فصلنامه مطالعات کاربردی در علوم اجتماعی و جامعه‌شناسی
سال هشتم، شماره ۴ (پیاپی: ۳۶)، ویژه نامه پاییز ۱۴۰۴

حمایت از داده‌های شخصی به‌عنوان حق مالی جدید در حقوق خصوصی ایران

عبدالمومن علی پور[۱]

تاریخ دریافت: ۱۴۰۴/۰۶/۲۹
تاریخ پذیرش: ۱۴۰۴/۰۷/۳۰
کد مقاله: ۵۳۴۶۱

چکـیده

ورود شتابان فناوری هوش مصنوعی به حوزه‌های مختلف اقتصادی، اجتماعی و پزشکی، تحولات بنیادینی در روابط حقوقی و نظام مسئولیت مدنی ایجاد کرده است. در حقوق ایران، مسئولیت مدنی عمدتاً بر اساس سه رکن تقصیر، رابطه سببیت و ضرر طراحی شده است که این چارچوب سنتی در مواجهه با سامانه‌های خودآموز و تصمیم‌گیر مستقل ناکارآمد به نظر می‌رسد. هوش مصنوعی با ویژگی‌های منحصر به فردی مانند یادگیری مستمر، تصمیم‌گیری مستقل، رفتار غیرقابل پیش‌بینی و دخالت چندین عامل انسانی و ماشینی، چالش‌های جدی در اثبات تقصیر، رابطه سببیت و تعیین میزان ضرر ایجاد کرده است. این وضعیت باعث شده که نظام حقوقی ایران نتواند به شکل کامل و منصفانه خسارات ناشی از خطاهای هوش مصنوعی را جبران کند و نیاز به بازاندیشی و توسعه مکانیسم‌های حقوقی نوین احساس شود. با بررسی تطبیقی تجربیات بین‌المللی و ظرفیت‌های فقهی و حقوقی ایران، این پژوهش نشان می‌دهد که ترکیبی از اصلاح قوانین سنتی، ایجاد رژیم‌های مسئولیت ویژه، پذیرش مسئولیت محض در موارد پرخطر، توسعه مقررات بیمه‌ای و شفافیت الگوریتمی می‌تواند پاسخگوی نیازهای حقوقی ناشی از هوش مصنوعی باشد. چنین رویکردی هم حفاظت از حقوق زیان‌دیدگان را تضمین می‌کند و هم از توسعه مسئولانه فناوری‌های نوین حمایت می‌نماید. در نتیجه، بازنگری در اصول مسئولیت مدنی و ایجاد چارچوب قانونی نوین، پیش‌شرط همسوسازی حقوق ایران با تحولات جهانی و تضمین عدالت در مواجهه با فناوری‌های هوشمند است.

واژگـان کلـیدی: هوش مصنوعی، مسئولیت مدنی، تقصیر، رابطه سببیت، حقوق ایران

۱ – عنوان نویسنده

۱- مقدمه

تحولات فناوری هوش مصنوعی در دهه‌های اخیر، بسیاری از حوزه‌های اقتصادی، اجتماعی و پزشکی را متحول ساخته است و پیامدهای گسترده‌ای در نظام حقوقی ایجاد کرده است. این فناوری‌ها با ویژگی‌هایی مانند تصمیم‌گیری خودکار، یادگیری مستمر و توانایی تحلیل داده‌های عظیم، نقش مؤثری در بهبود کارایی و کاهش خطاهای انسانی دارند (کریمی، ۱۴۰۰). با این حال، ورود سامانه‌های هوشمند به عرصه‌های پیچیده زندگی روزمره، چالش‌های تازه‌ای را در حوزه مسئولیت مدنی ایجاد کرده است، زیرا اصول سنتی مسئولیت مدنی ایران بر مبنای رفتار انسانی و پیش‌بینی‌پذیری طراحی شده‌اند (کاتوزیان، ۱۳۹۱، ص. ۱۰۳). در نظام حقوقی ایران، مسئولیت مدنی عمدتاً بر پایه سه رکن اساسی تقصیر، رابطه سببیت و ضرر شکل گرفته است (صفایی، ۱۳۹۶). این ارکان به شکل سنتی قادر به پوشش خسارات ناشی از اقدامات انسانی هستند و در شرایط کلاسیک پاسخگو هستند، اما با ورود هوش مصنوعی، تحلیل تقصیر و رابطه علیت با دشواری مواجه شده است. سامانه‌های خودآموز می‌توانند بدون دخالت مستقیم انسان تصمیم‌گیری کنند و در نتیجه، انتساب تقصیر یا تعیین علت اصلی خسارت به شکل سنتی دشوار می‌شود (احمدی، ۱۴۰۰، ص. ۷۵). یکی از مهم‌ترین چالش‌ها در مواجهه با هوش مصنوعی، اثبات تقصیر انسانی است. در سامانه‌های پزشکی هوشمند یا خودروهای خودران، خطا ممکن است ناشی از نقص الگوریتم، داده‌های ناقص یا تعامل بین چند عامل انسانی و ماشینی باشد و هیچ شخص مشخصی مستقیماً مسئول شناخته نشود. این وضعیت، فرآیند دادرسی و جبران خسارت را پیچیده و زمان‌بر می‌کند و ضرورت بازاندیشی در نظام حقوقی ایران را نمایان می‌سازد (کریمی، ۱۴۰۰، ص. ۹۱).

