق با مبانی فقهی و قانونی کشورمان است؟ پاسخ به این پرسش‌ها مستلزم بررسی تطبیقی دقیق میان دو نظام حقوقی و شناسایی نقاط قوت و ضعف هر یک است. همچنین، باید مشخص شود که چه خلأهایی در قوانین ایران وجود دارد که مانع حمایت مؤثر از زیان‌دیدگان نقض داده‌ها شده و چگونه می‌توان این خلأها را جبران کرد. پژوهش حاضر با هدف بررسی مسئولیت مدنی ناشی از نقض داده‌های شخصی با رویکرد تطبیقی میان حقوق ایران و اتحادیه اروپا نگاشته شده است. تلاش خواهد شد تا با تحلیل مبانی نظری، بررسی چارچوب‌های قانونی، و تطبیق رویه‌های حقوقی موجود، تصویری جامع از وضعیت فعلی و مطلوب ارائه گردد. همچنین با تکیه بر اصول حقوق بشر، حقوق خصوصی و قواعد عام مسئولیت مدنی، امکان‌سنجی اصلاحات قانونی و نهادی در ایران مورد توجه قرار می‌گیرد. بدیهی است که چنین مطالعه‌ای می‌تواند بستر مناسبی برای تدوین قانون جامع حفاظت از داده‌ها در کشور فراهم سازد. روش تحقیق در این پژوهش، توصیفی–تحلیلی با رویکرد تطبیقی است. اطلاعات مورد استفاده عمدتاً از منابع کتابخانه‌ای، قوانین، اسناد بین‌المللی، و رویه قضایی داخلی و خارجی استخراج شده است. همچنین، تلاش شده است تا با بهره‌گیری از تحلیل حقوق تطبیقی، تفاوت‌های مفهومی، ساختاری و اجرایی میان دو نظام حقوقی ایران

و اتحادیه اروپا تبیین گردد. مطالعه موردی بر روی مقررات GDPR و ارزیابی مقررات ایران در قالب قوانین جزایی، مدنی و مقررات خاص نیز در دستور کار قرار دارد.

نقض داده‌های شخصی نه‌تنها به حقوق فردی آسیب می‌زند، بلکه اعتماد عمومی به نظام‌های فناوری، دولت و نهادهای اقتصادی را نیز تضعیف می‌کند. وجود یک نظام مؤثر مسئولیت مدنی که امکان جبران سریع، عادلانه و مؤثر خسارت را فراهم آورد، می‌تواند نقش مهمی در بازسازی این اعتماد ایفا کند. بنابراین، توسعه و تقویت ابزارهای حقوقی برای مقابله با نقض داده‌ها نه‌تنها در سطح فردی، بلکه در سطح ملی نیز دارای اهمیت راهبردی است.

۱- مفاهیم و مبانی

۱-۱- مفهوم داده‌های شخصی و پردازش آن

تعریف داده و اطلاعات کار مشکلی است تنها از دیدگاه استفاده کنندگان می‌توان آنها را از هم تشخیص داد. بدین منظور بعضی از تعاریف داده و اطلاعات از دیدگاه صاحبنظران مختلف ارائه شده است. واژه داده، مناسب‌ترین واژه‌ای است که به واقعیات شکل نیافته و بدون ساختار فراوان تولید شده توسط کامپیوتر، می‌توان اطلاق نمود که بر اعداد نمودارها و دیگر نوشته‌ها دلالت می‌کند و به تنهایی معنی ندارد. به بیانی دیگر داده‌ها حقایق و واقعیت‌های خام هستند و این اجزاء در پایگاه‌های داده ذخیره و مدیریت می‌شوند مطابق تعریف فرهنگ کامپیوتری مایکروسافت نیز داده عبارت از فقره یا فقراتی از اطلاعات باشد همچنین بنا به دانشنامه‌ی جهانی آکسفورد داده به اطلاعاتی اطلاق می‌شود که غالباً در قالب خاص و برای هدف مشخص تهیه شده است «ردمن[1]» معتقد است که داده‌ها عناصر اصلی اطلاعات هستند داده‌ها در صورتی به اطلاعات تبدیل می‌شوند که افراد بخواهند برای درک بیشتر از آنها استفاده کنند (انصاری، ۱۴۰۱: ۷۲). اطلاعات داده‌های خلاصه‌ای هستند که گروه بندی ذخیره پالایش و سازماندهی شده‌اند تا بتوانند معنی دار شوند اطلاعات زمانی ارزش پیدا می‌کنند که برای یک بعد، خاص یک فرد خاص یک هدف خاص و در زمان خاص گردآوری و آماده شوند لذا اطلاعاتی که برای یک مدیر، جنبه اطلاعاتی دارد برای مدیر دیگر ممکن است اصلاً ارزشی نداشته باشد. داده‌های شخصی یکی از انواع داده‌های مرتبط با موضوع ما می‌باشد که در ادامه به شرح آن خواهیم پرداخت (انصاری، ۱۳۸۸: ۲۳).

---

1. Redman

۱-۲- تمایز داده‌های عادی از داده‌های حساس

در نظام‌های حقوقی معاصر، داده‌های شخصی به دو دسته کلی تقسیم می‌شوند: داده‌های عادی و داده‌های حساس. داده‌های عادی شامل اطلاعاتی هستند که به‌طور معمول در تعاملات روزمره افراد مورد استفاده قرار می‌گیرند، مانند نام، نشانی، شماره تلفن و اطلاعات تماس. در مقابل، داده‌های حساس شامل اطلاعاتی هستند که افشای آن‌ها می‌تواند به تبعیض یا آسیب جدی به فرد منجر شود، مانند اطلاعات پزشکی، نژادی، مذهبی، گرایش‌های جنسی و دیدگاه‌های سیاسی. این تمایز در مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) به‌وضوح بیان شده است و برای داده‌های حساس، سطح بالاتری از حفاظت در نظر گرفته شده است (قطبی راوندی، ۱۳۹۹: ۲۲). در حقوق ایران، اگرچه قانون جامعی در زمینه حفاظت از داده‌های شخصی وجود ندارد، اما در برخی قوانین و مقررات پراکنده، به‌طور ضمنی به تمایز بین داده‌های عادی و حساس اشاره شده است. برای مثال، در قانون جرایم رایانه‌ای، افشای اطلاعات خصوصی افراد جرم‌انگاری شده است، که می‌تواند شامل داده‌های حساس باشد. با این حال، نبود تعریف دقیق و جامع از داده‌های حساس در قوانین ایران، چالش‌هایی را در زمینه حمایت مؤثر از این نوع داده‌ها ایجاد کرده است (انصاری و همکاران، ۱۳۸۸: ۲۷). در مقررات GDPR، پردازش داده‌های حساس تنها در شرایط خاص و با رعایت الزامات سخت‌گیرانه مجاز است. برای مثال، رضایت صریح و آگاهانه فرد موضوع داده، یکی از پیش‌شرط‌های اصلی برای پردازش داده‌های حساس است. همچنین، در مواردی که پردازش برای منافع عمومی یا درمان‌های پزشکی ضروری باشد، ممکن است استثنائاتی اعمال شود. این رویکرد نشان‌دهنده اهمیت بالای داده‌های حساس و لزوم حمایت ویژه از آن‌هاست (زینس، ۱۳۹۰: ۲۳).

در مقابل، در حقوق ایران، نبود چارچوب قانونی مشخص برای پردازش داده‌های حساس، موجب شده است که در عمل، تفاوتی بین داده‌های عادی و حساس قائل نشوند. این وضعیت می‌تواند به نقض حریم خصوصی افراد و آسیب‌های جدی به آن‌ها منجر شود. بنابراین، ضرورت تدوین قانون جامع حفاظت از داده‌های شخصی با در نظر گرفتن تمایز بین داده‌های عادی و حساس در ایران احساس می‌شود (همان، ۳۸). تمایز بین داده‌های عادی و حساس، تأثیر مستقیمی بر مسئولیت مدنی ناشی از نقض داده‌ها دارد. در مواردی که داده‌های حساس نقض می‌شوند، خسارات وارده به فرد می‌تواند شدیدتر باشد و در نتیجه، مسئولیت مدنی ناقض نیز افزایش یابد. در حقوق اتحادیه اروپا، این موضوع به‌خوبی در نظر گرفته شده است و در تعیین میزان جبران خسارت، نوع داده‌های نقض‌شده مورد توجه قرار می‌گیرد (انصاری، ۱۴۰۱: ۱۰۲). در نهایت، تمایز بین داده‌های عادی و حساس، نه‌تنها در سطح حقوقی، بلکه در سطح اخلاقی و اجتماعی نیز اهمیت دارد. حفاظت از داده‌های حساس، به‌ویژه در حوزه‌هایی مانند سلامت، مذهب و

گرایش‌های شخصی، برای حفظ کرامت انسانی و جلوگیری از تبعیض ضروری است. بنابراین، نظام‌های حقوقی باید با درک این اهمیت، سازوکارهای مناسبی برای حمایت از داده‌های حساس تدوین و اجرا کنند.

۱-۳- مفهوم نقض داده‌های شخصی

نقض داده‌های شخصی به معنای هرگونه دسترسی، افشاء، تغییر، یا از بین بردن غیرمجاز داده‌های شخصی است که می‌تواند به آسیب‌های مادی یا معنوی به فرد منجر شود. در مقرراتGDPR ، نقض داده‌ها به‌طور گسترده تعریف شده و شامل هرگونه نقض امنیتی است که منجر به تخریب، از بین رفتن، تغییر، افشاء یا دسترسی غیرمجاز به داده‌های شخصی می‌شود (انصاری، ۱۴۰۱: ۱۲۷). در حقوق ایران، مفهوم نقض داده‌های شخصی به‌طور صریح تعریف نشده است. با این حال، در قانون جرایم رایانه‌ای، برخی رفتارها مانند دسترسی غیرمجاز به داده‌های رایانه‌ای و افشای اسرار شخصی جرم‌انگاری شده‌اند. این موارد می‌توانند به‌عنوان مصادیقی از نقض داده‌های شخصی تلقی شوند، اما نبود تعریف جامع و دقیق، موجب ابهام در تفسیر و اجرای قانون شده است (قطبی راوندی و همکاران، ۱۳۹۹: ۲۹). نقض داده‌های شخصی می‌تواند به اشکال مختلفی رخ دهد، از جمله حملات سایبری، افشای اطلاعات توسط کارکنان، یا اشتباهات فنی در سیستم‌های اطلاعاتی. در هر یک از این موارد، اگر داده‌های شخصی افراد بدون مجوز مناسب در دسترس افراد غیرمجاز قرار گیرد، نقض داده‌ها محسوب می‌شود. این موضوع اهمیت بالای امنیت اطلاعات و آموزش کارکنان را نشان می‌دهد. در مقررات GDPR، در صورت وقوع نقض داده‌های شخصی، مسئول پردازش داده‌ها موظف است ظرف ۷۲ ساعت، نقض را به مقام نظارتی مربوطه گزارش دهد. همچنین، در مواردی که نقض می‌تواند به حقوق و آزادی‌های افراد آسیب برساند، اطلاع‌رسانی به افراد موضوع داده نیز الزامی است. این الزامات به‌منظور افزایش شفافیت و پاسخگویی در موارد نقض داده‌ها تدوین شده‌اند (Goddard,2017: 48). در حقوق ایران، چنین الزامات مشخصی برای گزارش‌دهی نقض داده‌های شخصی وجود ندارد. این خلأ قانونی می‌تواند موجب تأخیر در واکنش به نقض داده‌ها و افزایش آسیب به افراد شود. بنابراین، تدوین مقرراتی مشابه با GDPR در زمینه گزارش‌دهی نقض داده‌ها، می‌تواند گامی مؤثر در جهت حفاظت از حقوق افراد باشد(محمدی کردخیلی، ۱۴۰۱: ۱۶). مفهوم نقض داده‌های شخصی، به‌عنوان یکی از محورهای اصلی در حوزه حفاظت از داده‌ها، نیازمند توجه ویژه در نظام‌های حقوقی است. تعریف دقیق، شناسایی مصادیق، و تدوین سازوکارهای مناسب برای پیشگیری و واکنش به نقض داده‌ها، از جمله اقدامات ضروری در این زمینه هستند.

