فصلنامه علمی تخصصی فقه و حقوق معاصر

سال دوازدهم- بهار1405- شماره 35-ص82-102

نقش هوش مصنوعی و مسئولیت حقوقی آن در حفاظت از حریم خصوصی

حاتم صارمی[1]

چکیده

رشد فزاینده فناوری‌های مبتنی بر هوش مصنوعی و ورود آن‌ها به عرصه‌های مختلف تصمیم‌گیری، نظارت و پردازش داده‌ها، موجب طرح مباحث جدیدی در حوزه مسئولیت حقوقی نسبت به صیانت از حریم خصوصی شده است. هوش مصنوعی با توانایی گردآوری، تحلیل و بهره‌برداری از داده‌های شخصی، امکان مداخله در حریم خصوصی افراد را افزایش می‌دهد و این امر ضرورت تعیین حدود و ثغور مسئولیت اشخاص حقیقی و حقوقیِ توسعه‌دهنده، بهره‌بردار یا ناظر بر این سامانه‌ها را دوچندان می‌کند. پژوهش حاضر با روش توصیفی ـ تحلیلی، به بررسی مبانی حقوقی مرتبط با تکالیف و الزامات حاکم بر استفاده از سامانه‌های هوشمند در مواجهه با داده‌های شخصی می‌پردازد و تلاش می‌کند جایگاه مسئولیت مدنی و آثار ناشی از نقض قواعد حریم خصوصی را تبیین نماید. نتایج نشان می‌دهد که خودکار بودن فرآیندها، گستره وسیع جمع‌آوری داده‌ها و دشواری احراز تقصیر، نظام‌های سنتی مسئولیت را با چالش‌هایی جدی مواجه می‌سازد و لزوم ایجاد چارچوب‌های حقوقی جدید یا بازنگری در قواعد موجود، برای تضمین حمایت مؤثر از حریم خصوصی افراد، امری اجتناب‌ناپذیر است.

کلیدواژگان: هوش مصنوعی، حریم خصوصی، داده‌های شخصی، مسئولیت مدنی، حمایت حقوقی.

[1] - گروه حقوق،حقوق خصوصی،واحد تهران شمال، دانشگاه آزاد اسلامی،تهران،ایران

مقدمه

ظهور و گسترش فزاینده فناوری‌های مبتنی بر هوش مصنوعی در دهه‌های اخیر، پارادایم‌های سنتی حقوق را در حوزه‌های مختلف، به‌ویژه در عرصه تعاملات دیجیتال، با چالشی بنیادین مواجه ساخته است. این سامانه‌های نوین که بر پایه پردازش‌های پیچیده و تحلیل‌های کلان‌داده استوارند، فراتر از ابزارهای ساده مخابراتی، دارای نوعی توانمندی در تصمیم‌گیری و استنتاج هستند که مرز میان عمل انسانی و فعل مکانیکی را کم‌رنگ کرده است. در نظام‌های حقوقی معاصر، مواجهه با این پدیده نیازمند بازنگری در مفاهیم کلاسیک «شخصیت حقوقی» و «عاملیت» است؛ چرا که هوش مصنوعی به عنوان یک نهاد فناورانه، به طور مستقیم بر حقوق بنیادین شهروندان اثرگذار بوده و ضرورت تدوین چارچوب‌های هنجاری جدید را ایجاب می‌نماید.

حق بر حریم خصوصی، به عنوان یکی از مصادیق برجسته حقوق بشر و آزادی‌های مشروع، در مواجهه با توانمندی‌های تجسسی و تحلیلی هوش مصنوعی در وضعیتی شکننده قرار گرفته است. این حق که در نظام‌های حقوقی پیشرفته و اسناد بین‌المللی بر پایه «حمایت از داده‌ها» و «کنترل فرد بر اطلاعات شخصی» بازتعریف شده، اکنون با سامانه‌هایی روبروست که قادرند از میان توده‌های عظیم اطلاعاتی غیرمرتبط، جزئی‌ترین ابعاد زندگی خصوصی افراد را استخراج و پیش‌بینی کنند. تداخل کارکردهای هوشمند با قلمرو خصوصی اشخاص، نه‌تنها امنیت روانی جامعه را تهدید می‌کند، بلکه مبانی آزادی اراده و کرامت انسانی را نیز که از ارکان حقوق مدنی هستند، تحت‌الشعاع قرار می‌دهد.

یکی از غامض‌ترین مسائل حقوقی در این حوزه، ماهیت‌شناسی مسئولیت ناشی از نقض حریم خصوصی توسط سامانه‌های هوشمند است. در حقوق کلاسیک، مسئولیت مدنی غالباً بر پایه «تقصیر» یا «رابطه سببیت» میان فعل فاعلی مختار و ضرر وارده استوار است؛ اما در هوش مصنوعی، به دلیل پیچیدگی‌های فنی و وجود نوعی خودمختاری در فرآیندهای درونی، انتساب ضرر به یک شخص معین (اعم از سازنده، مالک یا بهره‌بردار) با دشواری‌های اثباتی فراوانی روبروست. این وضعیت که در ادبیات حقوقی از آن به «بحران انتساب» یاد می‌شود،

ایجاب می‌کند که مبانی سنتی مسئولیت، از جمله نظریه خطر و مسئولیت مطلق، در پرتو تحولات نوین بازخوانی شوند تا از بی‌جبران ماندن خسارات معنوی و مادی ناشی از افشای داده‌ها جلوگیری گردد.

علاوه بر چالش‌های انتساب، خلاءهای قانونی در تعیین حدود تکالیف اشخاص مداخله‌گر در چرخه حیات هوش مصنوعی، بر ابهامات موجود افزوده است. در نبودِ مقرراتی که به طور صریح وظایف «مراقبت متعارف» را برای توسعه‌دهندگان این فناوری‌ها در جهت صیانت از حریم خصوصی تبیین کند، رویه‌های قضایی در تطبیق قواعد عام ضمان قهری با مصادیق نوین دچار تشتت می‌گردند. تبیین این موضوع که آیا نقض حریم خصوصی در این بستر باید به عنوان یک فعالیت خطرناک تلقی شود یا تابع قواعد عمومی تسبیب باشد، هسته اصلی مباحثات حقوقی کنونی را تشکیل می‌دهد که مستلزم تحلیل دقیقِ ماهیتِ تعهدات (تعهد به وسیله یا نتیجه) در قراردادهای ارائه خدمات هوشمند است.