رکن دوم مسئولیت مدنی، یعنی رابطه سببیت، نیز با ورود هوش مصنوعی با مشکل مواجه شده است. سامانه‌های هوشمند معمولاً تحت تأثیر عوامل متعدد عمل می‌کنند و تعیین علت اصلی خسارت دشوار است. بر اساس تحلیل حقوقی ایران، بدون اثبات رابطه علیت بین فعل زیان‌آفرین و ضرر، مسئولیت محقق نمی‌شود و این امر، پرونده‌های قضایی پیچیده فناوری را با بن‌بست مواجه می‌سازد (صفایی، ۱۳۹۶، ص. ۲۱۲). ضرر، سومین رکن مسئولیت مدنی، در محیط‌های هوش مصنوعی نیز چالش‌برانگیز است. سامانه‌های پیچیده می‌توانند ضررهای اقتصادی، معنوی یا اطلاعاتی ایجاد کنند که اندازه‌گیری و اثبات آن‌ها با قواعد سنتی دشوار است. نمونه بارز آن، سیستم‌های تشخیص پزشکی هوشمند هستند که خطاهای تشخیصی می‌توانند همزمان منجر به آسیب جسمی و روانی شوند و نظام سنتی قادر به ارزیابی دقیق و جبران چنین ضررهایی نیست (محسن‌نژاد، ۱۳۹۴، ص. ۱۴۷). با توجه به این محدودیت‌ها، برخی پژوهشگران پیشنهاد داده‌اند که برای سامانه‌های هوشمند، رژیم مسئولیت ویژه یا مسئولیت محض در نظر گرفته شود تا زیان‌دیدگان بدون اثبات تقصیر یا رابطه سببیت دقیق، امکان مطالبه خسارت داشته باشند. این رویکرد با اصول فقهی همچون قاعده «من أتلف مال الغیر فهو له ضامن» و قاعده «لاضرر» همخوانی دارد و می‌تواند تعادل میان توسعه فناوری و حمایت از حقوق افراد را حفظ کند (محسن‌نژاد، ۱۳۹۴، ص. ۱۴۹). از دیگر مسائل مهم، پیش‌بینی‌ناپذیری رفتار سامانه‌های هوش مصنوعی است. سیستم‌های یادگیری ماشین قادرند با تغییر محیط و داده‌ها، رفتار متفاوتی از خود نشان دهند و الگوریتم‌ها به‌طور خودکار اصلاح شوند. این ویژگی، تحلیل علیت و تقصیر را پیچیده‌تر می‌کند و نشان می‌دهد که قواعد سنتی مسئولیت مدنی برای پاسخگویی به این نوع فناوری‌ها کافی نیستند (قنبری، ۱۳۹۹، ص. ۲۸). تجربه حقوق تطبیقی نشان می‌دهد که بسیاری از کشورها برای مقابله با این چالش‌ها، رژیم مسئولیت ویژه هوش مصنوعی ایجاد کرده‌اند. در این چارچوب، جبران خسارت بدون نیاز به اثبات تقصیر یا رابطه سببیت انجام می‌شود و با مقررات بیمه‌ای و ضمانت اجرایی همراه است. ایران می‌تواند با الهام از این تجربه، چارچوب قانونی منطبق با فناوری‌های نوین طراحی کند و حقوق زیان‌دیدگان را تضمین نماید (قنبری، ۱۳۹۹، ص. ۳۵).

ظرفیت‌های فقهی و اسلامی نیز می‌تواند در اصلاح نظام مسئولیت مدنی نقش مؤثری ایفا کند. اصولی مانند «لاضرر» و «من أتلف مال الغیر فهو له ضامن» می‌توانند پایه‌ای برای انتساب مسئولیت حتی در شرایط پیچیده فناوری فراهم کنند. با بازاندیشی و اجتهاد نوین، این اصول قابلیت تطبیق با سامانه‌های خودآموز و تصمیم‌گیر مستقل را دارند و می‌توانند چارچوبی حقوقی برای نوآوری مسئولانه ارائه دهند (محسن‌نژاد، ۱۳۹۴، ص. ۱۴۹). در نهایت، بررسی تعارض میان اصول سنتی مسئولیت مدنی و ویژگی‌های هوش مصنوعی نشان می‌دهد که نظام حقوقی ایران برای پاسخگویی به خسارات ناشی از فناوری‌های نوین، نیازمند اصلاحات و بازنگری گسترده است. ترکیبی از اصلاح قوانین سنتی، تدوین مقررات ویژه، ایجاد مکانیسم‌های بیمه‌ای، شفافیت الگوریتمی و بهره‌گیری از ظرفیت‌های فقهی می‌تواند بهترین رویکرد برای همسوسازی حقوق ایران با تحولات جهانی باشد (کریمی، ۱۴۰۰، ص. ۹۷).با توجه به موارد فوق، هدف پژوهش حاضر آن است که ضمن تحلیل تعارض هوش مصنوعی با اصول مسئولیت مدنی ایران، راهکارهایی جامع برای بازنگری و اصلاح نظام حقوقی ارائه دهد. این اقدام، علاوه بر حفاظت از حقوق زیان‌دیدگان، زمینه را برای توسعه مسئولانه فناوری‌های نوین فراهم می‌سازد و امکان بهره‌برداری ایمن و قانونی از سامانه‌های هوشمند را تضمین می‌کند (احمدی، ۱۴۰۰، ص. ۸۲).

۲-مفهوم و ماهیت داده های شخصی

داده‌های شخصی به اطلاعاتی اطلاق می‌شوند که به طور مستقیم یا غیرمستقیم هویت یک فرد را شناسایی یا قابل شناسایی می‌کنند. این داده‌ها شامل نام، شماره ملی، تاریخ تولد، اطلاعات تماس، سوابق پزشکی، داده‌های مالی و حتی رفتارهای آنلاین کاربران می‌شوند (قنبری، ۱۳۹۹، ص. ۲۲). ماهیت داده‌های شخصی دو جنبه مهم دارد: نخست، ارتباط آن با حریم خصوصی و حقوق فردی، و دوم، ارزش اقتصادی بالقوه‌ای که می‌تواند در بازار اطلاعات و خدمات دیجیتال داشته باشد. از منظر حقوقی، داده‌های شخصی نه تنها جنبه حفاظتی و امنیتی دارند، بلکه می‌توان آن‌ها را به عنوان دارایی یا حق مالی نیز در نظر گرفت. این دیدگاه مبتنی بر این است که داده‌های شخصی قابلیت انتفاع اقتصادی دارند و مالکیت آن‌ها می‌تواند به شکل قراردادی یا قانونی منتقل شود (کریمی، ۱۴۰۰، ص. ۸۸). ویژگی بارز داده‌های شخصی، غیرملموس بودن و قابلیت تکثیر آسان آن‌هاست، به طوری که یک داده می‌تواند بدون تخریب داده اصلی، چندین بار استفاده یا معامله شود. این خصوصیت موجب می‌شود ارزش اقتصادی داده‌ها متفاوت از دارایی‌های سنتی ارزیابی شود. همچنین، داده‌های شخصی دارای ماهیت چندلایه هستند. علاوه بر ارزش مالی، داده‌ها حامل اطلاعات حساس و محرمانه نیز می‌باشند که حفاظت از آن‌ها مستلزم رعایت اصول اخلاقی و قانونی است. از این رو، داده‌های شخصی به‌طور همزمان جنبه حقوقی، اقتصادی و اخلاقی دارند و بنابراین تحلیل ماهیت آن‌ها در چارچوب حقوق خصوصی نیازمند توجه به تمامی این ابعاد است. در نهایت، شناسایی داده‌های شخصی به عنوان دارایی یا حق مالی می‌تواند زمینه‌ساز توسعه نظام حقوقی نوین در ایران باشد که هم از حقوق فردی حمایت می‌کند و هم امکان بهره‌برداری اقتصادی مسئولانه از اطلاعات را فراهم می‌سازد (محسن‌نژاد، ۱۳۹۴، ص. ۱۴۴).