۱-٤- عناصر مسئولیت مدنی

در تحلیل مسئولیت مدنی، سه عنصر اساسی شامل تقصیر، زیان و رابطه سببیت، ستون‌های اصلی شکل‌گیری این نهاد حقوقی محسوب می‌شوند. تقصیر، رفتاری خلاف موازین متعارف یا قانونی است که از شخصی سر زده و از نظر حقوقی قابل سرزنش تلقی می‌شود؛ در حوزه نقض داده‌های شخصی، این عنصر ممکن است در قالب کوتاهی در اجرای تدابیر امنیتی، افشای غیرمجاز اطلاعات، یا عدم رعایت مقررات حمایتی مانند GDPR نمود یابد. دومین عنصر، «زیان» است که می‌تواند مادی (نظیر سرقت هویت یا سوءاستفاده مالی) یا معنوی (مانند خدشه به حیثیت یا آرامش روانی فرد) باشد؛ به‌ویژه در حوزه داده‌های شخصی، زیان‌های معنوی معمولاً گسترده‌تر و پیچیده‌تر هستند. در حقوق ایران نیز، مطابق ماده ۱ قانون مسئولیت مدنی، صرف وجود ضرر شرط ضروری تحقق مسئولیت است. عنصر سوم، «رابطه سببیت» است که وجود پیوند علی بین رفتار زیان‌بار و ضرر وارده را ایجاب می‌کند؛ در نظام‌های حقوقی پیشرفته مانند اتحادیه اروپا، این رابطه اغلب بر اساس اصول علمی و آماری، یا سازوکارهایی مانند وارون‌سازی بار اثبات (reverse burden of proof) ارزیابی می‌شود (کاتوزیان، ۱۳۹۵: ۷۸). در فضای دیجیتال، پیچیدگی فنی فرایندها باعث شده اثبات رابطه سببیت به چالشی جدی بدل شود؛ به‌گونه‌ای که برخی حقوقدانان پیشنهاد داده‌اند در مواردی که امکان اثبات فنی وجود ندارد اما قرائن قوی موجود است، فرض رابطه سببیت برقرار شود. در مجموع، این سه عنصر با وجود اهمیت اساسی‌شان، در مواجهه با تحولات دنیای فناوری نیازمند بازنگری و تفسیر توسعه‌گرا هستند تا از حقوق افراد در برابر نقض داده‌های شخصی به‌طور مؤثر حمایت شود.

۱-٤-۱- تقصیر

تقصیر به معنای رفتار نادرست یا بی‌احتیاطی است که منجر به ورود ضرر به دیگری می‌شود. در حقوق ایران، تقصیر به‌عنوان یکی از ارکان اصلی مسئولیت مدنی شناخته می‌شود و اثبات آن برای مطالبه خسارت ضروری است. ماده ۱ قانون مسئولیت مدنی ایران تصریح می‌کند که هر کس بدون مجوز قانونی، عمداً یا در نتیجه بی‌احتیاطی، به جان یا مال یا حیثیت یا آزادی یا شهرت تجارتی یا به هر حق دیگر متعلق به افراد لطمه‌ای وارد کند، مسئول جبران خسارت خواهد بود. در مقررات GDPR، مسئولیت مدنی ممکن است بدون نیاز به اثبات تقصیر نیز اعمال شود. برای مثال، اگر پردازش‌گر داده نتواند اثبات کند که اقدامات لازم برای حفاظت از داده‌ها را انجام داده است، ممکن است مسئول شناخته شود، حتی اگر تقصیر خاصی از سوی او اثبات نشده باشد. این رویکرد، مسئولیت را از تقصیرمحوری به سمت مسئولیت مبتنی بر خطر یا نتیجه سوق می‌دهد (لطیف زاده و همکاران، ۱۴۰۰: ۱۹). در بسیاری از موارد نقض داده‌های شخصی، اثبات تقصیر پردازش‌گر داده به دلایل فنی و حقوقی با دشواری همراه است؛

چرا که زیان‌دیده معمولاً به سیستم‌های فنی، پروتکل‌های امنیتی و فرآیندهای درون‌سازمانی دسترسی ندارد. این چالش در حقوق ایران جدی‌تر است، زیرا قانون‌گذار سازوکار معکوس بار اثبات را پیش‌بینی نکرده است؛ در حالی که در اتحادیه اروپا، بر اساس ماده ۸۲ مقررات عمومی حفاظت از داده‌ها (GDPR)، مسئول داده باید نشان دهد که هیچ‌گونه تخلفی از مقررات صورت نگرفته یا زیان وارده خارج از کنترل وی بوده است. چنین رویه‌ای نشان می‌دهد که در موارد نقض داده‌های شخصی، مسئولیت مدنی به سمت یک الگوی مبتنی بر «فرض تقصیر» یا حتی «مسئولیت عینی» در حال حرکت است. در نتیجه، حمایت مؤثر از اشخاص نیازمند اصلاح قوانین ملی در راستای بهره‌گیری از سازوکارهای حمایتی و تخصصی نظیر فرض تقصیر در این حوزه است (انصاری، ۱۴۰۰: ۳۴).

۱-٤-۲- زیان

عنصر دوم مسئولیت مدنی، زیان است که بدون تحقق آن، مطالبه خسارت از نظر حقوقی ممکن نیست. زیان در حوزه داده‌های شخصی ممکن است ماهیت مادی، معنوی یا حیثیتی داشته باشد. برای مثال، افشای اطلاعات پزشکی یک فرد می‌تواند موجب تبعیض در اشتغال یا آسیب به اعتبار وی شود، که هر دو نوعی از زیان غیرمستقیم یا غیرمالی محسوب می‌شوند. در حقوق ایران، ماده ۱ قانون مسئولیت مدنی، صراحتاً «حیثیت» و «شهرت» را از مصادیق زیان می‌داند. اما در رویه قضایی، ارزیابی زیان معنوی با تردید و گاه بی‌اعتنایی مواجه بوده است. در حالی که در نظام حقوقی اتحادیه اروپا، ماده ۸۲ GDPR به روشنی بیان می‌دارد که اشخاص موضوع داده‌ها در صورت ورود هر نوع زیان، اعم از مادی یا غیرمادی، حق دریافت غرامت دارند. این نگرش حمایتی، زمینه‌ای برای جبران عادلانه خسارات ناشی از نقض داده‌ها فراهم کرده است، به‌ویژه در مواردی که آثار زیان آشکارا مالی نبوده ولی زیان‌دیده متحمل آسیب‌های روانی یا حیثیتی شده است (انصاری، ۱۴۰۱: ۶۳).

۱-٤-۳- رابطه سببیت

رابطه سببیت، به‌عنوان سومین رکن مسئولیت مدنی، به معنای وجود پیوند مستقیم یا غیرمستقیم میان عمل زیان‌بار و خسارت وارده است. اثبات این رابطه به‌ویژه در حوزه فناوری‌های دیجیتال، بسیار دشوارتر از دعاوی سنتی مسئولیت مدنی است، زیرا داده‌ها ممکن است در بستر شبکه‌های متعدد، با مشارکت اشخاص مختلف و در سیستم‌های پیچیده پردازش شوند. در چنین شرایطی، تعیین اینکه دقیقاً کدام کنش یا کوتاهی منجر به بروز زیان شده، نیازمند دانش تخصصی و گاه استفاده از کارشناسی‌های فنی و امنیت سایبری است. در حقوق ایران، رویه قضایی الزاماً مبتنی بر اثبات رابطه علیت مستقیم است، در حالی که در مقرراتGDPR ، نگاه منعطف‌تری وجود دارد؛ یعنی کافی است که نقض تعهدات امنیتی یا

اصول پردازش داده «احتمالاً» موجب زیان شده باشد، تا مسئولیت متوجه پردازش‌گر گردد، مگر اینکه وی خلاف آن را اثبات کند. به این ترتیب، در حوزه داده‌ها، تفکیک دقیق میان رابطه سببیت حقوقی و فنی امری ضروری است و می‌تواند در مسیر تحقق عدالت نقش تعیین‌کننده‌ای داشته باشد (غمامی، ۱۳۸۹: ۱۳).

۱-۵- مبانی مسئولیت مدنی در حوزه داده‌ها

مبانی مسئولیت مدنی در حوزه داده‌ها، برخلاف مسئولیت‌های سنتی، متأثر از پیچیدگی‌های فناوری اطلاعات، گسترش فضای دیجیتال، و اهمیت روزافزون حریم خصوصی اشخاص است. این مبانی از چهار دیدگاه اصلی قابل بررسی‌اند: مبنای تقصیر، مبنای خطر، مبنای انصاف، و مبنای حمایت از حریم خصوصی. مبنای تقصیر که بر پایه رفتار قابل سرزنش فاعل است، در شرایطی کاربرد دارد که متولی داده‌ها در انجام تکالیف خود از جمله تأمین امنیت، اخذ رضایت آگاهانه، یا رعایت اصل شفافیت، کوتاهی کرده باشد. در مقابل، مبنای خطر ناظر به مسئولیت صرف‌نظر از تقصیر است؛ یعنی صرف بهره‌برداری از داده‌ها، به‌ویژه در سیستم‌های بزرگ و خودکار، فرد را در معرض خطر قرار داده و بنابراین جمع‌کننده یا پردازشگر داده‌ها باید مسئولیت زیان را بپذیرد. مبنای انصاف نیز در شرایطی که اثبات تقصیر یا رابطه‌ی علیت دشوار یا غیرممکن است، می‌کوشد از منظر عدالت جبرانی، حمایت مؤثری از زیاندیده به‌عمل آورد. در نهایت، مبنای حمایت از حریم خصوصی که خاص حوزه داده‌هاست، بر این اصل استوار است که داده‌های شخصی بخشی از شخصیت فرد محسوب می‌شوند و هرگونه خدشه به آن‌ها، حتی بدون زیان مادی یا اثبات تقصیر، باید مسئولیت‌آور باشد (قناد و همکاران، ۱۳۹۹: ۳۱). در حقوق اتحادیه اروپا، به‌ویژه در مقررات GDPR، این مبانی در هم تنیده شده‌اند تا یک سازوکار جامع، پیشگیرانه و جبرانی برای حفاظت از اطلاعات شخصی فراهم آورند. در حقوق ایران نیز، هرچند هنوز قانون جامعی همچون GDPR وجود ندارد، اما اصول کلی مسئولیت مدنی و حقوق مربوط به شخصیت می‌تواند زمینه‌های پذیرش و توسعه این مبانی را فراهم سازد.

۱-۵-۱- نظریه تقصیر

نظریه تقصیر، یکی از بنیادی‌ترین مبانی توجیه‌کننده مسئولیت مدنی در حقوق سنتی است. بر اساس این نظریه، مسئولیت مدنی تنها زمانی محقق می‌شود که فعل یا ترک فعلی از سوی فاعل صورت گرفته باشد که برخلاف معیارهای عرفی یا قانونی رفتار متعارف بوده و در نتیجه، به دیگری زیانی وارد شده باشد. در حقوق ایران نیز ماده ۱ قانون مسئولیت مدنی، تقصیر را به‌عنوان مبنای اصلی در نظر گرفته و جبران ضرر را مشروط به آن دانسته است. در حوزه نقض داده‌های شخصی، این نظریه زمانی کاربرد دارد که

مسئول پردازش داده، از استانداردهای امنیتی یا تعهدات قانونی خود عدول کرده باشد؛ برای مثال، عدم استفاده از سیستم رمزنگاری یا حفاظت مناسب از سرورها. اما دشواری بزرگ این نظریه در این حوزه آن است که اثبات تقصیر نیازمند آگاهی دقیق از فرایندهای فنی درون‌سازمانی و نحوه مدیریت داده‌هاست؛ امری که از توان بسیاری از افراد زیان‌دیده خارج است. به همین دلیل، منتقدان نظریه تقصیر در این حوزه بر این باورند که این نظریه توان پاسخگویی مؤثر به خسارات مدرن، از جمله آسیب‌های داده‌ای را ندارد، مگر آنکه با نهادهایی چون فرض تقصیر یا مسئولیت تضامنی تکمیل شود (عوده، ۱۳۸۹: ۲۶).