پژوهش حاضر با درک ضرورت‌های فوق، درصدد است تا با رویکردی تحلیلی و با استناد به مبانی حقوق مدنی و استانداردهای صیانت از داده‌ها، نقش هوش مصنوعی را در استحاله مفهوم حریم خصوصی واکاوی نماید. هدف اصلی این نوشتار، تبیین مدل‌های مطلوب مسئولیت حقوقی است که بتواند ضمن حمایت از نوآوری‌های فناورانه، تضمین‌کننده حق بر خلوتِ اشخاص و جبران‌کننده آسیب‌های ناشی از فرآیندهای هوشمند باشد. با بررسی تطبیقی و تحلیل دکترین‌های موجود، این مقاله تلاش می‌کند راهکارهایی جهت تدوین نظام قانونی منسجم ارائه دهد که در آن، مسئولیت‌پذیری حقوقی به عنوان ابزاری برای مهار قدرت نظارتی هوش مصنوعی عمل نماید.

1- کلیات، مفاهیم حقوقی و مبانی نظری حمایت از حریم خصوصی

1-1-تحلیل مفهوم حریم خصوصی به‌عنوان حق بنیادین شخصیت

حریم خصوصی در نظام‌های حقوقی معاصر، فراتر از یک حق ساده فردی، به‌عنوان یکی از ارکان «حقوق شخصیت» شناخته می‌شود؛ حوزه‌ای که به حمایت از کرامت، آزادی اراده و استقلال وجودی انسان می‌پردازد. این حق، تجلی بنیادین اصل کرامت انسانی است و بر مبنای آن، هر شخص حق دارد زندگی شخصی، روابط

خانوادگی، اطلاعات فردی و نحوه حضور خود در عرصه عمومی را کنترل کند. در دکترین حقوقی، حریم خصوصی نه‌تنها از تعرض مادی و فضولی دیگران مصون دانسته شده، بلکه به‌عنوان حق تعیین حدود دسترسی دیگران به اطلاعات و رفتارهای فردی تلقی می‌شود. از همین رو، شالوده آن بر مفهوم «خودآیینی اطلاعاتی» استوار است؛ یعنی اختیار فرد در تعیین اینکه چه چیزی و تحت چه شرایطی از زندگی او قابل مشاهده یا بهره‌برداری باشد.[1]

از منظر حقوق بشر، حریم خصوصی جایگاهی ویژه دارد، زیرا تعرض به آن، به‌طور مستقیم ساختار هویتی و وضعیت شخصی انسان را هدف قرار می‌دهد. در اسناد بین‌المللی، این حق در زمره حقوق بنیادین و غیرقابل‌سلب قلمداد شده و حمایت از آن شرط تحقق سایر آزادی‌ها دانسته می‌شود. این دیدگاه، حریم خصوصی را نه یک حق فرعی، بلکه سنگ‌بنای آزادی‌های مدنی مانند آزادی بیان، آزادی رفت‌وآمد و امنیت شخصی می‌داند. هنگامی که شخص نتواند حدود زندگی خصوصی خود را کنترل کند، امکان تصمیم‌گیری آزادانه و زیستن بدون هراس نیز از او سلب می‌شود. به همین دلیل، حفاظت از این حق ملازم با تضمین امنیت روانی، حیثیت فردی و احترام به شأن اجتماعی افراد است.[2]

در حقوق داخلی نیز، حریم خصوصی به‌عنوان بخشی از قلمرو شخصیت افراد شناخته شده و حمایت از آن در قالب قواعد عام مسئولیت مدنی، ضمان قهری و نیز اصول ناظر بر منع افشا، نظارت یا بهره‌برداری غیرمجاز از اطلاعات تجسم یافته است. این حق، به‌ویژه در بستر فناوری‌های نوین، نقش بارزتری یافته؛ چرا که هرگونه دسترسی، پردازش یا انتشار داده‌های مربوط به شخص، مستقیماً با هویت فردی و حیثیت اجتماعی او در ارتباط است. جایگاه بنیادین این حق اقتضا می‌کند که هر نوع تعرض به آن، به دلیل لطمه به کرامت انسانی، واجد وصف نامشروع بوده و مستوجب ضمانت‌اجراهای مؤثر باشد. بدین ترتیب، حریم خصوصی نه صرفاً یک امتیاز فردی

[1] - باشی پور حقیقی،سیدامیر؛ شجاعیان،خدیجه؛ علایی،حسین(1403)، تاثیرگذاری هوش مصنوعی برحق بر حریم خصوصی بیماران با تاکید بر چالش ها و خلاها، مجله حقوق پزشکی، دوره هجدهم،ص8

[2] - اصلانی، محسن؛ زمانی، سید قاسم؛ راعی، مسعود (1401)، ضمانت اجرای نقض تعهدات حقوق بشری دولت‌ها در حقوق بین الملل با رویکردی به فقه جزا، فصلنامه فقه جزای تطبیقی، دوره دوم، شماره چهارم، ص63

بلکه محور حقوق شخصیت است؛ محوری که نظام حقوقی مکلف است آن را در برابر هرگونه تهاجم، چه انسانی و چه فناورانه، مورد حمایت کامل قرار دهد.