۳-حقوق افراد بر داده‌های شخصی در حقوق ایران

حقوق داده‌های شخصی از جمله حقوق نوظهور در عصر دیجیتال به شمار می‌آید و هدف اصلی آن حفاظت از حریم خصوصی و اطلاعات شخصی افراد است. داده‌های شخصی شامل اطلاعات شناسایی مستقیم یا غیرمستقیم مانند نام، شماره ملی، سوابق پزشکی، مالی و رفتارهای آنلاین افراد می‌شود (قنبری، ۱۳۹۹: ۲۲). در حقوق ایران، با افزایش استفاده از فناوری‌های نوین، نیاز به شناسایی و حمایت از این داده‌ها روز به روز ملموس‌تر شده و مسئولیت نهادها و اشخاص در قبال حفاظت از اطلاعات شخصی اهمیت ویژه‌ای یافته است. قانون تجارت الکترونیک ایران (مصوب ۱۳۸۲) از جمله قوانین اساسی است که به نحوی به حفاظت از اطلاعات شخصی پرداخته است. این قانون استفاده از داده‌ها را محدود به اهداف قانونی و مشروع دانسته و بر لزوم رضایت فرد برای جمع‌آوری و پردازش اطلاعات تأکید می‌کند (کریمی, ۱۴۰۰: ۸۸). همچنین، قوانین مربوط به جرایم رایانه‌ای، مجازات‌های مرتبط با افشای غیرمجاز داده‌ها و دسترسی غیرمجاز به اطلاعات شخصی را مشخص کرده‌اند، هرچند در برخی موارد خلا قانونی برای موارد جدید فناوری هوش مصنوعی و سیستم‌های خودآموز دیده می‌شود (صفایی, ۱۳۹۶: ۱۰۶). حق اطلاع‌رسانی و شفافیت یکی از ارکان اصلی حقوق داده‌های شخصی است. افراد باید از نوع داده‌های جمع‌آوری‌شده، اهداف استفاده و مدت نگهداری آن‌ها مطلع شوند. این حق، زمینه اعتماد کاربران به سامانه‌های دیجیتال و ایجاد امنیت روانی در استفاده از خدمات آنلاین را فراهم می‌کند (احمدی, ۱۴۰۰: ۷۵). در ایران، رویه قضایی و مقررات قانونی موجود هنوز به طور کامل نحوه تحقق این حق را مشخص نکرده‌اند و اغلب به تفسیرهای محدود بسنده شده است.

حق دسترسی و اصلاح داده‌ها نیز اهمیت بالایی دارد. کاربران باید بتوانند به داده‌های شخصی خود دسترسی داشته باشند و در صورت خطا یا ناقص بودن اطلاعات، امکان اصلاح یا حذف آن‌ها فراهم شود. این حق، هم با اصول فقهی مانند «لاضرر» و هم با استانداردهای بین‌المللی مطابقت دارد و به عنوان یکی از محورهای اصلاح قوانین داده‌های شخصی در ایران پیشنهاد شده است (محسن‌نژاد, ۱۳۹۴: ۴۴). بحث مالکیت داده‌های شخصی و امکان انتساب ارزش مالی به آن‌ها از موضوعات نوظهور در حقوق خصوصی ایران است. با توجه به اینکه داده‌ها قابلیت بهره‌برداری اقتصادی دارند، شناسایی آن‌ها به عنوان دارایی یا حق مالی می‌تواند امکان انتقال و معامله قانونی را فراهم کند (کریمی, ۱۴۰۰: ۱۴۰). این امر می‌تواند بستری برای ایجاد حقوق مالی و قراردادی جدید بر داده‌های شخصی در نظام حقوقی ایران فراهم آورد. مسئولیت نهادها و اشخاص در برابر نقض حقوق داده‌های شخصی نیز از دیگر ابعاد مهم است. قوانین ایران مسئولیت استفاده‌کنندگان و پردازش‌کنندگان داده‌ها را در صورت افشای غیرمجاز یا سوءاستفاده مشخص کرده‌اند، اما تعیین میزان مسئولیت و سازوکار جبران خسارت در موارد پیچیده فناوری هنوز ناقص است (قنبری, ۱۳۹۹: ۱۴).این خلأ قانونی، ضرورت بازنگری و ایجاد مقررات اختصاصی برای داده‌های شخصی را روشن می‌کند. استفاده از قراردادها و توافقنامه‌ها به عنوان ابزاری برای حمایت از داده‌های شخصی، یکی دیگر از راهکارهای عملی است. نهادهای خصوصی و شرکت‌های فناوری می‌توانند با قراردادن شروط مشخص در قراردادهای خدمات، حقوق کاربران را تضمین کرده و از افشای غیرمجاز داده‌ها جلوگیری نمایند (یوسفی, ۱۳۹۸: ۶۵) این ابزار می‌تواند در کوتاه‌مدت خلأهای قانونی موجود را تا زمان اصلاح قوانین پر کند. در نهایت، ترکیبی از اصلاح قوانین موجود، تدوین مقررات اختصاصی، بهره‌گیری از ظرفیت‌های فقهی و

استفاده از سازوکارهای قراردادی و بیمه‌ای می‌تواند حقوق افراد بر داده‌های شخصی را در ایران به‌طور جامع تضمین نماید. چنین چارچوبی هم حفاظت از حریم خصوصی را تقویت می‌کند و هم امکان بهره‌برداری مشروع و اقتصادی از داده‌ها را فراهم می‌سازد (محسن‌نژاد, ۱۳۹۴: ۱۴۷). این رویکرد، پیش‌نیاز توسعه نظام حقوقی نوین در زمینه داده‌های شخصی و تطبیق با استانداردهای بین‌المللی است.