۱-۵-۲- نظریه خطر (ریسک)

نظریه خطر، مبنای جدیدتر و توسعه‌یافته‌تری نسبت به نظریه تقصیر در حوزه مسئولیت مدنی به‌شمار می‌رود که با تحولات فناوری و صنعتی قرن بیستم ظهور یافت. این نظریه مبتنی بر آن است که هر کس با فعالیت خود، خطری برای دیگران ایجاد می‌کند، باید خسارات ناشی از آن را جبران کند، حتی اگر مرتکب تقصیر نشده باشد. در حوزه داده‌های شخصی، شرکت‌ها و سازمان‌هایی که اطلاعات حساس افراد را جمع‌آوری و ذخیره می‌کنند، با این عمل، ریسک‌های بالقوه‌ای برای حریم خصوصی افراد ایجاد می‌نمایند. برای مثال، پلتفرم‌های دیجیتال، حتی اگر تمامی اقدامات امنیتی را رعایت کرده باشند، به‌دلیل ذات آسیب‌پذیر داده‌ها، همچنان امکان بروز نشت اطلاعات وجود دارد. در چنین شرایطی، بر اساس نظریه خطر، مسئولیت مدنی باید بدون نیاز به اثبات تقصیر، صرفاً بر مبنای وقوع زیان و ارتباط با فعالیت پردازش‌گر اعمال گردد. مقررات GDPR نیز گرچه در ظاهر همچنان از مفهوم تقصیر بهره می‌برد، اما در عمل، با تحمیل استانداردهای بسیار بالا و سازوکارهای معکوس اثبات، به نظریه خطر بسیار نزدیک شده است. در نتیجه، پذیرش این نظریه در حقوق ایران می‌تواند گامی مهم در جهت حمایت از حقوق کاربران و تضمین امنیت داده‌ها باشد (انصاری، ۱۴۰۰: ۸۳).

۱-۵-۳- نظریه انصاف

نظریه انصاف، با تکیه بر اصول اخلاقی و عدالت توزیعی، تلاش دارد خلأهای نظام‌های خشک حقوقی را در مواردی که اثبات عناصر سنتی مسئولیت دشوار یا غیرممکن است، جبران نماید. این نظریه می‌پذیرد که در مواردی ممکن است هیچ‌گونه تقصیر یا حتی خطر غیرمتعارفی از سوی مسئول مشاهده نشود، اما عدالت ایجاب می‌کند که زیان‌دیده تنها نماند و خسارت وارده به نوعی جبران شود. در حوزه داده‌های شخصی، مواردی وجود دارد که به‌رغم رعایت تمامی استانداردهای فنی، اطلاعات کاربران نشت می‌یابد و خسارات معنوی یا حیثیتی بر آن‌ها وارد می‌شود. نظریه انصاف در این موارد، با در نظر گرفتن ظرفیت مالی پردازش‌گر، میزان فایده‌ای که از پردازش داده برده است، و وضعیت زیان‌دیده، به‌دنبال ارائه راه‌حلی عادلانه

است. این نظریه در رویه قضایی برخی کشورهای اروپایی مورد توجه قرار گرفته و دادگاه‌ها بر اساس اصول انصاف، گاه حکم به جبران خسارت داده‌اند حتی در غیاب تقصیر یا خطر. پذیرش این نظریه در حقوق ایران، اگرچه هنوز نهادینه نشده، اما با استناد به اصول کلی حقوقی، از جمله قاعده لاضرر و اصل عدالت، قابلیت دفاع و توسعه دارد (انصاری، ۱۴۰۰: ۱۲۲).

۱-۵-٤- مبنای حمایت از حریم خصوصی

یکی از پیشرفته‌ترین دیدگاه‌ها در تبیین مسئولیت مدنی ناشی از نقض داده‌ها، رویکردی است که «حریم خصوصی» را نه‌تنها موضوع حمایت بلکه مبنای مستقل مسئولیت می‌داند. بر این اساس، نقض حریم خصوصی به‌خودی‌خود، واجد وصف نامشروع و مستوجب جبران خسارت است، بی‌آن‌که نیازی به اثبات تقصیر، خطر یا حتی زیان مادی باشد. این نگاه، مبتنی بر تحولات حقوق بشر و توسعه مفهوم حق بر داده‌های شخصی در قرن بیست‌ویکم است. در نظام حقوقی اتحادیه اروپا، این نگرش به‌ویژه پس از تصویب GDPR تقویت شد و دیوان عدالت اروپا نیز در آرای مختلف، بر شأن مستقل «حق بر حفاظت از داده‌ها» تأکید کرده است. به‌عبارت دیگر، داده‌های شخصی نه صرفاً اطلاعات، بلکه بخشی از شخصیت حقوقی و شأن انسانی افراد تلقی می‌شود. در حقوق ایران، گرچه صراحت قانونی در این زمینه وجود ندارد، اما با استناد به اصول فقهی چون حرمت تجسس و حفظ اسرار و همچنین قواعد عام شریعت اسلامی، می‌توان بر لزوم حمایت ویژه از داده‌های شخصی و مسئولیت مدنی ناشی از نقض آن‌ها استدلال کرد. چنین رویکردی زمینه‌ساز تدوین قوانین نوین حمایتی در ایران خواهد بود (کاتوزیان، ۱۳۹۵: ۴۶).

۱-٦- تاریخچه‌ی حمایت از داده‌ها

حمایت و پاسداری از داده‌ها و اطلاعات مربوط به زندگی اشخاص نیز با تاخیری کم و بیش طولانی نسبت به سایر موضوعات مورد حمایت در حریم خصوصی مورد توجه انسانها و به طور کلی جوامع قرار گرفت.

۱-٦-۱- تاریخچه قانونگذاری در سطح داخلی

ظهور فناوری اطلاعات و ارتباطات مزایای بسیاری را برای تمامی مردم جهان به ارمغان آورده و خواهد آورد. با وجود نقش ویژه‌ی آن در زندگی افراد و جوامع مختلف این تکنولوژی بستر مناسبی برای نادیده گرفتن حقوق و آزادیهای فردی و اجتماعی اشخاص می‌باشد به منظور جلوگیری از معضلات و مشکلات ناشی از آن حاکمیت قانون در این حوزه اجتناب ناپذیر است. با این وجود در طول دهه ۱۹۶۰، هر دو

بخش دولتی و خصوصی کسب منفعت از طریق پردازش خودکار داده‌ها را مهم‌تر از مشکلات مربوط به حفظ حریم خصوصی که ناشی از فناوری جدید بود می‌دانستند اما با گذشت سالها کشورها کم کم توجه بیشتری از خود نسبت به خطرات احتمالی پنهان در فناوری نشان دادند و اقدام به تدوین قوانینی در این حوزه کردند (انصاری، ۱۳۸۶: ۵۹).

اولین قانون ملی با هدف حمایت از حریم خصوصی اطلاعاتی افراد در سال ۱۹۷۳ در کشور سوئد شکل گرفت. قانون ۱۹۷۳ تنها ثبت‌های کامپیوتری پردازش داده‌های شخصی را پوشش می‌داد. در این قانون مفاد زیادی در رابطه با چگونگی پردازش داده‌ها یا اصول کلی حمایت از داده‌ها وجود نداشت. مطابق آن برای هر ثبت نیاز به یک مجوز قبلی از مراجع حمایت از داده‌های شخصی بود مراجع ضمن دادن مجوز شرایط خاصی را نیز برای آن ثبت تعیین می‌کردند در کنار این، قانون قوانین متعددی برای حمایت از داده‌های شخصی خاص به تصویب رسید. برخلاف قانون عام ۱۹۷۳ شرایط ثبت داده‌های شخصی خاص در قوانین مذکور اعلام شده بود. دولت آلمان نیز در سال ۱۹۷۳ لایحه‌ای مرتبط با پردازش داده‌ها تدوین می‌کند. این لایحه بعد از اصلاحات فراوان به دلیل اختلافاتی که بین دولت با مجلس فدرال و نمایندگان وجود داشت سرانجام در سال ۱۹۷۷ به تصویب رسید این قانون به صورت منحصر بفرد به داده‌های شخصی نمی‌پرداخت بلکه به منظور حمایت از حریم خصوصی داده‌ها را در برابر تعرضات مورد حمایت قرار می‌داد. این قانون در سال‌های ۲۰۰۹ و ۲۰۱۰ مورد اصلاحاتی قرار گرفت در سال ۱۹۸۳ بر مبنای تصمیم دادگاه قانون اساسی فدرال حمایت از داده‌ها در ابعاد جدیدی توسعه پیدا می‌کند بر اساس نظر دادگاه تعیین سرنوشت اطلاعاتی به عنوان یک حق اساسی برای اشخاص شناخته می‌شود و هر دخل و تصرفی در داده‌های شخصی باید با رضایت موضوع داده یا یک مجوز قانونی باشد. دیوان قانون اساسی آلمان در رأی صادره در ۱۵ دسامبر با استناد به اصول ۱ و ۲ قانون اساسی مصوب سال ۱۹۴۹ به ترتیب در مورد کرامت انسانی و حق برخورداری از رشد شخصیتی چنین اظهار نظر می کند قاعدتاً قانون اساسی این توان را برای فرد می‌شناسد که بتواند برای انتقال داده‌های شخصی‌اش و استفاده از آنها تصمیم گیری کند. در سال ۱۹۹۰ این حقوق و تکالیف در قالب قانون جدیدی به تصویب می‌رسند (لطیف زاده، ۱۴۰۱: ۱۱).

فرانسه سومین کشوری است که در سال ۱۹۷۸ با تصویب قانونی در زمینه‌ی فناوری اطلاعات فایل‌های داده و حقوق و آزادیهای فردی به حمایت از داده‌های شخصی پرداخت برخی بر این باورند که دستور العمل اروپایی ۱۹۹۵ حمایت از داده‌ها با الهام از این قانون تدوین شده است. بعدها قانون ۱۹۷۸ برای مطابقت با آخرین تغییرات قوانین اتحادیه اروپا چندین بار اصلاح شده است. همچنین مراجع مستقلی به منظور نظارت بر اعمال قانون مذکور و آگاه کردن موضوع داده و کنترلگر از حقوق و تکالیفشان پیش بینی شده بود (Misek,2018: 23).

۱-٦-۲- تاریخچه قانونگذاری در سطح منطقه‌ای

بعد از جنگ جهانی دوم شورای اروپا به منظور ترویج حاکمیت قانون دموکراسی حقوق بشر و توسعه‌ی اجتماعی در سال ۱۹۵۰ کنوانسیون اروپایی حقوق بشر را تصویب کرد. ماده ۸ این کنوانسیون درباره‌ی حمایت از حریم خصوصی و زندگی خانوادگی اعلام می‌دارد:

۱. هرکس از حق احترام به زندگی خصوصی و خانوادگی خانه و مراسلات خود برخوردار است.
۲. در اجرای این حق هیچ مداخله‌ای نباید از سوی هیچ یک از مقامات دولتی صورت گیرد مگر مداخلات منطبق بر قانون و مواردی که در یک جامعه‌ی مردم سالار به دلایل حفظ امنیت ملی، ایمنی عمومی یا رفاه اقتصادی کشور پیشگیری از هرج و مرج و جرائم حفاظت از سلامتی و اخلاقیات یا حفاظت از حقوق سایرین ضروری تشخیص داده شوند (لطیف زاده، ۱۴۰۱: ۱۲).

همانگونه که پیشتر به آن اشاره شد با ظهور فناوری اطلاعات نیاز به قوانین دقیقی بود برای حمایت از داده‌های شخصی به منظور مصون نگه داشتن حریم خصوصی افراد از هرگونه تعرض همچنین با توجه به اینکه فضای مجازی فضایی بدون مرز است تعدد نظامهای حقوقی حمایتی موجب می‌شد بخش عمده‌ای از تلاشهای قانونگذارن در امر قانونمند کردن این فضا با ناکامی مواجه شود بنابر این در اواسط دهه‌ی ۱۹۷۰ کمیته‌ی وزیران شورای اروپایی قطعنامه‌های مختلفی را با توجه به ماده ۸ کنوانسیون مذکور در این زمینه به تصویب رساند برای مثال می‌توان به کنوانسیون حمایت از افراد در مقابل پردازش خودکار داده‌های شخصی اشاره کرد این کنوانسیون اولین سند اروپایی به شمار می‌آید که صراحتاً به موضوع حمایت از داده‌ها پرداخته است و تا قبل از لازم الاجرا شدن آیین نامهی ۲۰۱۶ تنها سند الزام آور در این حوزه محسوب می‌شد کلیه‌ی پردازشهایی که توسط بخش خصوصی یا عمومی انجام می‌شوند مشمول این کنوانسیون خواهند بود هدف آن حمایت از حریم خصوصی اشخاص در برابر سوء استفاده‌هایی است که ضمن پردازش داده‌های شخصی ممکن است رخ دهد. اما همچنان تصویب چنین کنوانسیونهایی نتوانست یکپارچگی لازم را در سطح اتحادیه اروپا ایجاد کند در حالی که برخی کشورها رویهای سخت گیرانه را در این حوزه اعمال می‌کردند در بعضی دیگر قوانینی در این ارتباط وجود نداشت (همان، ۱۵).