2-1-تبیین ماهیت حقوقی هوش مصنوعی در نظام حقوقی

در تحلیل ماهیت حقوقی هوش مصنوعی، نخستین رویکرد آن است که این فناوری را در حکم «ابزار» تلقی می‌کند؛ ابزاری پیشرفته که صرفاً کارکردهای انسان را در پردازش داده‌ها، تحلیل و تصمیم‌سازی تقویت می‌کند، اما فاقد هرگونه اراده مستقل حقوقی است. در این برداشت، رابطه انسان با سامانه هوشمند همانند رابطه کاربر با ابزارهای متعارف است و فعل حقوقی منتسب به شخصی است که ابزار را در اختیار دارد یا آن را هدایت می‌کند. بر مبنای این نگاه، مسئولیت مدنی در وقوع ضرر ناشی از عملکرد هوش مصنوعی، بر پایه قواعد سنتی تسبیب تحلیل می‌شود و شخص بهره‌بردار یا دستوردهنده، در حکم مباشر یا مسبب شناخته می‌گردد. این تفسیر با اصول بنیادین حقوق مدنی سازگار است؛ زیرا هوش مصنوعی را فاقد شخصیت و فاقد ظرفیت انتساب اراده می‌داند. رویکرد دوم، هوش مصنوعی را «شیء» محسوب می‌کند؛ یعنی نهادی فاقد شخصیت، که مالکیت بر آن همانند مالکیت بر اموال دیگر، واجد آثار حقوقی مشخص است. در این رویکرد، سامانه هوشمند در زمره اموالی قرار می‌گیرد که می‌تواند موضوع حق مالکیت، موضوع قرارداد و حتی موضوع تعهدات نگهداری و مراقبت باشد. مطابق این دیدگاه، خسارات ناشی از عملکرد هوش مصنوعی، همانند خسارات ناشی از سایر اموال خطرزا یا پیچیده، می‌تواند تحت قواعد مسئولیت ناشی از نگهداری اموال، مسئولیت مبتنی بر خطر یا تعهد به مراقبت مورد بررسی قرار گیرد. این رویکرد در بسیاری از نظام‌های حقوقی با پذیرش مقررات خاص برای «اموال خطرزا» هم‌خوانی دارد و امکان اعمال قواعد ضمان قهری، از جمله قاعده اتلاف و تسبیب را فراهم می‌کند.رویکرد سوم، هوش مصنوعی را «واسطه فعل انسانی» می‌داند؛ به این معنا که فناوری یادشده، ماهیتی میانه میان ابزار و فاعل انسانی پیدا می‌کند و نقشی فعال در شکل‌گیری نتیجه ایفا می‌نماید، بی‌آنکه خود واجد اراده حقوقی باشد. در این نگاه، فعل نهایی به انسان منتسب است، ولی واسطه‌گری سامانه هوشمند در تحقق ضرر، موجب پیچیدگی در تعیین مباشر، مسبب و سبب اقوی می‌شود. این تحلیل، با مفهوم «واسطه مستقل» یا «عامل خودکار» در برخی

نظام‌های حقوقی مقایسه‌پذیر است و به‌ویژه در مواردی که بهره‌بردار بر فرآیندهای درونی کنترل کامل ندارد، نظام‌های مبتنی بر خطر یا مسئولیت تضامنی را تقویت می‌کند. بدین ترتیب، هوش مصنوعی نه صرفاً ابزار است و نه فاعل، بلکه حلقه‌ای میان اراده انسانی و نتیجه زیان‌بار است.[1]

در مجموع، تعیین ماهیت حقوقی هوش مصنوعی از میان سه برداشت فوق، آثار تعیین‌کننده‌ای بر نظام مسئولیت حقوقی دارد. تلقی آن به‌عنوان ابزار، مسئولیت را به سمت قواعد تقصیر و تسبیب سوق می‌دهد؛ تلقی آن به‌عنوان شیء، مسئولیت را در چارچوب نگهداری اموال خطرزا و نظریه خطر سامان می‌دهد؛ و تلقی آن به‌عنوان واسطه فعل انسانی، نظریه‌های نوینی چون مسئولیت ترکیبی یا مسئولیت توزیعی را برجسته می‌سازد. از آنجا که هیچ‌یک از این برداشت‌ها به‌تنهایی پاسخگوی پیچیدگی‌های هوش مصنوعی نیستند، بسیاری از نظام‌های حقوقی به‌سمت مدل‌های تلفیقی حرکت کرده‌اند تا بتوانند تعامل میان انسان، فناوری و زیان را با دقت بیشتری تحلیل کنند. این ضرورت نشان می‌دهد که ماهیت حقوقی هوش مصنوعی، مفهومی ثابت و ایستا نیست، بلکه در حال شکل‌گیری و نیازمند تنظیم‌گری متناسب با کارکردهای نوین آن است.

1-3-قلمرو شمول حمایت حقوقی از داده‌های شخصی و اطلاعات خصوصی

قلمرو حمایت حقوقی از داده‌های شخصی، در نخستین گام، شامل هر نوع داده‌ای است که به‌طور مستقیم یا غیرمستقیم به شناسایی یک شخص حقیقی منجر شود. این داده‌ها صرفاً محدود به نام، نشانی یا شماره تماس نیستند، بلکه دامنه گسترده‌ای از اطلاعات هویتی، خانوادگی، ارتباطی، مالی، زیستی و رفتاری را دربرمی‌گیرند. هر داده‌ای که بتواند ویژگی‌های فرد را آشکار سازد یا با ترکیب در کنار سایر داده‌ها، قابلیت انتساب به یک شخص را پیدا کند، در دایره حمایت قرار می‌گیرد. از این منظر، داده‌های خام و داده‌های پردازش‌شده هر دو

[1] - بنافی، فرشته (1402)، حفاظت از حق حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی، نشریه پژوهش حقوق خصوصی، دوره 12، شماره 45، ص160-154

تحت حمایت قرار دارند، زیرا هر دو به شکلی بالقوه توانایی نقض حریم خصوصی و تحمیل آثار زیان‌بار بر حیثیت و موقعیت اجتماعی فرد را دارند. بنابراین، هر نوع دسترسی، پردازش یا افشای این داده‌ها بدون مبنای قانونی یا رضایت معتبر، واجد وصف نامشروع است.[1]

دومین بخش از قلمرو حمایت، «اطلاعات خصوصی» است که صرف‌نظر از ماهیت داده‌ای، ناظر بر قلمرو شخصی و غیرعلنی زندگی فرد است. این بخش شامل روابط خانوادگی، مکاتبات، ارتباطات خصوصی، سبک زندگی، عادات رفتاری، سوابق پزشکی، وضعیت مالی و کلیه اموری است که شخص، عرفاً یا قانوناً انتظار محرمانگی نسبت به آن‌ها دارد. در این حوزه، معیار نه صرفاً قابلیت شناسایی، بلکه «انتظار معقولِ محرمانگی» است؛ یعنی جایی که فرد از منظر اجتماعی و حقوقی انتظار دارد دیگران به آن وارد نشوند. این دسته از اطلاعات، به دلیل ارتباط مستقیم با کرامت انسانی، از بالاترین سطح حمایت برخوردارند و تعرض به آن‌ها در قالب برداشت، تحلیل یا ذخیره‌سازی می‌تواند به‌عنوان تعرض به شخصیت و حیثیت فرد تلقی شود.