۴-داده‌های شخصی به‌عنوان حق مالی در حقوق خصوصی ایران

با پیشرفت فناوری‌های اطلاعاتی و دیجیتال، داده‌های شخصی نه تنها از منظر حفاظت از حریم خصوصی اهمیت یافته‌اند، بلکه از جنبه اقتصادی و مالی نیز ارزش قابل توجهی پیدا کرده‌اند. داده‌های شخصی شامل اطلاعات شناسایی مستقیم و غیرمستقیم افراد است که می‌تواند شامل مشخصات هویتی، سوابق پزشکی و مالی، رفتارهای آنلاین و الگوهای مصرف باشد (قنبری، ۱۳۹۹: ۲۲). این اطلاعات با توجه به قابلیت پردازش و تحلیل داده‌ها، قابلیت تبدیل شدن به دارایی با ارزش اقتصادی را دارند و در نتیجه می‌توان آن‌ها را به عنوان حق مالی در حقوق خصوصی مورد توجه قرار داد. در حقوق ایران، مالکیت و انتفاع از دارایی‌ها معمولاً به اموال مادی محدود می‌شود، اما داده‌های شخصی با توجه به قابلیت بهره‌برداری اقتصادی و انتقال حقوقی، می‌توانند در قالب حقوق مالی و دارایی معنوی تعریف شوند (کریمی، ۱۴۰۰: ۸۹). به عنوان مثال، شرکت‌ها می‌توانند با کسب مجوز قانونی، داده‌های شخصی را جمع‌آوری، تحلیل و برای ارائه خدمات یا اهداف تجاری به کار گیرند. در این چارچوب، داده‌های شخصی به شکل دارایی قابل معامله، اجاره یا انتقال حقوقی درآمده و مشمول حمایت حقوقی می‌شوند. ویژگی مهم داده‌های شخصی که آن را به دارایی با ارزش تبدیل می‌کند، قابلیت تکثیر و استفاده همزمان بدون تخریب اصل داده است. این خصوصیت موجب می‌شود ارزش مالی داده‌ها متفاوت از دارایی‌های سنتی و ملموس ارزیابی شود و نیاز به ایجاد سازوکارهای قانونی خاص برای حفاظت از این حقوق احساس شود (محسن‌نژاد، ۱۳۹۴: ۱۴۴). بنابراین، شناسایی داده‌های شخصی به عنوان حق مالی، علاوه بر حفاظت از مالکیت فردی، امکان بهره‌برداری اقتصادی مشروع را فراهم می‌آورد و زمینه توسعه کسب‌وکارهای نوین دیجیتال را تقویت می‌کند. از منظر حقوق خصوصی، داده‌های شخصی به عنوان حق مالی دارای ابعاد مختلفی است: نخست، حق مالکیت اطلاعات، یعنی توانایی استفاده، بهره‌برداری و انتقال داده‌ها؛ دوم، حق انتفاع اقتصادی، که اجازه می‌دهد مالک داده از داده‌های خود به‌طور مستقیم یا از طریق قرارداد سود کسب کند؛ و سوم، حق کنترل و مدیریت دسترسی، که امکان تعیین نحوه استفاده دیگران از داده‌ها را فراهم می‌کند (صفایی، ۱۳۹۶: ۲۱۰).این ترکیب حقوقی، چارچوبی جامع برای تعریف داده‌های شخصی به عنوان دارایی مالی فراهم می‌آورد.

چالش اصلی در شناسایی داده‌های شخصی به عنوان حق مالی در ایران، نبود مقررات اختصاصی و تعریف قانونی دقیق است. قوانین موجود مانند قانون تجارت الکترونیک و قانون جرایم رایانه‌ای تنها به حفاظت از داده‌ها به عنوان اطلاعات شخصی پرداخته‌اند و به صراحت به ارزش اقتصادی و حقوق مالی آن‌ها اشاره نکرده‌اند (قنبری، ۱۳۹۹ .(p. 34 ,این خلا قانونی باعث شده که در عمل، مالکیت مالی بر داده‌ها و امکان بهره‌برداری اقتصادی محدود شود و نیازمند بازنگری و تدوین مقررات ویژه باشد. استفاده از سازوکارهای قراردادی و بیمه‌ای می‌تواند تا حدی این خلا را جبران کند. به عنوان مثال، شرکت‌ها می‌توانند در قراردادهای خدمات دیجیتال، حقوق مالی کاربران بر داده‌های شخصی را شفاف مشخص کنند و شرایط بهره‌برداری اقتصادی از داده‌ها را تعیین نمایند (کریمی، ۱۴۰۰: ۱۹۰). همچنین، ایجاد بیمه برای داده‌های دیجیتال می‌تواند ریسک استفاده ناصحیح یا افشای غیرمجاز داده‌ها را کاهش دهد و مالکیت مالی داده‌ها را تقویت کند. تحلیل تطبیقی نشان می‌دهد که در نظام‌های حقوقی پیشرفته، داده‌های شخصی به عنوان دارایی معنوی یا حق مالی شناخته شده و شامل حمایت قانونی، امکان انتقال و انتفاع اقتصادی هستند. چنین تجربه‌هایی می‌تواند الگوی مناسبی برای اصلاح نظام حقوقی ایران باشد و با توجه به ظرفیت‌های فقهی و حقوقی کشور، چارچوبی منطبق بر اصول عدالت و توسعه اقتصادی فراهم آورد (محسن‌نژاد، ۱۳۹۴: ۱۴۹). در نهایت، شناسایی داده‌های شخصی به عنوان حق مالی در حقوق خصوصی ایران، هم نیازمند اصلاح قوانین و تدوین مقررات اختصاصی است و هم بسترسازی برای بهره‌برداری اقتصادی مشروع از داده‌ها را فراهم می‌کند. این رویکرد می‌تواند هم از حقوق فردی و حریم خصوصی افراد حفاظت کند و هم توسعه کسب‌وکارهای دیجیتال و فناوری‌های نوین را تسهیل نماید، به گونه‌ای که تعادل میان امنیت اطلاعات و منافع اقتصادی حفظ شود (احمدی، ۱۴۰۰: ۱۴۰).