۲- قوانین و مقررات ایران و اتحادیه اروپا

۲-۱- حقوق حفاظت از داده‌های شخصی در اتحادیه اروپا

اتحادیه اروپا برای یکسان‌سازی قواعد پردازش داده‌های شخصی، در سال ۱۹۹۵ دستورالعمل ۴۶/۹۵ را تصویب کرد. سپس، در سال ۲۰۰۰، منشور حقوق و آزادی‌های اساسی را به تصویب رساند که در ماده ۸، حق حفاظت از اطلاعات را شناسایی کرد. در سال ۲۰۱۰، سند «رویکرد جامع در مورد محافظت از داده‌ها» به منظور تقویت حقوق اشخاص و گسترش ابعاد بازار داخلی تصویب شد. بر اساس این سند، کمیسیون اروپا در سال ۲۰۱۲ بسته اصلاحات جدیدی را پیشنهاد داد که در نهایت به تصویب مقررات ۶۷۹/۲۰۱۶ در ۲۷ آوریل ۲۰۱۶ منجر شد. این مقررات، که جایگزین دستورالعمل ۱۹۹۵ شد، از ۲۵ مه ۲۰۱۸ لازم‌الاجرا گردید و کنترل‌کنندگان، پردازشگران و افراد موضوع داده را بدون در نظر گرفتن ملیت یا محل اقامت شامل می‌شود (انصاری، ۱۴۰۱: ۶۳). بر اساس ماده ۳ مقررات عمومی حفاظت از داده‌ها، این مقررات به تمامی کنترل‌کنندگان و پردازشگرانی که در اتحادیه اروپا مستقر هستند یا داده‌های اشخاص اروپایی را پردازش می‌کنند، اعمال می‌شود. کنترل‌کننده، شخص حقیقی یا حقوقی است که اهداف و ابزار پردازش داده‌های شخصی را تعیین می‌کند، در حالی که پردازشگر، شخصی است که به نیابت از کنترل‌کننده پردازش داده‌ها را انجام می‌دهد (ماده ۴ مقررات عمومی حفاظت از داده‌ها).

۲-۱-۱- مقررات عمومی حفاظت از داده‌ها

طبق بند ۱ ماده ۴ مقررات عمومی حفاظت از داده‌ها، داده شخصی هرگونه اطلاعات مربوط به شخص حقیقی شناخته‌شده یا قابل‌شناسایی است، از جمله نام، شماره شناسایی، اطلاعات مکانی، شناسه آنلاین، یا ویژگی‌های فیزیکی، ژنتیکی، روانی، اقتصادی، فرهنگی و اجتماعی. این تعریف در کنوانسیون مدرن حفاظت از داده‌های شخصی (اصلاح ۲۰۱۸) نیز آمده است.

با توجه به تأثیر پردازش داده‌های شخصی بر حریم خصوصی، ماده ۷ منشور حقوق و آزادی‌های اساسی اتحادیه اروپا به حفاظت از زندگی خصوصی تأکید دارد. ماده ۹ مقررات عمومی حفاظت از داده‌ها، برخی از داده‌های حساس مانند اطلاعات نژادی، قومی، عقاید مذهبی، داده‌های ژنتیکی و بیومتریک، اطلاعات سلامتی و گرایش جنسی را تحت محدودیت‌های خاصی قرار داده است (Georgieva & Kumer, 2020: 369). پردازش این داده‌ها، جز در موارد مشخص‌شده در قانون، ممنوع است و کنترل‌کنندگان و پردازشگران موظف‌اند تدابیر فنی و سازمانی مناسبی را برای تضمین امنیت آن‌ها اتخاذ کنند (ماده ۲۵ مقررات عمومی حفاظت از داده‌ها). در مواردی که پردازش داده‌های حساس در مقیاس بزرگ انجام می‌شود، کنترل‌کننده باید پیش از انجام پردازش، اثرات آن را ارزیابی کند. همچنین، در

چنین مواردی، انتصاب «مأمور حفاظت از داده» الزامی است تا بر عملکرد کنترل‌کننده و پردازشگر نظارت داشته باشد.

۲-۲- حفاظت از داده‌های شخصی در نظام حقوقی ایران

نظام حقوقی ایران در راستای حمایت از داده‌های شخصی با تصویب قانون تجارت الکترونیکی در سال ۱۳۸۲، مفهوم «داده پیام» و «داده پیام‌های شخصی» را وارد ادبیات حقوقی کرد. این قانون برخی اطلاعات را تحت حمایت کیفری قرار داده است (ماده ۱ ق.ت.ا). با تصویب قانون انتشار و دسترسی آزاد به اطلاعات (۱۳۸۷) و قانون جرائم رایانه‌ای (۱۳۸۸)، برخی جرائم نظیر دسترسی و تغییر غیرمجاز داده‌ها جرم‌انگاری شد (حیدری و همکاران، ۱۳۹۹: ۵۹). به دلیل رشد فناوری اطلاعات، نیاز به قوانین تخصصی‌تر احساس شد. در سال ۱۳۹۶، «لایحه حمایت از داده و حریم خصوصی در فضای مجازی» و در سال ۱۳۹۷، «لایحه صیانت از داده‌های شخصی» تدوین شد که هنوز در مجلس بررسی می‌شود. این لوایح اصطلاحاتی همچون «کنترل‌گر» و «پردازشگر» را معرفی کرده و دامنه شمول آن‌ها حتی اشخاص خارج از کشور را نیز در برمی‌گیرد (بند ۴ و ۵ ماده ۱ لایحه).

قانون تجارت الکترونیکی، داده پیام شخصی را هرگونه اطلاعات مرتبط با فرد حقیقی معین می‌داند. همچنین، شیوه‌نامه تفکیک اطلاعات، داده‌های شخصی را شامل داده‌های هویتی، مکانی، اقتصادی و ارتباطاتی می‌داند. ماده ۵۸ ق.ت.ا ذخیره، پردازش و توزیع داده‌های حساس مانند اطلاعات قومی، مذهبی و پزشکی را بدون رضایت ممنوع کرده است (ماده ۵۹ ق.ت.ا). علاوه بر این، ضمانت اجرای تخلفات در ماده ۷۱ ق.ت.ا یک تا سه سال حبس تعیین شده که رویکردی کیفری است، برخلاف اتحادیه اروپا که از ضمانت اجراهای غیرکیفری مانند جریمه نقدی استفاده می‌کند.

در مجموع، قانونگذار ایران برخلاف اتحادیه اروپا تنها داده‌های شخصی حساس را مشمول مقررات سختگیرانه کرده و سایر داده‌های شخصی مشمول حمایت خاصی نیستند. این در حالی است که اتحادیه اروپا برای همه داده‌های شخصی، الزامات حفاظتی یکسانی در نظر گرفته و برای داده‌های حساس تدابیر مضاعفی مانند ارزیابی حفاظت از داده و مأمور حفاظت از داده را مقرر کرده است (حیدری و همکاران، ۱۳۹۹: ۵۹).

۲-۳- ماهیت حق حمایت از داده‌ها

در این بخش، به بررسی این پرسش می‌پردازیم که آیا حمایت از داده‌ها یک حق اساسی ویژه محسوب می‌شود و باید آن را به عنوان یک حق اساسی بشری تلقی کرد. این حق، بازتابی از تلاش‌هایی فراتر از استدلال‌های حقوقی صرف است که بر مبنای آن، حمایت از داده‌ها به‌عنوان یک حق اساسی شناخته

شده است، زیرا اتحادیه اروپا چنین برداشتی را اتخاذ کرده است. پاسخ به این پرسش، به تدوین‌کنندگان پیش‌نویس منشور کمک کرده است تا نشان دهند چرا حمایت از داده‌ها را یک حق اساسی مستقل می‌دانند؛ هرچند که منابع محدودی به این موضوع پرداخته‌اند. در تفسیر برخی از متخصصان، اشاره شده است که ازآنجاکه ماده ۷ منشور حقوق بنیادین اتحادیه اروپا، طیف گسترده‌ای از موضوعات ازجمله زندگی خانوادگی، خصوصی، خشونت خانگی و محرمانگی ارتباطات را پوشش می‌دهد، تدوین‌کنندگان منشور، ماده‌ای مجزا را برای حمایت از داده‌های شخصی اختصاص دادند تا به این مسئله توجه کافی شود. به همین دلیل، ماده ۸ منشور، حق حمایت از داده‌های شخصی را به‌عنوان یک حق اساسی جدید و مستقل از حق احترام به زندگی خصوصی و خانوادگی به رسمیت شناخته است. این ماده از اسناد مختلف حقوقی الهام گرفته است، هرچند که حمایت از داده‌های شخصی را به‌عنوان یک حق ویژه در چارچوب اسناد بین‌المللی حقوق بشر به رسمیت نمی‌شناسد. ماده ۸ منشور، به‌طور خاص تحت تأثیر ماده ۸ کنوانسیون اروپایی حقوق بشر قرار گرفته است که در آرای دادگاه اروپایی حقوق بشر پیرامون حفاظت از حریم خصوصی و زندگی خصوصی مورد استناد قرار گرفته است، هرچند که این کنوانسیون به‌صراحت به حفاظت از داده‌های شخصی اشاره‌ای نکرده است (قناد، ۱۳۹۹: ۱۷).

با این‌حال، این استدلال‌ها به‌تنهایی نمی‌توانند موضوع را از نظر حقوقی به‌روشنی تبیین کنند. درعین‌حال، بررسی قواعد حمایت از داده‌ها و آرای دادگاه اروپایی نشان می‌دهد که برخی از این قواعد به‌وضوح به‌عنوان اصول اساسی شناخته می‌شوند. به‌عنوان نمونه، دستورالعمل‌ها و مقررات اتحادیه اروپا درباره پردازش داده‌های شخصی حساس، مانند اطلاعات مربوط به گرایش سیاسی یا جنسی، وضعیت پزشکی یا نژاد، آنها را به‌عنوان داده‌های ضروری و اساسی در یک جامعه دموکراتیک معرفی کرده‌اند. علاوه بر این، برخی از پرونده‌های مورد بررسی در دیوان دادگستری اتحادیه اروپا، ماهیتی دارند که حمایت از آنها را می‌توان به‌عنوان حمایت از حقوق اساسی انسان تلقی کرد.

۳- مسئولیت مدنی در نقض داده‌های شخصی

۳-۱- ضرر و زیان در مسئولیت مدنی ناشی از نقض داده‌های شخصی

برای تحقق مسئولیت مدنی وجود سه رکن لازم است وجود ضرر و خسارت، تقصیر یا فعل زیانبار و رابطه‌ی سببیت عرفی هدف مسئولیت مدنی جبران ضرر است؛ بنابراین، بدون ضرر، مسئولیت نیز وجود نخواهد داشت ضرر از نظر فقهی این چنین تعریف شده است: نقصی است در مال یا آبرو یا نفس یا شأنی از شئون موجود انسان یا شأنی که مقتضی نزدیک آن وجود دارد به نحوی که عرف آنشان را موجود می‌بیند (محقق داماد، ۱۳۹۳: ۲۸). بدیهی است رکن ضرر نسبت به نقض حریم خصوصی داده وقتی

محقق می‌شود که وجود حریم خصوصی داده انکار نشده باشد یکی از نظریه‌هایی که اخیراً در میان حقوقدانان غربی مطرح شده است و مسئولیت مدنی ناشی از نقض حریم خصوصی داده را تحت تأثیر قرار می‌دهد، نظریه‌ی نقض حریم خصوصی داده است. با پذیرش نظریه‌ی نقض حریم خصوصی داده، نقض حریم خصوصی داده موجب مسئولیت نخواهد شد؛ زیرا سالبه به انتفای موضوع خواهد بود و در واقع ضرری محقق نشده است قائلان نظریه‌ی نقض حریم خصوصی داده که در آمریکا بیشتر طرفدار دارد ادله‌ای برای این نظریه مطرح کرده‌اند گفته شده شناسایی حریم خصوصی داده به نفع خلاف کارهاست و این دسته از افراد اطلاعاتی برای مخفی کردن دارند و الا حریم خصوصی داده‌ها و اطلاعات دغدغه‌ی عمومی نیست (قهرمانی، ۱۳۷۷: ۲۹).