سومین بخش از قلمرو شمول، داده‌هایی است که در بستر فناوری‌های نوین و محیط‌های هوشمند تولید می‌شوند؛ داده‌هایی که ممکن است ظاهراً بی‌اهمیت یا غیرشخصی به‌نظر برسند، اما در عمل، با پردازش و ترکیب، می‌توانند تصویری دقیق از زندگی فرد ایجاد کنند. داده‌های رفتاری، الگوهای استفاده از خدمات، سوابق جست‌وجو، داده‌های مکانی و داده‌های تولیدشده در تعامل با سامانه‌های هوشمند در این دسته قرار می‌گیرند. قانون‌گذار در بسیاری از نظام‌های حقوقی، این داده‌ها را در گستره حمایت قرار داده است، زیرا قدرت پیش‌بینی‌گری و تحلیل‌پذیری آن‌ها ممکن است نسبت به داده‌های کلاسیک حتی خطرآفرین‌تر باشد. بنابراین، قلمرو حمایت حقوقی از داده‌های شخصی و اطلاعات خصوصی امروزه بسیار فراتر از داده‌های هویتی سنتی است و دامنه‌ای گسترده را شامل می‌شود که هدف آن، حفظ کنترل فرد بر زندگی خصوصی خود و جلوگیری از مداخلات ناموجه انسانی یا فناورانه است.[2]

[1] - بهبودی، عادله (1401)، هوش مصنوعی در امنیت سایبری، پانزدهمین کنفرانس بین المللی فناوری اطلاعات، کامپیوتر و مخابرات، ص10

[2] - حکمت نیا،محمود؛ محمدی، مرتضی؛ واثقی، محسن(1398)، مسئولیت مدنی ناشی از تولید ربات‌های مبتنی بر هوش مصنوعی خودمختار، نشریه حقوق اسلامی،دوره16، شماره60، ص245

1-4-مبانی فقهی و حقوقی لزوم صیانت از اسرار و اطلاعات اشخاص

در مبانی فقهی، لزوم صیانت از اسرار و اطلاعات خصوصی اشخاص بر پایه مفاهیم بنیادینی همچون «کرامت انسانی» و «حرمت عِرض و آبرو» استوار است. فقه اسلامی با تکیه بر ادله شرعی، از جمله نهی صریح از «تجسس» در امور خصوصی دیگران، حریمی مصون از تعرض برای افراد قائل است که نفوذ به آن بدون اذن صاحب حق، نامشروع تلقی می‌شود. علاوه بر این، «قاعده لاضرر» به‌عنوان یکی از قواعد حاکم و راهبردی، هرگونه اقدام فناورانه یا انسانی را که منجر به ورود آسیب به حیثیت یا منافع مادی و معنوی افراد از طریق افشای اسرار گردد، نفی می‌کند. همچنین، امانت‌داری در قبال داده‌هایی که در اختیار اشخاص یا سازمان‌ها قرار می‌گیرد، از مصادیق «امانت شرعی» محسوب شده و هرگونه کوتاهی در حفظ آن، موجب تحقق مسئولیت و ضمان قهری برای صاحب ید خواهد بود.

از منظر حقوقی، صیانت از اطلاعات خصوصی به‌عنوان یکی از مصادیق بارز «حقوق شخصیت» و حقوق بنیادین شهروندی شناخته می‌شود. در قانون اساسی و سایر قوانین موضوعه، حیثیت و حریم خصوصی اشخاص از تعرض مصون داشته شده و دولت مکلف به ایجاد چارچوب‌های حمایتی برای صیانت از این حق گشته است. این مبنای حقوقی بر این اصل استوار است که اطلاعات شخصی، بخشی از دارایی‌های معنوی و هویتی فرد است و هرگونه پردازش یا تحلیل غیرمجاز آن، به‌منزله تعدی به تمامیتِ شخصیتی انسان تلقی می‌گردد. در واقع، حق بر محرمانگی اطلاعات، لازمه تحقق آزادی فردی و امنیت قضایی در جامعه است و بدون حمایت قانونی از این قلمرو، امکان زیستِ باکرامت در فضای عمومی و خصوصی سلب خواهد شد.

در دکترین مسئولیت مدنی، مبنای لزوم صیانت از اسرار بر نظریه «تعهد به مراقبت» و «پیشگیری از وقوع ضرر» استوار است. بر اساس این دیدگاه، اشخاصی که به واسطه فعالیت‌های فنی یا حرفه‌ای خود به داده‌های دیگران دسترسی پیدا می‌کنند، دارای یک «رابطه امانی» با صاحبان داده هستند. در نتیجه، هرگونه افشا یا عدم اتخاذ تدابیر امنیتی کافی که منجر به دسترسی اشخاص ثالث به این اطلاعات شود، مصداق «تقصیر» محسوب شده و موجب مسئولیت مدنی فاعل می‌گردد. حقوقدانان معتقدند که صیانت از اطلاعات نه‌تنها یک تکلیف اخلاقی، بلکه یک

تعهد قانونی ناشی از حسن نیت در قراردادها و الزامات خارج از قرارداد است که هدف آن حفظ توازن میان منافع عمومی و حقوق فردی است.[1]