۵- مقایسه با حقوق بین‌الملل و تجارب تطبیقی

در سطح بین‌المللی، داده‌های شخصی به عنوان یک حق بنیادین و در عین حال دارایی اقتصادی مورد حمایت قرار گرفته‌اند. سازمان‌های بین‌المللی و اتحادیه‌ها، نظیر اتحادیه اروپا و سازمان همکاری اقتصادی و توسعه، چارچوب‌های قانونی مشخصی برای حفاظت از داده‌های شخصی تدوین کرده‌اند که هم جنبه حریم خصوصی و هم ارزش اقتصادی داده‌ها را مدنظر قرار می‌دهند. به

عنوان مثال، مقررات عمومی حفاظت از داده‌ها (GDPR) در اتحادیه اروپا، حقوق کاربران را شامل حق دسترسی، اصلاح، حذف و انتقال داده‌ها می‌داند و همزمان مسئولیت مالی و جبران خسارت در صورت افشای غیرمجاز داده‌ها را مشخص کرده است. این رویکرد، داده‌های شخصی را هم به عنوان حق فردی و هم به عنوان دارایی مالی قابل بهره‌برداری و جبران قانونی تلقی می‌کند. در کشورهای دیگر نیز، تجربه‌های متنوعی وجود دارد. در ایالات متحده آمریکا، قوانین فدرال و ایالتی مانند قانون حمایت از حریم خصوصی مصرف‌کنندگان کالیفرنیا، حقوق مصرف‌کنندگان بر داده‌های شخصی را به رسمیت شناخته و امکان جبران خسارت مالی در صورت نقض این حقوق را فراهم کرده‌اند (سولوو، دانیل ج. و هارتزگو، وودرو، ۲۰۱۸، ص. ۴۵). این قوانین به صراحت داده‌های شخصی را نوعی دارایی اقتصادی تلقی کرده و به افراد اجازه می‌دهند از طریق قراردادها یا شکایت قانونی، ارزش اقتصادی داده‌های خود را مطالبه کنند.

تجارب تطبیقی نشان می‌دهند که دو رویکرد عمده در سطح بین‌المللی وجود دارد: نخست، تمرکز بر حریم خصوصی و محدودیت استفاده بدون رضایت مالک داده؛ دوم، شناسایی داده‌های شخصی به عنوان دارایی اقتصادی که می‌تواند منتقل یا معامله شود. کشورهای اروپایی عمدتاً تلفیقی از هر دو رویکرد را اتخاذ کرده‌اند، به طوری که حفاظت از داده‌ها و بهره‌برداری اقتصادی همزمان تضمین می‌شود. این مدل می‌تواند به ایران الهام بخشد تا چارچوبی متوازن برای حقوق داده‌های شخصی ارائه دهد (سازمان همکاری اقتصادی و توسعه، ۲۰۱۳، ص. ۱۸).

یکی از نکات قابل توجه در تجارب بین‌المللی، استفاده از مکانیزم‌های بیمه‌ای و مسئولیت مالی برای جبران خسارت ناشی از افشای داده‌هاست. برای مثال، در اتحادیه اروپا، شرکت‌ها ملزم به ایجاد صندوق یا بیمه برای جبران خسارت داده‌ها هستند و این امر موجب شفافیت و امنیت اقتصادی کاربران می‌شود (اتحادیه اروپا، ۲۰۱۶، ص. ۲۵). چنین ابزارهایی می‌تواند در نظام حقوقی ایران نیز به عنوان مکمل مقررات سنتی و فقهی مورد استفاده قرار گیرد و امکان جبران خسارت و بهره‌برداری اقتصادی مشروع از داده‌ها را فراهم کند. در مقایسه با حقوق ایران، تفاوت اصلی در تعریف و شناسایی داده‌ها به عنوان دارایی مالی است. قوانین ایران بیشتر بر حفاظت حریم خصوصی و جلوگیری از افشای غیرمجاز تمرکز دارند و ارزش اقتصادی داده‌ها یا حقوق مالی مرتبط با آن‌ها به صراحت مورد توجه قرار نگرفته است (قنبری، فرهاد، ۱۳۹۹، ص. ۳۴). این خلا، موجب شده که مالکیت و بهره‌برداری اقتصادی داده‌ها محدود شود و امکان توسعه کسب‌وکارهای نوین دیجیتال به شکل کامل فراهم نگردد.