در نقد این دلیل باید گفت اولاً حریم خصوصی داده مورد نیاز هر انسانی است که از لحاظ روانی سالم است و نقض آن آزار دهنده است. ثانیاً اگر این مبنا مورد پذیرش شارع می‌بود، غیبت جایز بود؛ زیرا با این مبنا، از آنجا که موضوع غیبت، فردی است که خلافی انجام داده، پس می‌توان گفت غیبت بازدارندگی از خطا ایجاد می‌کند و حال آنکه چنین چیزی هرگز مورد پذیرش شارع نیست. گفته شده نتیجه‌ی وضع قوانین درباره‌ی حریم خصوصی داده کوچک‌تر شدن دوربین‌ها و وسایل نقض حریم خصوصی داده است در حالی که راحت‌تر شدن نقض حریم (در نتیجه‌ی توسعه فناوری) حمایت بیشتر از حریم خصوصی داده را می‌طلبد نه نفی آن را. اگر امروزه نقض حریم خصوصی داده برای اشخاص ساده‌تر و کم هزینه‌تر شده و احتمال نقض حریم خصوصی داده بسیار بیشتر شده است، باید حمایتهای حقوقی از زیان دیده بیشتر شود نه اینکه از اساس منکر وجود حریم خصوصی داده شویم باید هر چقدر نقض حریم ساده‌تر می‌شود و احتمال آشکار شدن شخص مسئول کمتر می‌شود محتمل میزان مسئولیت حقوقی نقض کننده‌ی حریم خصوصی داده افزایش یابد تا توازن و نظم حقوقی حفظ شود (حیدری و همکاران، ۱۳۹۸: ۳۱).

به نظر می‌رسد بهترین دلیلی که می‌توان برای نظریه‌ی نقض حریم خصوصی اقامه کرد، نبود انتظار متعارف برای حفظ اطلاعات داده‌ها در عصر کنونی است. به عبارت دیگر فناوری اطلاعات، مزایا و معایبی دارد که به صورت یک بسته به ما عرضه شده و ما نمی‌توانیم از مزایای آن بدون تبعات منفی آن استفاده کنیم، یا هر دو (مزایا و تبعات) یا هیچ کدام. نقض حریم خصوصی، داده هزینه‌ی مزایای بسیاری است که از آن برخورداریم و باید به آنها توجه داشته باشیم (به لسان فقهی من له الغنم فعلیه الغرم) زندگی در یک مملکت پایگاه داده مسائل مثبتی هم دارد؛ برای مثال سوابق اعتبار گزارش بدهی‌ها پرداخت‌ها عدم پرداختها نظم پرداختها و ...) اطلاعات و داده‌ها مفیدی را درباره‌ی توان افراد برای تقبل مسئولیت‌های مالی به وام دهنده‌ها می‌دهند. پایگاه‌های داده گردآوری و ارزیابی داده‌ها را ممکن می‌سازند و در بعد نظری، به مصرف کننده و اقتصاد کمک می‌کنند (شهیدی، ۱۳۸۲: ۷۳).

در ایالات متحده تا چند دهه‌ی پیش متقاضیان دریافت وام باید با وام دهنده مستقیماً ملاقات و هفته‌ها صبر کنند تا سابقه‌ی اعتبار آنها مشخص شود. امروز به کمک پایگاه‌های داده‌ی مرکزی می‌توان پاسخ تقاضای وام را به صورت تلفنی دریافت کرد. این پایگاه‌های داده تصمیم گیری را بسیار آسان‌تر سریع‌تر و کارآتر کرده‌اند مغازه‌ها از کارت‌های تخفیف، نه تنها برای جلب مشتری، بلکه برای ارزیابی کارایی تبلیغات نیز استفاده می‌کنند این کارت‌ها باعث می‌شود که صاحبان مغازه‌ها چگونگی تأثیر قیمت را بر تقاضا ارزیابی و خریدهای آینده‌ی مشتریان خود را بهتر پیش بینی کنند «اسمارت تگ[1]» که نوعی سامانه الکترونیکی است برای دریافت عوارض، استفاده از کارت «ایزی پس[2]» را پدید آورده است «ایزی پس» کارتی است مغناطیسی که با پرداخت مبلغی شارژ شده و با هر بار، استفاده مبلغ عوارض به طور خودکار از میزان اعتبار آن کم می‌شود. این یعنی سرعت و سهولت بیشتر برای رانندگان... و همچنین اینکه پایگاه داده در حال ثبت داده‌ها درباره عبور و مرور ما از ایستگاه‌های اخذ عوارض و حتی سرعت ما با مقایسه زمان سفر، با فاصله‌ی بین دو ایستگاه اخذ عوارض هستند. به تعبیر غربی‌ها، برادر بزرگ، مراقب رفتار و اعمال ما است (عوده، ۱۳۸۹: ۱۱۵).

نظریه‌ی «نقض حریم خصوصی داده‌ها» در کشور آمریکا طرح و ترویج شده است. نکته‌ی جالب و قابل تأمل در این خصوص این است که با توجه به مباحث حریم خصوصی داده‌ها و مالکیت فکری (تا حدی که به مال انگاری حریم خصوصی داده‌ها بر اساس الگوی مالکیت فکری منجر شده است)، رویکرد سیستم حقوقی آمریکا به این دو مقوله کاملاً متفاوت است. در حالی که آنها مدافع جدی مالکیت فکری بودند نه تنها از مال انگاری حریم خصوصی داده‌ها دفاع نمی‌کنند، بلکه معتقد به نقض حریم خصوصی داده‌ها هستند. این شائبه به صورت جدی وجود دارد که این تفاوت، رویکرد ناشی از ملاحظات غیر حقوقی باشد؛ زیرا هم اکنون بیشترین نفع و کمترین زیان از نقض حریم خصوصی داده‌ها متوجه آمریکا می‌شود، به دلیل اینکه اینترنت ابزاری در دست سازمان NSA[3] آمریکا است و نقض حریم خصوصی داده‌ها کاربران و پردازش آنها نه تنها برای این سازمان به سادگی امکان پذیر است بلکه اساساً، جزء وظایف ذاتی این سازمان است (قاسم‌زاده، ۱۳۸۷: ۵۷)

ضررهای ناشی از نقض حریم خصوصی اطلاعات به طور خاص خسارات معنوی ناشی از تجاوز به حقوق شخصیت محسوب می‌شوند. حقوق مربوط به شخصیت حقوقی است که به هر انسانی، قطع نظر از وابستگی‌اش به گروه اجتماعی خاصی تعلق دارد. حقوقی که بیشتر از شخص انسان حمایت می‌کند تا

---

1. Smart Tag
2. Easy Pass
3. آژانس امنیت ملی آمریکا (NSA) نهادی اطلاعاتی است که مسئول جمع‌آوری و تحلیل اطلاعات الکترونیکی و ارتباطی برای حفظ امنیت ملی ایالات متحده است.

منافع مادی او حقوق مربوط به شخصیت، برخلاف حقوق مالی، غیرقابل انفکاک از شخص و شخصیت انسان است (انصاری، ۱۴۰۰: ۵۲). به تعریف «ژان دابن[۱]»، حقوق مربوط به شخصیت، حقوقی است که موضوع آنها عناصر تشکیل دهنده‌ی شخصیت است. هرچند خسارتهای ناشی از نقض حریم خصوصی غالباً جنبه‌ی معنوی دارند لکن در مورد حریم خصوصی اطلاعات و داده‌ها بر مبنای تئوری مال انگاری حریم خصوصی اطلاعات و داده‌ها نقض آن خسارت مادی به شمار می‌رود لذا در ادامه به بررسی این نظریه می‌پردازیم.

۳-۲- مسئولیت مدنی ناشی از نقض داده‌های شخصی در ارتباطات اینترنتی

مسئولیت مدنی ناشی از نقض داده‌های شخصی در ارتباطات اینترنتی از مهم‌ترین چالش‌های حقوقی عصر دیجیتال به شمار می‌آید. با گسترش استفاده از فناوری‌های ارتباطی و اینترنت، حجم عظیمی از داده‌های شخصی افراد در بسترهای مختلف مانند شبکه‌های اجتماعی، پیام‌رسان‌ها، پلتفرم‌های تجارت الکترونیک و خدمات ابری منتقل و ذخیره می‌شود. در این میان، هرگونه نقض، افشاء، دسترسی غیرمجاز، یا استفاده نادرست از این داده‌ها می‌تواند موجب ورود خسارت‌های مادی و معنوی به افراد شود. بر این اساس، نظام‌های حقوقی مختلف از جمله ایران و اتحادیه اروپا، تلاش کرده‌اند تا با شناسایی حقوق افراد نسبت به داده‌های خود، تعیین وظایف و مسئولیت‌های اشخاص حقیقی و حقوقی که این اطلاعات را پردازش یا نگهداری می‌کنند، و نیز پیش‌بینی سازوکارهای جبران خسارت، از حریم خصوصی اشخاص در فضای مجازی حمایت کنند. در حقوق ایران، هرچند قوانین پراکنده‌ای در این زمینه وجود دارد، اما نبود قانون جامع حمایت از داده‌ها، باعث بروز ابهامات فراوانی در تعیین مسئولیت مدنی ناشی از نقض اطلاعات در فضای ارتباطات اینترنتی شده است (انصاری، ۱۴۰۰: ۲۵). در مقابل، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) با ارائه چارچوبی مشخص، از جمله اصل رضایت، اصل شفافیت، و حق دسترسی و حذف اطلاعات، توانسته است الگویی پیشرفته برای شناسایی مسئولیت‌های مدنی در این زمینه ارائه دهد.

---

[۱] ژان دابن (Jean Dabin) یک حقوقدان برجسته و شناخته‌شده بلژیکی است. او یکی از متفکران تأثیرگذار در حوزه‌ی حقوق مدنی، به‌ویژه حقوق شخصیت (Droits de la personnalité) در نظام حقوقی رومی–ژرمنی (Civil Law) بوده است.

۳-۲-۱- مسئولیت مدنی ناشی از ارتباطات از منظر حقوق ایران

موضوع مسئولیت مدنی ناشی از ارتباطات اینترنتی به صورت مستقل در قانون مدنی مورد اشاره قرار نگرفته است و تنها در این خصوص می‌توان به عمومات مواد قانون مدنی مراجعه نمود. تاریخچه مسئولیت مدنی ناشی از ارتباطات اینترنتی ناظر به یکی از مباحث مهم نظری این شاخه حقوق است که درصدد بیان توجیه قاعده حقوقی لزوم جبران خسارت زیان دیده است. یا این توضیح که وقتی اساس مسئولیت مدنی را به عنوان یک قاعده معرفی کرده و عقیده داریم که وارد کننده زیان متعهد به پرداخت خسارت است این سؤال مطرح می‌شود که دلیل مشروعیت این قاعده چیست؟ پاسخ به این سؤال به دلیل مشروعیت مسئولیت مدنی بازگشته و از این به مبنای مسئولیت مدنی تعبیر می‌شود. شناخت مبنا و تاریخچه مسئولیت ریشه در امور دیگری دارد که برآیند آنها خود را به عنوان پایه مسئولیت مدنی نشان می‌دهد با شناخت مبنای مسئولیت حقوق دانان تلاش می‌کنند ساختار نظام مندی از ارکان شرایط و قواعد حاکم بر مسئولیت مدنی ترسیم کنند و با عنایت به مبنا، احکام موضوعات جدید را بیابند. ماده ۳۰۷ قانون مدنی، منابع و موجبات تحقق مسئولیت را منحصراً احصا کرده است. بنابراین موضوع مسئولیت مدنی غالباً مصداق یکی از موارد مذکور در این ماده خواهد بود. به جز در مورد غصب که به عقیده حقوقدانان از حیث مبنا و قلمرو احکام با مسئولیت مدنی تفاوت دارد (کاتوزیان، ۱۳۸۲: ۲۶).