لذا، تلاقی مبانی فقهی و حقوقی نشان می‌دهد که ضرورت حفاظت از داده‌ها در عصر هوش مصنوعی، ناشی از یک ضرورت اجتماعی و نظم عمومی است. هوش مصنوعی با توانایی استخراج اسرار مکتوم از میان توده‌های داده، عملاً می‌تواند «قاعده کتمان سر» را با چالش مواجه کند؛ لذا نظام حقوقی با تکیه بر اصولی همچون «سلطه انسان بر خویشتن» و «قاعده احترام به مال و عمل مسلم»، نظارت بر این سامانه‌ها را الزامی می‌داند. در این چارچوب، صیانت از اطلاعات تنها به معنای خودداری از افشا نیست، بلکه شامل تکالیف ایجابی نظیر شفافیت در پردازش، محدودیت در جمع‌آوری و تضمین امنیت داده‌هاست. این مبانی، شالوده هرگونه قانون‌گذاری در حوزه فناوری‌های نوین را تشکیل می‌دهند تا اطمینان حاصل شود که پیشرفت فنی، به قیمت فروپاشیِ حریم‌های اخلاقی و حقوقی تمام نگردد.

1-5-رابطه میان اصل کرامت انسانی و ممنوعیت مداخله غیرمجاز در حریم خصوصی

اصل کرامت انسانی به‌عنوان بنیادین‌ترین ارزش حقوقی در نظام‌های حقوقی و فقهی، مبنای مشروعیت بسیاری از حقوق اساسی از جمله حق بر حریم خصوصی است. کرامت انسان اقتضا می‌کند که هر فرد، دارای عرصه‌ای مصون از تعرض باشد تا بتواند هویت، شخصیت و اراده آزاد خود را شکل داده و بدون بیم از نظارت یا مداخله غیرمجاز، زندگی شخصی و روابط خصوصی خود را سامان دهد. در این چارچوب، حریم خصوصی نه‌تنها یک حق مستقل، بلکه جلوه‌ای از احترام به جایگاه ذاتی انسان است؛ زیرا افشای اسرار یا دسترسی ناموجه به اطلاعات فرد، عملاً شخصیت انسانی او را ابزار اراده دیگری می‌سازد و با مقام والای انسان به‌مثابه غایت و نه وسیله، تعارضی آشکار دارد.

[1] - میرشکاری،عباس؛ ثابت قدم،فاطمه؛ اصغرنیا،مرتضی(1403)، درآمدی بر چالش های فناوری هوش مصنوعی در حوزه حریم خصوصی، فصلنامه علمی مطالعات حقوقی فضای مجازی، سال سوم،شماره چهارم،ص73

از منظر حقوق اساسی، ممنوعیت مداخله غیرمجاز در حریم خصوصی، یک تکلیف مستقیم و برآمده از اصل کرامت انسانی برای دولت‌ها و اشخاص است. هرگونه ورود به عرصه خصوصی اشخاص—اعم از نظارت، گردآوری داده، پردازش یا افشای اطلاعات—تنها در صورتی مشروع است که یا با رضایت معتبر شخص همراه باشد، یا مستند به اختیار قانونی و ضرورت‌های استثنایی باشد. قوانین اساسی و اسناد حقوق بشری، این ممنوعیت را در کنار اصولی چون احترام به حیثیت، آزادی اندیشه و حق بر خودمختاری فردی قرار داده‌اند، زیرا تعرض به حریم خصوصی می‌تواند کرامت انسان را مخدوش کرده و او را در معرض برچسب‌گذاری، کنترل، تبعیض و بی‌اعتباری اجتماعی قرار دهد. لذا ممنوعیت مداخله غیرمجاز، سازوکاری اجرایی برای پاسداشت یک اصل ارزشی بنیادین است.

نتیجتاً، پیوند میان کرامت انسانی و حریم خصوصی، پیوندی ماهوی و ناگسستنی است: کرامت، مبنای وجودی حق بر حریم خصوصی است و صیانت از این حریم، ابزار تحقق کرامت در زندگی واقعی انسان‌ها. در عصر فناوری‌های نوین و نظام‌های پردازش داده مبتنی بر جمع‌آوری گسترده اطلاعات، این رابطه اهمیت مضاعف یافته است؛ زیرا کوچک‌ترین دسترسی یا تحلیل ناموجه از داده‌های فرد، می‌تواند تصویری کامل از هویت او آشکار کند و به‌طور مستقیم با کرامتش در تعارض قرار گیرد. بنابراین، نظام‌های حقوقی در تفسیر و اجرای قواعد مربوط به حریم خصوصی، ناگزیرند اصل کرامت انسانی را به‌عنوان معیار تفسیر، محدودسازی دخالت‌ها و تشخیص مشروعیت اعمال، در نظر گیرند تا توازن میان پیشرفت فناوری و مقام والای انسان حفظ شود.

2-تحول تاریخی مفهوم حریم خصوصی از حقوق سنتی به حقوق نوین

تحول مفهوم حریم خصوصی در حقوق، از مرحله‌ای آغاز شد که در نظام‌های سنتی، اهتمام اصلی بر صیانت از «حرمت منزل»، «اسرار خانوادگی» و «آبرو» معطوف بود. در این دوره، حریم خصوصی بیشتر جنبه مکانی و حیثیتی داشت و حمایت حقوقی عمدتاً ناظر بر جلوگیری از ورود فیزیکی غیرمجاز، افشای اسرار خانوادگی یا تعرض به حیثیت اجتماعی افراد بود. قواعد فقهی همچون حرمت تجسس، قاعده لاضرر و اصل احترام به آبرو، و نیز قواعد عرفی و اخلاقی، مهم‌ترین ابزارهای حمایت محسوب می‌شدند. در حقوق کلاسیک، حریم خصوصی