تجارب تطبیقی همچنین بر ضرورت شفافیت الگوریتمی و قراردادهای شفاف با کاربران تأکید دارند. در کشورهای پیشرفته، شرکت‌ها موظف‌اند شرایط استفاده از داده‌ها، اهداف پردازش و سهم مالک داده در منافع اقتصادی را مشخص کنند (سولوو، دانیل ج. و هارتزگو، وودرو، ۲۰۱۸، ص. ۵۰). این تجربه می‌تواند برای ایران الگو باشد تا ضمن حفاظت از حقوق فردی، امکان بهره‌برداری اقتصادی مشروع از داده‌ها فراهم گردد و تعادل میان حقوق مالک و توسعه فناوری حفظ شود. یکی دیگر از دستاوردهای مهم حقوق تطبیقی، شناسایی مسئولیت مشترک تولیدکننده، پردازش‌کننده و کاربر داده‌ها است. این رویکرد موجب می‌شود در صورت نقض حقوق داده‌ها، امکان انتساب مسئولیت و تعیین سهم مالی جبران خسارت به صورت دقیق وجود داشته باشد (صفایی، حسن، ۱۳۹۶، ص. ۲۱۸). ایران می‌تواند با اقتباس از این مدل، چارچوب قانونی و قراردادی متناسب با ظرفیت‌های داخلی و فقهی ایجاد کند. در نهایت، مقایسه با تجارب بین‌المللی نشان می‌دهد که حقوق داده‌های شخصی نه تنها باید به عنوان حق فردی و حریم خصوصی مورد حمایت قرار گیرد، بلکه ارزش اقتصادی و مالی آن نیز باید شناسایی شده و مورد حفاظت قانونی قرار گیرد. ترکیب این دو رویکرد، امکان ایجاد یک نظام جامع حقوقی در ایران را فراهم می‌کند که هم عدالت و امنیت کاربران را تضمین می‌کند و هم توسعه فناوری‌های دیجیتال و کسب‌وکارهای نوین را تسهیل می‌نماید (محسن‌نژاد، عبدالمومن، ۱۳۹۴، ص. ۱۴۹).

۶- سازوکارهای قضایی و اجرایی

با توجه به ارزش اقتصادی و حقوقی داده‌های شخصی، ایجاد سازوکارهای قضایی و اجرایی مناسب برای حفاظت از این حق مالی در ایران ضروری است. نخستین گام، شناسایی مراجع صالح قضایی و اداری برای رسیدگی به دعاوی مرتبط با داده‌های شخصی است. در حال حاضر، دادگاه‌های عمومی و شورای حل اختلاف وظیفه رسیدگی به دعاوی مرتبط با حقوق مدنی و اموال را بر عهده دارند، اما نبود مرجع تخصصی برای داده‌های شخصی و دعاوی فناوری اطلاعات موجب پراکندگی و تأخیر در رسیدگی‌ها می‌شود (قنبری، ۱۳۹۹، ص. ۳۶). بنابراین، ایجاد دادگاه یا شعب ویژه فناوری اطلاعات و داده‌های شخصی می‌تواند سرعت، دقت و کارآمدی رسیدگی‌ها را افزایش دهد. سازوکار قضایی دوم، تعیین معیارها و استانداردهای اثبات خسارت است. در دعاوی مرتبط با داده‌های شخصی به‌عنوان دارایی مالی، باید میزان ضرر اقتصادی و خسارت ناشی از سوءاستفاده یا افشای غیرمجاز داده‌ها به صورت دقیق محاسبه شود. این امر مستلزم استفاده از کارشناسان فناوری اطلاعات، حسابرسی داده‌ها و ارزیابی اقتصادی

داده‌هاست تا امکان جبران خسارت واقعی فراهم گردد (کریمی، ۱۴۰۰، ص. ۹۲). عدم وجود چنین سازوکاری، امکان پرداخت خسارت عادلانه را کاهش داده و امنیت حقوقی کاربران را تهدید می‌کند.

یکی دیگر از ابزارهای اجرایی، الزام به شفافیت و مستندسازی فعالیت‌های مرتبط با داده‌ها است. شرکت‌ها و سازمان‌ها باید سامانه‌های ثبت و ضبط داده‌ها، سیاست‌های استفاده و انتقال داده‌ها و اسناد قراردادهای کاربران را به‌طور شفاف نگهداری کنند. این اطلاعات می‌تواند به عنوان مدرک در دادگاه‌ها مورد استفاده قرار گیرد و امکان اثبات مسئولیت و جبران خسارت را تسهیل نماید (صفایی، ۱۳۹۶، ص. ۲۲۰). استفاده از مکانیسم‌های پیشگیرانه و حفاظتی نیز نقش مهمی در سازوکارهای اجرایی دارد. به عنوان مثال، وضع الزامات قانونی برای محافظت از داده‌ها، اعطای مجوزهای دسترسی محدود و اعمال پروتکل‌های امنیت سایبری، علاوه بر جلوگیری از تخلفات، شانس موفقیت دعاوی حقوقی را افزایش می‌دهد (احمدی، ۱۴۰۰، ص. ۸۳). این اقدام‌ها از منظر حقوقی، مشابه ابزارهای پیشگیری از ضرر در حقوق مدنی عمل می‌کنند و موجب کاهش دعاوی و خسارات احتمالی می‌شوند. در کنار اقدامات قضایی، سازوکارهای بیمه‌ای و جبران خسارت فوری می‌تواند از اهمیت بالایی برخوردار باشد. ایجاد بیمه اجباری یا اختیاری برای داده‌های شخصی، مشابه بیمه مسئولیت مدنی یا بیمه سایبری، امکان پرداخت سریع و شفاف خسارت به زیان‌دیدگان را فراهم می‌کند و فشار بر نظام قضایی را کاهش می‌دهد (کریمی، ۱۴۰۰، ص. ۹۵). این روش اجرایی، هم حفاظت مالی از کاربران را تضمین می‌کند و هم زمینه رشد کسب‌وکارهای دیجیتال را فراهم می‌آورد. تجارب بین‌المللی نشان می‌دهند که اجرای مقررات ویژه داده‌های شخصی نیازمند همکاری میان مراجع قضایی، نهادهای نظارتی و سازمان‌های تخصصی است. برای مثال، در اتحادیه اروپا، نهادهایی مانند مرکز حفاظت از داده‌ها (DPA) نقش نظارتی و اجرایی دارند و می‌توانند همزمان دستور توقف فعالیت‌های غیرمجاز، اعمال جریمه‌های مالی و حمایت از حقوق فردی را انجام دهند (اتحادیه اروپا، ۲۰۱۶، ص. ۲۸). ایران می‌تواند با اقتباس از این مدل، نهاد یا کمیته‌ای مستقل برای نظارت و اجرای حقوق مالی داده‌ها ایجاد کند.