سؤال این است که آیا این منابع قابل تطبیق با فضای سایبر نیز و اعمال ارتکابی در فضای سایبر نیز در قالب منابع مذکور در ماده قابل تبیین است؟ در این خصوص نظرات مختلفی قابل طرح است. در باب اتلاف ماده ۳۲۸ قانون مدنی عنوان می‌دارد هر کس مال غیر را تلف کند ضامن آن است و باید مثل یا قیمت آن را بدهد اعم از این که از روی عمد تلف کرده باشد یا بدون عمد و اعم از این که عین باشد یا منفعت و اگر آن را ناقص یا معیوب کند ضامن نقص قیمت آن مال است. در این ماده، مال مفهوم وسیعی دارد و شامل اعیان، منافع، حقوق و عدم النفع مسلم نیز می‌شود. حقوق نیز خود به انواعی تقسیم می‌شود و شامل حق فرد بر تمامیت جسمی، حیثیت خانوادگی یـا بـر شهرت تجاری یا آزادی افراد و سایر حقوق مرتبط می‌شود در اتلاف از بین بردن مال است حال آنکه فضای سایبر اساساً فضایی است که در آن «بالمباشره مستقیم یا به عبارت فقها ارتباط مستقیم و مباشرتی به معنی مرسوم قابل تحقق نیست با این حال باید دید آیا در فضای سایبر اصولاً تحقق مسئولیت مدنی از باب اتلاف امکان پذیر است یا خیر؟ یعنی مثلاً آیا ویروسی که یک «هکر» در شبکه اینترنت وارد کرده و از این طریق به اطلاعات و نرم افزارهای دیگری صدمه وارد کرده است، این صدمه از باب اتلاف است؟ یعنی مباشرتاً محسوب می‌شود و «هکر» مباشر اتلاف است یا اینکه ویروس مزبور، واسطه میان «هکر» و خسارت وارده است که در این صورت باید عمل زیان زننده را تحت باب تسبیب یا اتلاف بالتسبیب بررسی کرد؟ فایده این بحث، زمانی ظهور پیدا خواهد کرد که توجه شود که در حقوق، ایران اتلاف و تسبیب، دو منبع

مستقل ایجاد مسئولیت مدنی هستند و از گذشته قواعد و شروط این دو منبع برای تحقق مسئولیت مدنی متفاوت است. برای مثال در باب تسبیب به عقیده برخی از حقوقدانان تقصیر رکن تحقق مسئولیت است و بدون آن اصولاً مسئولیت مدنی از باب تسبیب قابل تحقق نیست، در حالی که در باب اتلاف، برای تحقق مسئولیت نیازی به تقصیر عامل زیان نیست (ادیب، ۱۳۸۵: ۸۰).

به نظر می‌رسد که می‌توان برخی از افعال زیان بار در فضای سایبر را مصداق باب اتلاف دانست از جمله نقض کپی رایت و نقض علائم تجاری ایراد عدم امکان تحقق مباشرت به اتلاف در فضای سایبر نیز قابل پذیرش نیست چون آنچه میان اتلاف و تسبیب تفاوت گذارده است صرفاً نقش مستقیم یا غیر مستقیم عامل زیان در این باره است (بجنوردی، ۱۳۷۱: ۷۰۵).

۳-۲-۲- مسئولیت مدنی ناشی از نقض داده‌های شخصی در ارتباطات اینترنتی در اتحادیه اروپا

در اتحادیه اروپا مبنای مسئولیت مدنی ناشی از ارتباطات اینترنتی متفاوت‌تر از حقوق ایران می‌باشد در اتحادیه اروپا تنها مبنای مسئولیت مدنی ناشی از ارتباطات اینترنتی را می‌توان در رویه‌ی قضائی و قوانین این کشور مورد مطالعه قرار داد و از این رو می‌توان به مبانی همچون قابلیت پیش بینی ضرر، احراز تقصیر، وحدت گرایی و خطر اشاره نمود. قابل پیش بینی بودن ضرر، امروزه یکی از شرایط قابل مطالبه بودن، زیان قابلیت پیش بینی آن برای عامل ورود زبان است. خسارتی که در فضای مجازی از سوی ارائه کننده خدمات اینترنتی ایجاد می‌شود باید قابل پیش بینی باشد. این قابلیت پیش بینی خواه بر اساس عرف و یا آگاهی ارائه کننده خدمات از نتایج زبان بار عمل خویش استوار می‌گردد به طور کل برخی از اعمال در خود این رکن را مفروض دارند (لطیف زاده و همکاران، ۱۴۰۰: ۲۵). شخصی که ویروس رایانه‌ای را در اینترنت پخش می‌نماید و یا به طور غیر مجاز به سیستم دیگری وارد می‌شود باید مسئولیت هرگونه خساراتی که از انتشار آن ویروس ایجاد می‌گردد و یا خساراتی را که از ورود غیر مجاز به سیستم دیگری حاصل می‌آید بر عهده بگیرد زیرا این قبیل از اعمال بالذات در محیط اینترنت از جمله فعالیتهای خرابکارانه به شمار می‌آیند و افراد و شرکت‌ها، همه ساله خسارات بسیاری از این چنین اعمالی متحمل می‌شوند. خودداری ارائه کنندگان خدمات اینترنتی از بکار بستن اقدامات و اعمال امنیتی و پیشگیرانه به منزله تقصیر به شمار می‌آید. البته، برخی بر این باورند که هم باید امکان پیدایش خسارت برای عامل ورود زیان و هم شخص زیان دیده برای او قابل پیش بینی باشند و حتی اگر زبان برای عامل ورود ضرر قابل پیش بینی بوده باشد ولی شخص زبان دیده برای او قابل پیش بینی نباشد وجود وظیفه‌ای در رابطه میان عامل ورود ضرر و زیان دیده به منظور اثبات مسئولیت عامل نفی می‌گردد. رویه قضائی در نظام حقوقی اتحادیه اروپا در مواردی که خسارت نتیجه مستقیم فعل زبـان بـار (ضرر) باشد، قابل پیش بینی بودن نوع ضرر را شرطی برای مطالبه ضرر می‌داند چه بسا که اگر ضرری بر فردی وارد،

آید باز هم این نوع ضرر می‌بایست قابلیت پیش بینی را دارا باشد (قناد و همکاران، ۱۴۰۰: ۱۹). این امر در حقوق ایران منطبق با نظری است که در مسئولیت بدون تقصیر اتلاف بالمباشره نیز قابل پیش بینی بودن ضرر را در تحقق ضرر قابل جبران شرط می‌داند چرا که پیش از این در رابطه‌ی با اتلاف بالتسبیب مورد بررسی قرار گرفت که در مقابل اتلاف بالمباشره قرار دارد. سؤالی که در اینجا می‌تواند مطرح گردد آن است که قابل پیش بینی بودن ضرر چگونه تواند مبنای مسئولیت مدنی ناشی از ارتباطات اینترنتی در اتحادیه اروپا عنوان گردد؟ به این مسئله می‌توان با طرح رویه قضائی در این رابطه به راحتی پاسخ گفت. در قضیه «بورهیل علیه یونگ[۱]» (۱۹۴۳)، خواهان صدای تصادفی را که در اثر قصور خوانده در موتورسواری حاصل شده بود، شنید اما صحنه تصادف را مشاهده نکرد مدتی بعد خواهان آثار سوء تصادف را مشاهده کرد و دچار شوک عصبی شد. دادگاه با این استدلال که آسیب وارد شده به خواهان قابل پیش بینی نبوده است علیه او رأی داده است. بر مینه ام، ۱۳۸۸ معیار قابلیت پیش بینی هم شخصی و هم نوعی است در اتحادیه اروپا در مسئولیت قراردادی قابلیت پیش بینی ضرر، شرط ضمان قراردادی دانسته شده است و آن را به اصل حاکمیت اراده نیز مستند نموده‌اند و گفته‌اند در قراردادها شرط قابلیت پیش بینی، ضرر بر اراده ضمنی متعاقدین مبتنی است. اما در مسئولیت، مدنی با اینکه عده‌ای خواسته‌اند قابلیت پیش بینی ضرر را، شرط تحقق مسئولیت، بدانند اما نظر مشهور برخلاف آن است لذا در مسئولیت مدنی، جبران ضرر تابع اصل جبران ضرر ناروا است (حیاتی، ۱۳۹۲: ۱۴۸).

احراز تقصیر، در میان مبانی مسئولیت مدنی ناشی از ارتباطات اینترنتی این عنوان می‌تواند شاه بیت مبانی ضرر غیر مستقیم پس از مبنای قابل پیش بینی بودن ضرر در اتحادیه اروپا محسوب گردد. در واقع کامل‌ترین ساختار مسئولیت مبتنی بر تقصیر در این عنوان نمودار گشته و موارد بسیاری از پرونده‌های مسئولیت مدنی را در بردارد (زینس و همکاران، ۱۳۹۰: ۲۹). در قرن نوزدهم دادگاه‌ها در اتحادیه اروپا کردند تا حقوق خطاها را به حقوق خطا تبدیل کنند که یکی از این روش‌ها گسترش و تقویت قلمرو بی احتیاطی یا تقصیر و تبدیل آن به یک اصل کلی برای مسئولیت بود؛ یعنی آنکه ضرری بر شخصی وارد آید و اگر تقصیری در بین نباشد، نمی‌توان شخص را مسئول شناخت. در اتحادیه اروپا اصل واحدی مبنای مسئولیت قرار نگرفته است همان طور که مسئولیت مبتنی بر تقصیر در همه‌ی موارد پذیرفته نشده است مسئولیت بدون تقصیر هم جایگزین آن نشده است. به نظر می‌رسد که در اتحادیه اروپا در موارد غفلت و بی احتیاطی اساس مسئولیت بر تقصیر بنا شده است و در موارد خاص از جمله نگهداری اشیای خطرناک یا اقداماتی که کارشناسی ویژه‌ای نیاز دارد، مسئولیت بدون تقصیر پذیرفته می‌شود غفلت و بی

---

[۱] قضیه «بورهیل علیه یونگ» (Bourhill v. Young, 1943) از دعاوی حقوق انگلستان است که در آن دیوان لردها، مسئولیت مدنی را به دلیل عدم پیش‌بینی‌پذیری آسیب روانی ناشی از حادثه‌ای که خواهان مستقیماً شاهد آن نبوده، رد کرد.

احتیاطی در اتحادیه اروپا به مفهوم خودداری از انجام کاری است که انسانی متعارف و معقول در آن شرایط انجام می‌داد و نیز انجام کاری که انسانی معقول و متعارف در آن شرایط انجام نمی‌داد و تقریباً معادل تقصیر در حقوق نوشته است جز این که شامل تقصیر عمدی نمی‌شود. در دعوای جبران خسارت بر اساس بی احتیاطی تقصیر ابتدا باید ثابت شود خوانده یک تعهدی نسبت به خواهان داشته است که فرد مقصر در خصوص لزوم اعمال مراقبت منطقی، این تکلیف را نقض کرده است (انصاری، ۱۴۰۱: ۱۵۸). در این راستا قاعده‌ای به وجود آمد تحت عنوان اصل مجاورتی که زمانی اعمال می‌شد که یک تعهد به مراقبت وجود داشته باشد به این معنا که اشخاص باید مراقبت منطقی اعمال کنند تا بدین وسیله از فعل یا ترک فعلی که به طور منطقی پیش بینی می‌کنند به دیگران آسیب می‌رساند جلوگیری کنند.

٤- مقایسه تطبیقی مسئولیت مدنی ناشی از نقض داده‌های شخصی در حقوق ایران و اتحادیه اروپا

٤-١- شباهت‌ها و تفاوت‌ها در شناسایی داده‌های شخصی

در تحلیل تطبیقی میان حقوق ایران و اتحادیه اروپا در زمینه شناسایی داده‌های شخصی، اولین گام بررسی مفهومی است که هر نظام حقوقی از داده شخصی ارائه می‌دهد. در مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR)، داده شخصی به‌عنوان هر نوع اطلاعاتی تعریف شده است که به فرد شناسایی‌شده یا قابل‌شناسایی مربوط می‌شود، اعم از نام، شماره ملی، اطلاعات مکانی، داده‌های ژنتیکی و زیستی و حتی داده‌های رفتاری یا فرهنگی. این تعریف دامنه وسیعی را شامل می‌شود که می‌تواند بسیاری از مصادیق اطلاعات را مشمول حمایت قانونی قرار دهد. در مقابل، در نظام حقوقی ایران، به‌ویژه در اسناد پراکنده‌ای مانند قانون جرائم رایانه‌ای و آیین‌نامه‌های مربوط به دولت الکترونیک، تعریفی منسجم، دقیق و یکپارچه از داده شخصی ارائه نشده است. این امر موجب ابهام در شناسایی مصادیق داده‌های مشمول حمایت شده و در موارد عملی، باعث سردرگمی مراجع قضایی و کاربران فضای مجازی شده است (Wong,2018: 43). از نظر تمایزگذاری میان داده‌های عادی و داده‌های حساس نیز، در مقررات GDPR ، داده‌های حساس به‌طور مشخص تعریف شده و شامل اطلاعاتی مانند گرایش جنسی، دیدگاه‌های سیاسی، باورهای مذهبی، عضویت‌های صنفی و اطلاعات مربوط به سلامت و ژنتیک می‌گردند. برای پردازش این نوع اطلاعات، شرایط سخت‌گیرانه‌تری در نظر گرفته شده است. در حقوق ایران، چنین تمایزی به‌صورت صریح وجود ندارد و در نتیجه، حساسیت قانونی پردازش برخی اطلاعات حیاتی به‌درستی در قوانین موضوعه منعکس نشده است. همین امر ممکن است زمینه‌ساز نقض حقوق بنیادین افراد و ورود آسیب‌های جبران‌ناپذیر شود (منصوریان و همکاران، ۱۳۹۵: ۱۷). یکی دیگر از

تفاوت‌های بنیادین، به دامنه شمول قوانین مربوط می‌شود. GDPR صرفاً محدود به کشورهای عضو اتحادیه اروپا نیست، بلکه دامنه اعمال آن بر تمام اشخاص حقیقی یا حقوقی که داده‌های شهروندان اروپایی را پردازش می‌کنند، تسری دارد. این رویکرد فراسرزمینی بر اهمیت داده‌ها به‌عنوان دارایی‌های راهبردی و نیز بر حاکمیت افراد بر اطلاعاتشان تأکید می‌کند. در مقابل، قوانین ایران اغلب ناظر به قلمرو جغرافیایی کشور بوده و فاقد رویکرد فرامرزی در حمایت از داده‌ها هستند، مسئله‌ای که در فضای بدون مرز اینترنت، چالش‌برانگیز می‌نماید.