عمدتاً به «حق بر تنهایی» یا «مصونیت از فضولی دیگران» محدود می‌شد و هنوز به‌عنوان یک حق مستقل یا دارای ابعاد اطلاعاتی شناخته نشده بود. با ورود جهان به عصر ارتباطات، فناوری‌های اطلاعاتی و سپس سامانه‌های هوشمند، مفهوم حریم خصوصی دچار گسترشی بنیادین شد و از قالب سنتیِ مکان‌محور و حیثیت‌محور، به یک «حق بر کنترل داده» و «حق بر خودمختاری اطلاعاتی» تبدیل گردید. در حقوق نوین، تمرکز اصلی بر داده‌های شخصی، نحوه گردآوری، پردازش، تحلیل و بهره‌برداری از آن‌ها است، زیرا تهدید علیه حریم خصوصی دیگر از مسیر نفوذ فیزیکی رخ نمی‌دهد، بلکه از طریق استخراج الگوها، پیش‌بینی رفتار و تحلیل اطلاعات صورت می‌گیرد. اسناد بین‌المللی و قوانین جدید، حریم خصوصی را به‌عنوان حقی پویا و چندبُعدی تلقی می‌کنند که علاوه بر حفاظت از زندگی شخصی، به پاسداشت کرامت انسانی، جلوگیری از سلطه اطلاعاتی و تأمین امنیت فردی در محیط‌های فناورانه نیز می‌پردازد. به این ترتیب، حریم خصوصی در حقوق نوین، به یکی از ارکان هویت فردی و آزادی‌های بنیادین بدل شده است.[1]

3-نقش گسترش ابزارهای پردازش اطلاعات در تشدید مخاطرات حقوقی حریم خصوصی

گسترش ابزارهای پردازش اطلاعات، ساختار سنتی حریم خصوصی را با چالشی بی‌سابقه مواجه کرده است. در گذشته، تعرض به حریم خصوصی غالباً از طریق دسترسی مستقیم، مشاهده فیزیکی یا افشای عمومی رخ می‌داد؛ اما ابزارهای فناورانه جدید، امکان استخراج اطلاعات را بدون تماس فیزیکی و حتی بدون آگاهی صاحب داده فراهم کرده‌اند. این ابزارها قادرند از میان حجم انبوه داده‌های پراکنده، مجموعه‌ای منسجم از اطلاعات حساس فرد تشکیل دهند و ابعادی از زندگی شخصی او را آشکار سازند که حتی خود فرد نیز به آن توجه ندارد. نتیجه این تحول، شکل‌گیری نوعی «نفوذ نامرئی» است که ماهیت آن با تعرض‌های سنتی کاملاً متفاوت است و از همین رو، نیازمند قواعد حمایتی ویژه و سازوکارهای حقوقی نوین است.

[1] - مکی، اکرم السادات؛ مکی، زهرا السادات؛ کشکولیان، اسماعیل(1403)، بررسی مسئولیت ناشی از اعمال هوش مصنوعی در نظام حقوقی ایران، نشریه علمی فقه، حقوق و علوم جزا، سال هشتم، شماره32،ص72

در سطح حقوقی، قدرت پردازش اطلاعات، تهدیدات پیچیده‌تری ایجاد کرده است؛ زیرا قابلیت تحلیل و بازسازی هویت افراد، امکان کنترل، پیش‌بینی رفتار و طبقه‌بندی آنان را فراهم می‌آورد. این امر نه‌تنها حق بر محرمانگی را خدشه‌دار می‌کند، بلکه بر حقوقی مانند آزادی اندیشه، خودمختاری فردی و برابری نیز تأثیر می‌گذارد. وقتی ابزارهای پردازش قادرند از رفتارهای ظاهراً بی‌اهمیت، داده‌هایی حساس مانند وضعیت سلامت، روابط خانوادگی یا ترجیحات شخصی را استنباط کنند، ظرفیت تهدید نسبت به حیثیت و کرامت انسان افزایش می‌یابد. در نتیجه، مفهوم تعرض از «افشای مستقیم» به «تحلیل و برداشت غیرمجاز» گسترش یافته و مسئولیت مدنی نیز نه‌تنها بر پایه افشا، بلکه بر مبنای پردازش ناموجه نیز شکل می‌گیرد. [1]

افزون بر این، گسترش این ابزارها، مسئولیت‌پذیری و نظارت حقوقی را دشوارتر کرده است. ماهیت پیچیده پردازش داده‌ها، باعث می‌شود منشأ آسیب، نقش فاعل، میزان تقصیر و نحوه وقوع تعرض به سادگی قابل تشخیص نباشد. در بسیاری از موارد، افراد یا نهادهایی که داده‌ها را جمع‌آوری می‌کنند، حتی نسبت به آثار ثانویه پردازش یا ترکیب داده‌ها آگاهی کافی ندارند. همین امر، زمینه ایجاد «مخاطرات ساختاری» را فراهم می‌کند؛ مخاطراتی که نه ناشی از سوءنیت، بلکه نتیجه ضعف سازوکارهای نظارتی، شفاف نبودن فرآیندهای پردازش و عدم رعایت حداقل‌های احتیاطی است. بنابراین، گسترش ابزارهای پردازش، ضرورت وضع قواعد دقیق‌تر، ایجاد استانداردهای سختگیرانه‌تر امنیت داده و تقویت نظریه تعهد به مراقبت را بر نظام‌های حقوقی تحمیل کرده است.

4-تحلیل مبانی و ارکان مسئولیت حقوقی ناشی از نقض حریم خصوصی

مسئولیت حقوقی ناشی از نقض حریم خصوصی بر مبنای مبانی فنی، اخلاقی و حقوقی مبتنی بر قراردادی و قهری استوار است که هر یک نقش کلیدی در تعیین مسئولیت و علت‌العلل وقوع ضرر دارند. از مبانی فقهی و حقوقی، «قاعده لاضرر» و اصل احترام به آبرو و کرامت انسانی، نشان‌دهنده الزام قانونی و اخلاقی اجتناب از هرگونه مداخله غیرمجاز است که منجر به ضرر و تضعیف شأن فرد می‌شود. در سطح حقوق مدنی و حقوق بشر،

[1] - مرتضوی،سیدمرتضی؛ خدایی فام،حجت(1404)، بررسی آثار به کارگیری هوش مصنوعی بر حریم خصوصی اشخاص و مسئولیت مدنی ناشی از آن، سال ششم، شماره22،ص10

این مسئولیت بر پایه «اصل جبران خسارت» و «نظریه تعهد به مراقبت» است که فاعل خطاکار باید در صورت نقض این حقوق، جبران خسارت‌های وارده را بر عهده گیرد. ارکان اصلی این مسئولیت شامل «خطای ناشی از انجام فعل خلاف قانون یا بی‌احتیاطی»، «ضرر وارد شده به شخص حقیقی یا حقوقی» و «رابطه سببیت میان فعل و ضرر» است که در صورت احراز هر سه، فرد یا نهاد مسئول باید پاسخگو باشد. این مجموعه مبانی و ارکان، نظام حقوقی را ملزم می‌کند که در قبال تعرض به حریم خصوصی، مسئولیت کیفری و مدنی فرد یا نهاد ناقض را تضمین کند و دفاع از کرامت و آزادی‌های فردی را اولویت بخشد.