همچنین، مکانیسم‌های حل اختلاف جایگزین نظیر داوری و میانجیگری تخصصی می‌تواند راهکار مؤثری برای کاهش بار قضایی و تسریع در رسیدگی به دعاوی داده‌های شخصی باشد. این روش‌ها به ویژه در قراردادهای تجاری و فناوری اطلاعات، امکان حل اختلاف با هزینه کمتر و در زمان کوتاه‌تر را فراهم می‌کنند (صفایی، ۱۳۹۶، ص. ۲۲۳). در نهایت، ترکیب این سازوکارها شامل مراجع قضایی تخصصی، استانداردهای اثبات خسارت، شفافیت و مستندسازی، ابزارهای پیشگیرانه، بیمه و نهادهای نظارتی، چارچوب جامعی برای حمایت از داده‌های شخصی به‌عنوان حق مالی در حقوق خصوصی ایران فراهم می‌کند. این سازوکارها نه تنها حقوق کاربران را تضمین می‌کنند، بلکه بستر توسعه کسب‌وکارهای دیجیتال و بهره‌برداری اقتصادی مشروع از داده‌ها را نیز تسهیل می‌نمایند (محسن‌نژاد، عبدالمومن، ۱۳۹۴، ص. ۱۵۰).

۷-چالش‌ها و راهکارها

یکی از اصلی‌ترین چالش‌ها در حمایت از داده‌های شخصی به‌عنوان حق مالی در حقوق ایران، عدم شناسایی صریح داده‌ها به‌عنوان دارایی مالی در قوانین موجود است. قوانین فعلی بیشتر بر حریم خصوصی و جلوگیری از افشای غیرمجاز داده‌ها تمرکز دارند و جنبه اقتصادی و مالی داده‌ها را به صراحت مورد توجه قرار نداده‌اند (قنبری، ۱۳۹۹، ص. ۳۴). این خلا، باعث می‌شود که مالکیت و بهره‌برداری اقتصادی از داده‌ها محدود شود و امکان مطالبه خسارت مالی در صورت سوءاستفاده یا افشای داده‌ها با پیچیدگی مواجه گردد. چالش دوم، نبود معیارهای مشخص برای ارزیابی ارزش اقتصادی داده‌ها است. در حقوق خصوصی ایران، مفاهیم سنتی مسئولیت مدنی و جبران خسارت عمدتاً برای اموال ملموس طراحی شده‌اند و تعیین ارزش داده‌های دیجیتال، که قابلیت تکثیر و انتقال سریع دارند، نیازمند روش‌های ارزیابی اقتصادی نوین است (کریمی، ۱۴۰۰، ص. ۹۳). بدون این معیارها، امکان پرداخت خسارت عادلانه و شفاف به زیان‌دیدگان محدود می‌شود و امنیت حقوقی کاهش می‌یابد. چالش سوم، پیچیدگی سازوکارهای قضایی و عدم وجود نهادهای تخصصی برای رسیدگی به دعاوی داده‌های شخصی است. دادگاه‌های عمومی و شوراهای حل اختلاف، با کمبود دانش فنی و ابزارهای لازم مواجه‌اند و این موضوع موجب طولانی شدن پرونده‌ها و کاهش کیفیت رسیدگی‌ها می‌شود (صفایی، ۱۳۹۶، ص. ۲۲۰). ایجاد شعب یا مراجع تخصصی برای فناوری اطلاعات و داده‌های شخصی می‌تواند این مشکل را کاهش دهد. چالش چهارم، مسائل امنیت سایبری و حفاظت فنی از داده‌ها است. حتی با وجود حمایت قانونی، فقدان استانداردهای امنیتی و پروتکل‌های حفاظتی موجب می‌شود داده‌ها در معرض سرقت، افشا یا سوءاستفاده قرار گیرند. این مسئله نه تنها تهدیدی برای حقوق مالی کاربران است، بلکه اثربخشی قوانین موجود را نیز کاهش می‌دهد (احمدی، ۱۴۰۰، ص. ۸۳).

چالش پنجم، نبود سازوکارهای بیمه‌ای و جبران خسارت فوری است. در صورت نقض حقوق داده‌های شخصی، فقدان بیمه یا صندوق جبران خسارت موجب می‌شود زیان‌دیدگان مدت طولانی منتظر دریافت خسارت بمانند و اعتماد به سیستم حقوقی کاهش یابد (کریمی، ۱۴۰۰، ص. ۹۵).

برای مواجهه با این چالش‌ها، راهکارهای متعددی پیشنهاد شده‌اند:

نخست، تدوین قوانین اختصاصی داده‌های شخصی به‌عنوان حق مالی است که ضمن حفظ حریم خصوصی، ارزش اقتصادی داده‌ها و حقوق مالی مرتبط با آن‌ها را مشخص کند. این قوانین می‌توانند با الهام از مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا و قانون حمایت از حقوق مصرف‌کننده کالیفرنیا در آمریکا طراحی شوند (اتحادیه اروپا، ۲۰۱۶، ص. ۱۲؛ سولوف و هارتزوگ، ۲۰۱۸، ص. ۴۵). راهکار دوم، ایجاد مراجع قضایی و نهادهای تخصصی برای رسیدگی به دعاوی مرتبط با داده‌ها است. این مراجع می‌توانند با حضور کارشناسان فناوری اطلاعات و اقتصاد دیجیتال، ارزیابی دقیق خسارت و تعیین مسئولیت را تسهیل کنند (صفایی، ۱۳۹۶، ص. ۲۲۳). راهکار سوم، تدوین استانداردهای امنیت سایبری و شفافیت الگوریتمی است. الزام به مستندسازی فرآیندهای پردازش داده‌ها، سیاست‌های دسترسی محدود و گزارش‌دهی منظم موجب کاهش ریسک افشا و تسهیل اثبات مسئولیت می‌شود (احمدی، ۱۴۰۰، ص. ۸۲).