از حیث اصول حاکم بر حفاظت از داده‌های شخصی، GDPR اصولی مانند شفافیت، تناسب، محدودیت هدف، صحت داده‌ها و امنیت را صریحاً مقرر کرده است. این اصول در طراحی سیستم‌های داده‌محور و نیز در ارزیابی عملکرد مسئولان پردازش، نقش مهمی ایفا می‌کنند. در حقوق ایران، این اصول یا اساساً پیش‌بینی نشده‌اند یا به‌صورت پراکنده و غیرالزام‌آور در اسناد مختلف دیده می‌شوند که به نبود هماهنگی اجرایی منجر شده است. در نتیجه، فرآیندهای پردازش اطلاعات در بسیاری موارد فاقد نظارت و سازوکارهای کنترل کیفیت و مشروعیت هستند (قطبی راوندی، ۱۳۹۹: ۲۱). همچنین، در حوزه رضایت‌مندی و حق تعیین سرنوشت اطلاعات، GDPR نقش فعالی برای صاحبان داده قائل شده است. فرد حق دارد در هر لحظه اطلاعات خود را حذف کند، از پردازش آنها ممانعت ورزد یا درخواست انتقال آنها را به سامانه‌ای دیگر داشته باشد. در ایران، این حقوق یا به‌طور ناقص پیش‌بینی شده‌اند یا در عمل ضمانت اجرایی مؤثری ندارند. این تفاوت در نوع نگاه به مفهوم مالکیت اطلاعات، بیانگر رویکردهای متفاوت دو نظام حقوقی در رابطه با کرامت انسانی و حریم خصوصی است.

٤-۲- نقش نهادهای ناظر و ضمانت‌های اجرایی

در نظام حقوقی اتحادیه اروپا، یکی از ارکان اساسی حمایت از داده‌های شخصی، وجود نهادهای ناظر مستقل و قدرتمند همچون «کمیسیون حفاظت از داده‌ها» در کشورهای عضو و هیئت حفاظت از داده‌های اروپا (EDPB) در سطح کلان است. این نهادها با وظایفی نظیر نظارت بر رعایتGDPR ، رسیدگی به شکایات شهروندان، صدور دستور توقف پردازش داده، و اعمال جریمه‌های مالی سنگین، نقش کلیدی در تضمین اجرای مؤثر مقررات دارند. در مقابل، در ایران چنین نهاد تخصصی مستقلی برای نظارت بر داده‌ها هنوز تشکیل نشده است و مسئولیت نظارت پراکنده میان نهادهایی نظیر پلیس فتا، وزارت ارتباطات و نهادهای قضایی تقسیم شده که فاقد انسجام نهادی و تخصصی لازم هستند (Voigt,2017: 30).

ضمانت‌های اجرایی GDPR ترکیبی از ابزارهای مدنی، کیفری و اداری هستند. از جمله می‌توان به الزام به جبران خسارت، تعلیق عملیات پردازش، جریمه‌های مالی تا سقف بیست میلیون یورو یا چهار

درصد گردش مالی جهانی اشاره کرد. این شدت در ضمانت اجرا به‌منظور ایجاد بازدارندگی و تضمین رعایت کامل اصول حاکم بر پردازش داده‌ها در نظر گرفته شده است. در ایران، ضمانت اجراهای محدود کیفری در قانون جرایم رایانه‌ای پیش‌بینی شده ولی سازوکارهای مدنی برای جبران خسارت یا اعمال ممنوعیت بر شرکت‌های ناقض، یا وجود ندارد یا فاقد کارآمدی لازم است. در نظام اروپایی، شفافیت نهاد ناظر و پاسخ‌گویی آن نسبت به شهروندان، از دیگر ارکان کارآمدی آن محسوب می‌شود. نهاد ناظر مکلف است به گزارش سالانه، گزارش عملکرد شرکت‌ها، و میزان رعایت حقوق داده از سوی مسئولان داده رسیدگی و نتایج آن را منتشر کند. این رویکرد در افزایش اعتماد عمومی بسیار مؤثر بوده است. در نظام ایران، چنین الزامی برای نهادهای درگیر دیده نمی‌شود و نبود شفافیت موجب بی‌اعتمادی عمومی و تداوم نقض داده‌ها شده است (لطیف زاده و همکاران، ۱۴۰۱: ۵۲). افزون بر این، در اروپا، نهاد ناظر دارای استقلال ساختاری و بودجه‌ای از دولت است که امکان دخالت سیاسی در فعالیت‌های آن را به حداقل می‌رساند. این استقلال به نهاد اجازه می‌دهد تا در برابر ناقضان، حتی اگر دولت یا نهادهای عمومی باشند، اقدام مقتضی انجام دهد. اما در ساختار حاکم بر ایران، اکثر نهادهای فعال در این حوزه زیرمجموعه قوه مجریه یا قضاییه بوده و فاقد استقلال عملکرد هستند (انصاری، ۱۴۰۰: ۸۳).

موضوع دیگری که موجب تقویت نهاد ناظر در اتحادیه اروپا شده، امکان تعامل فرامرزی و همکاری بین‌نهادی در سطح بین‌المللی است. نهادهای ناظر کشورهای عضو می‌توانند در قالب سازوکارهای مشترک، به بررسی پرونده‌های چندملیتی پرداخته و از اصول همگرایی در تصمیم‌گیری بهره‌مند شوند. در ایران، نه‌تنها چنین همکاری‌هایی در سطح بین‌المللی وجود ندارد، بلکه فقدان قانون جامع، زمینه تعامل با نظام‌های حقوقی پیشرفته را نیز دشوار کرده است.

٤-۳- چالش‌ها و راهکارهای تطبیقی برای ایران با الهام از تجربه اروپا

اولین چالش ایران در مسیر حمایت از داده‌های شخصی، فقدان قانون جامع و منسجم در این زمینه است. اگرچه تلاش‌هایی در قالب لایحه حمایت از داده‌ها صورت گرفته، اما این لایحه هنوز تصویب نشده و مفاد آن با اصول بین‌المللی مانند GDPR فاصله دارد. تجربه اروپا نشان می‌دهد که تصویب یک قانون جامع و صریح، نقطه شروعی برای تنظیم روابط داده‌محور و تضمین حقوق شهروندی است. پیشنهاد می‌شود که ایران با بهره‌گیری از اصول بنیادین GDPR، چارچوبی متناسب با ساختار اجتماعی، فرهنگی و فناوری داخلی خود طراحی و نهایی سازد (انصاری، ۱۴۰۱: ۶۸).

چالش دوم، نبود نهاد ناظر مستقل با اختیارات قانونی گسترده است. ایجاد چنین نهادی در ایران، می‌تواند بسیاری از خلأهای اجرایی، نظارتی و آموزشی در حوزه داده‌ها را برطرف کند. نهاد مذکور باید دارای شخصیت حقوقی مستقل، بودجه مشخص، و صلاحیت قضایی برای رسیدگی به تخلفات باشد. تجربه

نهادهای ناظر در کشورهای اروپایی نشان می‌دهد که تمرکز اختیارات در یک نهاد مستقل، به افزایش شفافیت، پاسخ‌گویی و کاهش موازی‌کاری کمک شایانی می‌کند.یکی دیگر از چالش‌ها، سطح پایین آگاهی عمومی نسبت به حقوق داده و حریم خصوصی در ایران است. در حالی‌که در اروپا فرهنگ «مالکیت اطلاعات شخصی» تثبیت شده، در ایران بسیاری از افراد نمی‌دانند که چه اطلاعاتی از آنان جمع‌آوری می‌شود و چگونه می‌توانند از حقوق خود دفاع کنند. راهکار این مسئله، آموزش عمومی از طریق رسانه‌ها، نظام آموزشی، و نهادهای مدنی است. همچنین مسئولان پردازش داده باید ملزم به ارائه اطلاع‌رسانی شفاف و دقیق به کاربران شوند (کاتوزیان، ۱۳۹۵: ۴۱). همچنین، ایجاد مکانیزم‌های مؤثر برای جبران خسارت‌های ناشی از نقض داده، ضرورتی اجتناب‌ناپذیر است. نظام حقوقی ایران باید سازوکارهای مشخصی برای طرح دعاوی مدنی علیه ناقضان و الزام آنان به پرداخت غرامت پیش‌بینی کند. استفاده از نهاد داوری، میانجی‌گری، و دادگاه‌های تخصصی داده می‌تواند روند رسیدگی را تسریع و کارآمد کند.

نتیجه

در عصر انفجار اطلاعات و گسترش فراگیر فناوری‌های ارتباطی، داده‌های شخصی انسان‌ها به سرمایه‌ای ارزشمند و گاه آسیب‌پذیر بدل شده‌اند. نگهداری، پردازش و بهره‌برداری از این داده‌ها، چه از سوی دولت‌ها و نهادهای عمومی و چه از سوی شرکت‌ها و اشخاص حقیقی، در بستری رخ می‌دهد که همزمان فرصتی بزرگ برای توسعه و خطری عظیم برای نقض حقوق بشر است. پژوهش حاضر نشان داد که نظام‌های حقوقی مدرن، به‌ویژه اتحادیه اروپا، با تصویب مقرراتی چون GDPR تلاش کرده‌اند تعادلی میان توسعه فناوری و حفظ حریم خصوصی برقرار سازند. این در حالی است که حقوق ایران با وجود پیشینه فقهی غنی در حمایت از حیثیت و کرامت انسان، هنوز در تدوین مقررات جامع و به‌روز در زمینه داده‌های شخصی با خلأ جدی مواجه است. تحلیل مبانی، عناصر و مصادیق مسئولیت مدنی ناشی از نقض داده‌ها نشان می‌دهد که به‌منظور حفظ کرامت انسانی در فضای مجازی، بازنگری اساسی در قواعد سنتی مسئولیت مدنی ضروری است. از بررسی تطبیقی میان ایران و اتحادیه اروپا می‌توان دریافت که گرچه هر دو نظام حقوقی، اصل مسئولیت مدنی در برابر نقض داده‌های شخصی را پذیرفته‌اند، اما در نحوه‌ی شناسایی داده‌های حساس، تعیین اشخاص مسئول، و تدوین سازوکارهای جبران خسارت تفاوت‌های بنیادینی مشاهده می‌شود. مقررات GDPR علاوه بر ارائه‌ی تعریف دقیق از داده‌های شخصی و حساس، مسئولیت مدنی را نه‌فقط بر مبنای تقصیر بلکه در مواردی بر اساس فرض تقصیر و خطر نیز تنظیم کرده است. در حالی که در حقوق ایران، همچنان عنصر تقصیر نقش اساسی را ایفا می‌کند و بار اثبات آن نیز بر دوش زیان‌دیده باقی می‌ماند، امری که با توجه به ماهیت فنی و پیچیده داده‌های دیجیتال، اثبات آن را بسیار دشوار می‌سازد. این تفاوت، نشان‌دهنده ضرورت اصلاح قوانین ایران در راستای پذیرش الگوهای منعطف‌تر و حمایتی‌تر است. از دیگر