4-1-بررسی ارکان تحقق مسئولیت مدنی در نقض حریم خصوصی

تحقق مسئولیت مدنی در نقض حریم خصوصی مستلزم احراز ارکان سه‌گانه «فعل زیان‌بار»، «ورود ضرر» و «رابطه سببیت» است که در پرتو معیار تقصیر و تعهد به مراقبت تفسیر می‌شوند. نخست، فعل زیان‌بار می‌تواند به‌صورت اقدام مثبت مانند افشا، انتشار، پردازش یا بهره‌برداری غیرمجاز از اطلاعات خصوصی، یا ترک فعل همچون عدم اتخاذ تدابیر متعارف امنیتی برای حفاظت از داده‌ها تحقق یابد؛ معیار سنجش آن، تخلف از الزامات قانونی، نقض رضایت معتبر یا عدول از استانداردهای حرفه‌ای احتیاط است. دوم، ضرر باید واقعی و قابل انتساب باشد و می‌تواند مادی (زیان مالی، از دست رفتن فرصت‌ها) یا معنوی (لطمه به حیثیت، اضطراب، خدشه به کرامت) باشد؛ در حوزه حریم خصوصی، پذیرش خسارت معنوی نقش محوری دارد. سوم، رابطه سببیت زمانی احراز می‌شود که بین رفتار ناقض و زیان وارده، پیوندی مستقیم و مؤثر برقرار باشد؛ در موارد پیچیده فناورانه، این رابطه از طریق قرائن فنی و اصل قابلیت پیش‌بینی زیان احراز می‌گردد. با اجتماع این ارکان، مسئولیت مدنی مستقر شده و مرتکب مکلف به جبران کامل خسارت و اعاده وضعیت متضرر تا حد امکان خواهد بود.[1]

4-2-تحلیل مسئولیت اشخاص حقیقی و حقوقی در بهره‌برداری از سامانه‌های هوشمند

[1] - فهیمی کبیر، شیرین(1404)، بررسی حریم خصوصی و حفاظت از داده ها در عصر هوش مصنوعی، فصلنامه علمی مطالعات حقوق و علوم قضایی، سال دوم، شماره4،صص360

مسئولیت اشخاص حقیقی و حقوقی در بهره‌برداری از سامانه‌های هوشمند بر مبنای اصل انتساب رفتار، تعهد به مراقبت و نظریه خطر قابل تحلیل است؛ بدین معنا که هر شخصی که این سامانه‌ها را طراحی، راه‌اندازی، بهره‌برداری یا مدیریت می‌کند، در قبال آثار زیان‌بار ناشی از کارکرد آن‌ها پاسخگو است، مگر آنکه اثبات نماید تمامی تدابیر متعارف و فنی لازم را برای پیشگیری از ضرر اتخاذ کرده است. در مورد اشخاص حقیقی، مسئولیت معمولاً بر پایه تقصیر (اعم از بی‌احتیاطی، بی‌مبالاتی یا عدم رعایت ضوابط حرفه‌ای) استوار است؛ اما در خصوص اشخاص حقوقی، به‌ویژه شرکت‌ها و نهادهای بهره‌بردار، علاوه بر تقصیر سازمانی، می‌توان از مبنای «مسئولیت ناشی از فعالیت خطرزا» یا «مسئولیت کارفرما نسبت به اعمال کارکنان» بهره گرفت، زیرا انتفاع اقتصادی از سامانه و قدرت کنترل بر آن‌ها، رابطه سببیت را تقویت می‌کند. در این چارچوب، چنانچه نقض حریم خصوصی یا ورود خسارت ناشی از نقص در طراحی، ضعف نظارت، یا بهره‌برداری نامتعارف باشد، شخص حقوقی به‌عنوان بهره‌بردار اصلی مسئول جبران خسارت خواهد بود، حتی اگر فعل زیان‌بار به‌طور مستقیم توسط کارمند یا عامل فنی صورت گرفته باشد؛ زیرا کنترل، هدایت و نفع اقتصادی از فعالیت، مبنای استقرار مسئولیت را تشکیل می‌دهد.[1]

4-3-چالش انتساب فعل زیان‌بار در فرآیندهای تصمیم‌گیری غیرمستقیم

چالش انتساب فعل زیان‌بار در فرایندهای تصمیم‌گیری غیرمستقیم، نخست از آنجا ناشی می‌شود که در این فرایندها، تصمیم نهایی نه محصول یک اقدام صریح و منفرد انسانی، بلکه حاصل سلسله‌ای از پردازش‌های پیچیده، لایه‌مند و گاه غیرشفاف است که تنها بخش‌های محدودی از آن تحت کنترل مستقیم بهره‌بردار قرار دارد. این وضعیت سبب می‌شود مرز میان «فعل انسانی» و «اثر سامانه هوشمند» مخدوش گردد و تشخیص این‌که کدام بخش از نتیجه به رفتار انسانی قابل انتساب است، دشوار شود. ازاین‌رو، در تحلیل حقوقی، مسأله اصلی نه اثبات یک اقدام مشخص، بلکه تعیین میزان قابلیت پیش‌بینی، قابلیت کنترل و سهم تصمیم‌ساز در جریان تولید خروجی

[1] - علی پور،حسین؛ سلیمانپور،مهسا(1403)، تاثیر هوش مصنوعی بر حریم خصوصی و حقوق بشر در عصر دیجیتال، چهارمین کنفرانس بین المللی دانش و فناوری حقوق و علوم انسانی ایران،ص18

است. هرقدر فرایند تصمیم‌گیری پیچیده‌تر و خودکارتر باشد، فاصله میان رفتار انسانی و نتیجه افزایش یافته و بار اثباتی برای زیان‌دیده دشوارتر می‌شود.