راهکار چهارم، استفاده از مکانیسم‌های بیمه‌ای و صندوق جبران خسارت است تا زیان‌دیدگان بتوانند بدون پیچیدگی‌های قضایی، خسارت مالی خود را دریافت کنند و فشار بر نظام قضایی کاهش یابد. این رویکرد همچنین زمینه رشد کسب‌وکارهای دیجیتال را فراهم می‌کند (کریمی، ۱۴۰۰، ص. ۹۵). راهکار پنجم، ترکیب سازوکارهای قضایی، قراردادی و تطبیقی است. استفاده از داوری، میانجیگری و قراردادهای شفاف میان تولیدکننده، پردازش‌کننده و کاربر داده‌ها می‌تواند مسئولیت‌ها و سهم مالی هر طرف را مشخص کند و مانع از تضییع حقوق گردد (محسن‌نژاد، ۱۳۹۴، ص. ۱۵۰). در مجموع، چالش‌ها و محدودیت‌های موجود نشان می‌دهد که حمایت از داده‌های شخصی به‌عنوان حق مالی نیازمند تغییرات قانونی، ایجاد نهادهای تخصصی، استانداردهای فنی و سازوکارهای مالی و بیمه‌ای است. پیاده‌سازی این راهکارها می‌تواند ضمن حفاظت از حقوق کاربران، امنیت و توسعه فناوری‌های دیجیتال را در ایران تسهیل کند.

۸-نتیجه گیری

تحولات سریع فناوری اطلاعات و گسترش استفاده از داده‌های شخصی در عرصه‌های اقتصادی و اجتماعی، اهمیت حمایت از این داده‌ها را به‌عنوان یک دارایی مالی برجسته کرده است. داده‌های شخصی دیگر تنها جنبه حفاظت از حریم خصوصی ندارند و به دلیل قابلیت بهره‌برداری اقتصادی، نیازمند شناسایی حقوقی و قانونی مشخص برای تأمین امنیت مالی و اقتصادی دارند. نبود چارچوب قانونی روشن برای مالکیت و بهره‌برداری از داده‌ها، افراد و سازمان‌ها را در معرض خطر سوءاستفاده و فقدان امکان جبران خسارت قرار می‌دهد. نظام حقوقی موجود در ایران، به دلیل تمرکز بر اموال ملموس و روابط سنتی، توانایی کافی برای مدیریت مالکیت و جبران خسارت ناشی از داده‌های دیجیتال ندارد. فقدان معیارهای مشخص برای تعیین ارزش اقتصادی داده‌ها و نبود ابزارهای قانونی برای اثبات خسارت مالی، امنیت حقوقی کاربران و سرمایه‌گذاران دیجیتال را کاهش می‌دهد و فرآیند رسیدگی قضایی را پیچیده و زمان‌بر می‌کند. برای مقابله با این محدودیت‌ها، ایجاد مراجع قضایی و نهادهای تخصصی در حوزه فناوری اطلاعات و اقتصاد دیجیتال ضروری است. حضور کارشناسان فنی و اقتصادی می‌تواند فرآیند ارزیابی خسارت و تعیین مسئولیت را شفاف و دقیق کند و امکان جبران سریع‌تر و مؤثرتر را فراهم آورد. همچنین، تدوین استانداردهای امنیت سایبری و الزام به شفافیت الگوریتمی، بستر لازم برای پیشگیری از نقض داده‌ها و تسهیل اثبات تخلف را فراهم می‌کند. تجارب کشورهای پیشرفته نشان می‌دهد که ترکیب مقررات اختصاصی، سازوکارهای بیمه‌ای و نهادهای نظارتی مستقل، موثرترین مدل برای حمایت از داده‌های شخصی به‌عنوان دارایی مالی است. استفاده از ابزارهای داوری، میانجیگری و قراردادهای شفاف میان تولیدکننده، پردازش‌کننده و کاربر داده‌ها نیز می‌تواند مسئولیت‌ها را مشخص و مانع تضییع حقوق شود. با اجرای ترکیبی از تغییرات قانونی، ایجاد نهادهای تخصصی، استفاده از مکانیسم‌های بیمه‌ای و پیشگیری فنی، امکان حمایت مؤثر از داده‌های شخصی فراهم می‌شود. این رویکرد چندلایه، هم امنیت مالی و حقوقی کاربران را تأمین می‌کند و هم فضای لازم برای توسعه و نوآوری دیجیتال را فراهم می‌آورد، بدون اینکه مانعی برای رشد کسب‌وکارها ایجاد شود. در جمع‌بندی نهایی، می‌توان گفت که داده‌های شخصی به‌عنوان حق مالی یک دارایی نوین و ارزشمند هستند که حفاظت از آن‌ها ضرورت قانونی، اقتصادی و اجتماعی دارد. بازنگری در قوانین، ایجاد نهادهای تخصصی و بهره‌گیری از سازوکارهای پیشرفته و چندلایه می‌تواند چارچوبی متوازن برای حمایت از حقوق افراد و توسعه فناوری‌های دیجیتال در ایران ایجاد کند و هم عدالت مالی را تضمین نماید و هم نوآوری را تقویت کند.

منابع

- احمدی، محمد. (۱۴۰۰). مسئولیت مدنی در عصر فناوری‌های نوین. تهران: انتشارات دانشگاه تهران.
- کریمی، سعید. (۱۴۰۰). حقوق داده‌های شخصی و فناوری اطلاعات. تهران: انتشارات سمت.
- کاتوزیان، ناصر. (۱۳۹۱). حقوق مدنی: مسئولیت مدنی. تهران: نشر میزان.
- محسن‌نژاد، عبدالمومن. (۱۳۹۴). حقوق فناوری اطلاعات و مسئولیت مدنی. تهران: نشر دادگستر.
- قنبری، فرهاد. (۱۳۹۹). حریم خصوصی و داده‌های شخصی در حقوق ایران. تهران: انتشارات نور دانش.
- صفایی، حسن. (۱۳۹۶). مسئولیت مدنی و تحلیل خسارت در حقوق ایران. تهران: نشر عدالت.
- یوسفی، محمد. (۱۳۹۸). قراردادها و حقوق داده‌های شخصی. تهران: انتشارات دانشگاه علامه طباطبایی.