یافته‌های مهم پژوهش، فقدان نهاد ناظر مستقل و تخصصی در ایران برای نظارت بر پردازش داده‌ها و رسیدگی به نقض‌های احتمالی است. در اتحادیه اروپا، هر کشور عضو موظف به تشکیل یک مرجع مستقل حفاظت از داده‌هاست که علاوه بر نظارت مستمر، به شکایات شهروندان نیز رسیدگی می‌کند و دارای اختیارات گسترده‌ای برای صدور جریمه، دستور توقف پردازش، و اعمال دیگر ضمانت‌های اجرایی است. در مقابل، نظام حقوقی ایران نه‌تنها فاقد چنین نهادی است، بلکه نظارت بر داده‌ها میان نهادهای متعددی پراکنده شده که غالباً فاقد تخصص لازم در این حوزه هستند. پیشنهاد تشکیل یک نهاد ملی مستقل و فراگیر، با قابلیت همکاری بین‌المللی و برخوردار از اختیارات قضایی و اداری، می‌تواند گامی اساسی در جهت ارتقاء حمایت از داده‌های شخصی در ایران باشد. پژوهش همچنین نشان داد که داده‌های شخصی باید به‌مثابه بخشی از حقوق شخصیت و کرامت انسانی تلقی شوند، نه صرفاً دارایی‌هایی فاقد شأن ذاتی. در این چارچوب، نقض داده‌ها، نه‌فقط آسیب مالی، بلکه تعرضی به حریم خصوصی، استقلال فردی و حتی امنیت روانی اشخاص محسوب می‌شود. با چنین نگاهی، پذیرش خسارات معنوی به‌عنوان بخشی از ضرر قابل جبران در مسئولیت مدنی، اجتناب‌ناپذیر است. این در حالی است که نظام حقوقی ایران هنوز در پذیرش و ارزیابی خسارات معنوی ناشی از نقض داده‌ها، با چالش‌های نظری و عملی جدی مواجه است. استفاده از نظریه‌های نوین چون «مالکیت فکری بر داده‌ها» یا «انصاف جبرانی»، می‌تواند به غنای مبانی مسئولیت مدنی در این حوزه یاری رساند.

افزون بر آن، چالش نظری «نقض حریم خصوصی داده‌ها» که در برخی محافل غربی مطرح شده، در این پژوهش مورد نقد قرار گرفت. این نظریه که با تکیه بر گسترش فناوری‌های پایش و تحلیل داده، تضعیف حریم خصوصی را امری اجتناب‌ناپذیر می‌داند، عملاً مشروعیت مطالبه خسارت را زیر سؤال می‌برد. اما یافته‌های این تحقیق بر آن است که حتی در عصر داده‌های باز و الگوریتم‌های نظارت‌گر، همچنان باید از اصول بنیادین حریم خصوصی و کرامت انسانی دفاع کرد. اتفاقاً، هرچه دسترسی به داده‌ها آسان‌تر و خطر نقض بیشتر شود، ضرورت حمایت حقوقی قوی‌تر و پاسخ‌گویی سریع‌تر بیشتر احساس می‌شود. پذیرش این اصل، می‌تواند مبنای توسعه قواعد مدرن مسئولیت مدنی در حقوق ایران قرار گیرد.

در مجموع، مقاله حاضر با بررسی مبانی، عناصر و نهادهای مرتبط با مسئولیت مدنی ناشی از نقض داده‌های شخصی در دو نظام حقوقی ایران و اتحادیه اروپا، بر ضرورت تدوین قانون جامع حمایت از داده‌ها در ایران تأکید دارد. این قانون باید نه فقط از حیث مفهومی و ساختاری با مقررات پیشرفته‌ای مانند GDPR هماهنگ باشد، بلکه در ابعاد اجرایی نیز پاسخ‌گوی نیازهای شهروندان، فضای فناوری، و ملاحظات حقوق بشر باشد. پیشنهادهای پژوهش شامل: ایجاد نهاد ناظر مستقل، بازنگری در بار اثبات، پیش‌بینی خسارات معنوی، پذیرش مسئولیت غیرتقصیری در موارد خاص و آموزش عمومی حقوق داده‌هاست. بدون شک، تحقق این اهداف نیازمند اراده سیاسی، همگرایی نهادهای قانون‌گذاری، و همراهی جامعه حقوقی کشور است.

منابع

- انصاری، باقر. (۱۳۸۶). حقوق حریم خصوصی. تهران: سمت.
- انصاری، باقر. (۱۴۰۰). حقوق داده‌ها و هوش مصنوعی. تهران: سمت.
- انصاری، باقر. (۱۴۰۱). مطالعه تطبیقی حمایت از داده‌های شخصی در اروپا، آمریکا، چین و ایران. تهران: شرکت سهامی انتشار.
- انصاری، مسعود، و طاهری، محمدعلی. (۱۳۸۸). دانشنامه حقوق خصوصی (جلد ۲، چاپ ۳). تهران: جنگل.
- آشوری، محمد. (۱۳۸۲). آئین دادرسی کیفری (جلد ۲، چاپ ۳). تهران: سمت.
- بجنوردی، سید محمد حسن. (۱۳۷۹). قواعد فقه (چاپ ۳). تهران: نشر عروج.
- بیات کمیتکی، مهناز و بالوی، مهدی. (۱۳۹۶). روش حل تعارض حقوق فردی و منافع جمعی در رویه قضایی دادگاه اروپایی حقوق بشر. فصلنامه تحقیقات حقوقی، ۲۰، ۳۴۴-۳۱۹.
- حیدری، علی مراد، و جعفری، علی. (۱۳۹۸). جرائم علیه داده پیام‌های شخصی در تجارت الکترونیکی. پژوهشنامه حقوق کیفری، ۱۱(۱)، ۷۴-۱۰۵.
- زینس، چیام و محمدحسین. (۱۳۹۰). معنای سه مفهوم پرکاربرد داده، اطلاع و دانش. کتابداری و اطلاع‌رسانی، ۱۴(۲)، ۹-۵.
- ژوردن، پاتریس. (۱۳۸۵). اصول مسئولیت مدنی (مجید ادیب، مترجم) (چاپ ۲). تهران: میزان.
- شهیدی، مهدی. (۱۳۸۲). آثار قراردادها و تعهدات (چاپ ۱). تهران: مجمع علمی و فرهنگی مجد.
- عوده، عبدالقادر. (۱۳۸۹). بررسی تطبیقی حقوق جزای اسلامی و قوانین عرفی (حسن فرهودی‌نیا، مترجم) (جلد ۳، چاپ ۱). تهران: یادآوران.
- غمامی، مجید. (۱۳۸۳). قابلیت پیش‌بینی ضرر در مسئولیت مدنی (چاپ ۱). تهران: شرکت سهامی انتشار.
- قاسم‌زاده، سید مرتضی. (۱۳۸۷). مبانی مسئولیت مدنی (چاپ ۵). تهران: میزان.
- قطبی راوندی، مریم، ابراهیمی، معصومه‌السادات و بنی‌اسدی، مریم. (۱۳۹۹). تحلیل اینترنت اشیاء و کلان‌داده‌ها. در دهمین کنگره سراسری فناوری‌های نوین در حوزه توسعه پایدار، تهران.

- قناد، فاطمه و شریف، الهام. (۱۴۰۰). مطالعه‌ای اجمالی بر حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌های اتحادیه اروپا. حقوق فناوری‌های نوین، ۱-۲۲.
- قناد، فاطمه، و علیقلی، امیره. (۱۳۹۹). مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی. حقوق فناوری‌های نوین، ۲۹۷-۳۲۲.
- قهرمانی، نصرالله. (۱۳۷۷). مسئولیت مدنی وکیل دادگستری (چاپ ۱). تهران: گندم.
- کاتوزیان، ناصر. (۱۳۸۲). وقایع حقوقی (چاپ ۱). تهران: یلدا.
- کاتوزیان، ناصر. (۱۳۹۵). قواعد عمومی قراردادها. تهران: شرکت سهامی انتشار.
- لطیف‌زاده، مهدیه، قبولی درافشان، سید محمدمهدی، محسنی، سعید و عابدی، محمد. (۱۴۰۰). تحلیل بستر قانونی حمایت از داده شخصی در اتحادیه اروپا. پژوهشنامه پردازش و مدیریت اطلاعات، ۴۷۲-۴۳۹.
- لطیف‌زاده، مهدیه، قبولی‌درافشان، سید محمد مهدی، محسنی، سعید، و عابدی، محمد. (۱۴۰۱). تبیین اسباب مشروعیت پردازش داده‌ی شخصی از منظر حقوق اتحادیه اروپا و ایران. مطالعات حقوقی (علوم اجتماعی و انسانی شیراز)، ۱۴(۳)، ۳۲۵-۳۶۴.
- لطیف‌زاده، مهدیه، و قبولی‌درافشان، سید محمد مهدی. (۱۴۰۱). چگونگی انتقال بین‌المللی داده‌های شخصی (مطالعه تطبیقی در حقوق اتحادیه اروپا و نظام حقوقی ایران). پژوهشنامه حقوق تطبیقی، ۶(۱)، ۲۰۷-۲۳۰.
- محقق داماد، سید مصطفی. (۱۳۹۳). حقوق قراردادها در فقه امامیه: توافق اراده‌ها، شرایط متعاقدین و مورد معامله (جلد دوم). تهران: سمت.
- محمدی‌کردخیلی، حمید، صفوی، مجید، غلامعلی‌زاده، محمد، و اسمعیلی، حمیدرضا. (۱۴۰۱). مبانی مسئولیت مدنی ناشی از ارتباطات اینترنتی در حقوق ایران و اتحادیه اروپا. تحقیقات حقوقی بین‌المللی، ۱۵(۵۵)، ۴۵۱-۴۶۹.
- منصوریان، ناصرعلی و شیبانی، عادل. (۱۳۹۵). مفهوم منفعت عمومی و جایگاه آن در قانون‌گذاری ایران. دیدگاه‌های حقوق قضایی، ۲۱(۷۵ و ۷۶)، ۱۴۲-۱۱۷.

- Breen, S., Ouazzane, K., & Patel, P. (2020). GDPR: Is your consent valid? Business Information Review, 37(1), 19–24.
- Colcelli, V. (2019). Joint controller agreement under GDPR. EU and Comparative Law Issues and Challenges Series (ECLIC), (3), 1030–1047.
- Goddard, M. (2017). Viewpoint: The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, 59(6), 703–706.
- Misek,Jakub (2018). "Is the Definition of Personal Data Flawed? Hyperlink as Personal Data (Processing)", in: Svantesson, Dan Jerker & Kloza, Dariusz. (Eds.), Trans-Atlantic Data Privacy Relations as a Challenge for Democracy, Cambridge University Press.
- OECD (2010). Data Privacy Law-An International Perspective, Oxford, University Press.
- Schwartz, Paul (2019). "Global Data Privacy: The EU Way", New York University Law Review, 94(4), pp. 772-818.
- Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer International Publishing.
- Wong, Nadezhda (2018). "The law of everything. Broad concept of personal data and future of EU data protection law", Law, Innovation and Technology, 10(1), pp. 40-81.

Civil Liability Arising from Personal Data Breaches: A Comparative Study of Iranian Law and European Union Law

Abstract

Data privacy constitutes one of the foundational concepts in contemporary legal systems, gaining increasing significance with the expansion of information and communication technologies. This study explores civil liability arising from the violation of data privacy and provides an analytical examination of its three essential elements: harm, fault, and causation.

A major challenge in this area is the theory of "data privacy violation," proposed by certain Western legal scholars, which asserts that in the age of pervasive data monitoring and processing technologies, no reasonable expectation of privacy remains. This theory not only undermines the foundations of civil liability but also restricts the scope for claiming damages. In this paper, the aforementioned theory is critically evaluated, and the need for effective legal protection of victims is emphasized. The study further examines the non-material (moral) damages resulting from data privacy breaches, particularly due to their impact on personality rights. Finally, the possibility of classifying data privacy as a property right—drawing upon intellectual property theory—is analyzed.

The findings of the research indicate that while modern technologies may increase the risk of privacy violations, this should not lead to the erosion of legal protections for individuals. Rather, it underscores the necessity of strengthening compensation mechanisms and evolving civil liability frameworks to ensure a fair balance between public interests and individual rights.

Keyword: Civil Liability, Data Privacy, Harm, Privacy Violation Theory, Personality Rights