در مرحله بعد، چالش انتساب با این پرسش پیوند می‌یابد که آیا خروجی سامانه، «تصمیم» محسوب می‌شود یا «اقدام واسط» که در نهایت به تصمیم انسانی منتهی شده است. اگر بهره‌بردار یا تصمیم‌گیرنده نهایی بدون ارزیابی مستقل به خروجی اتکا کند، نقش او در سلسله علّی تصمیم تقویت شده و فعل زیان‌بار به او قابل انتساب خواهد بود؛ زیرا عدم اعمال نظارت و قضاوت انسانی مصداق ترک فعل زیان‌بار است. اما اگر فرایند به‌صورت لایه‌ای طراحی شده باشد و خروجی صرفاً نقش مشورتی داشته باشد، انتساب بیش از پیش وابسته به میزان کنترل و دسترسی بهره‌بردار به سازوکارهای داخلی پردازش و امکان اصلاح نتایج است. بنابراین، در فرایندهای غیرمستقیم، انتساب فعل زیان‌بار نیازمند تحلیل دقیق ساختار تصمیم‌سازی، نقش انسان در زنجیره علت و معلول، و میزان توانایی او در پیشگیری از نتیجه زیان‌بار است؛ اموری که موجب می‌شود نظریه تقصیر کلاسیک به تنهایی کفایت نکند و رویکردهای نوین مبتنی بر «مسئولیت ناشی از خطر» و «مسئولیت مبتنی بر کنترل» اهمیت بیشتری یابند.

4-4-قابلیت اعمال نظریه مسئولیت محض و مسئولیت مبتنی بر خطر

قابلیت اعمال نظریه مسئولیت محض و مسئولیت مبتنی بر خطر در حوزه بهره‌برداری از سامانه‌های هوشمند، از آنجا قابل توجیه است که برخی از این فعالیت‌ها به‌طور ذاتی با سطحی از خطرات پیش‌بینی‌ناپذیر برای حقوق اشخاص، به‌ویژه حریم خصوصی و امنیت اطلاعات، همراه هستند و در بسیاری از موارد اثبات تقصیر بهره‌بردار برای زیان‌دیده دشوار یا حتی غیرممکن می‌شود. در چنین شرایطی، نظریه مسئولیت محض بر این مبنا استوار است که صرف تحقق ضرر ناشی از فعالیت خطرناک، بدون نیاز به اثبات تقصیر، برای ایجاد تعهد به جبران خسارت کافی است؛ زیرا شخص یا نهادی که از یک فعالیت فناورانه و پیچیده بهره‌برداری می‌کند، عملاً منافع اقتصادی آن را نیز در اختیار دارد و باید پیامدهای زیان‌بار احتمالی آن را بپذیرد. در کنار آن، نظریه مسئولیت مبتنی بر خطر نیز با تأکید بر ایجاد یا کنترل منبع خطر، بهره‌بردار یا سازمان اداره‌کننده سامانه را مسئول می‌داند، حتی اگر همه تدابیر متعارف احتیاطی را اتخاذ کرده باشد؛ زیرا معیار اصلی در این رویکرد، «ایجاد وضعیت

خطرزا» و «قدرت کنترل بر آن» است. بر این اساس، در مواردی که نقض حریم خصوصی یا ورود خسارت ناشی از کارکرد این سامانه‌ها به‌گونه‌ای رخ دهد که شناسایی تقصیر فردی دشوار باشد، توسل به این نظریه‌ها می‌تواند ابزار مؤثری برای حمایت از زیان‌دیدگان و تضمین جبران خسارت فراهم آورد.

4-5-جبران خسارت مادی و معنوی ناشی از تعرض به حریم خصوصی اشخاص

جبران خسارت مادی ناشی از تعرض به حریم خصوصی، ناظر بر زیان‌های مالی قابل اندازه‌گیری است که در نتیجه افشا، بهره‌برداری یا استفاده غیرمجاز از اطلاعات خصوصی به زیان‌دیده تحمیل می‌شود. این نوع خسارت می‌تواند شامل کاهش درآمد، از دست رفتن فرصت‌های شغلی یا تجاری، هزینه‌های مستقیم برای ترمیم پیامدهای نقض (مانند هزینه‌های حقوقی، فنی یا درمانی) و نیز خسارات ناشی از سوءاستفاده اشخاص ثالث از داده‌های افشاشده باشد. در تحلیل حقوقی، شرط اصلی جبران، احراز رابطه سببیت میان تعرض به حریم خصوصی و زیان مالی وارده است و دادرس می‌تواند با بهره‌گیری از امارات، نظر کارشناسی و اصل جبران کامل خسارت، میزان ضرر را تعیین نماید، حتی اگر محاسبه دقیق آن با دشواری همراه باشد.

در مقابل، خسارت معنوی ناشی از تعرض به حریم خصوصی به لطمه‌هایی اطلاق می‌شود که مستقیماً کرامت انسانی، آرامش روانی، حیثیت اجتماعی و احساس امنیت شخص را مخدوش می‌سازد و ماهیتی غیرمالی دارد. در این حوزه، صرف نقض حریم خصوصی، بدون نیاز به اثبات زیان مادی، می‌تواند موجب تحقق خسارت معنوی گردد؛ زیرا تعرض به زندگی خصوصی به‌خودی‌خود ناقض شأن و شخصیت فرد است. حقوق معاصر، با فاصله گرفتن از نگاه سنتی محدودکننده، جبران این نوع خسارت را به‌عنوان یکی از ابزارهای اساسی حمایت از حقوق شخصیت به رسمیت شناخته و امکان تعیین غرامت پولی، صدور حکم به عذرخواهی رسمی، اعاده حیثیت یا منع ادامه رفتار ناقض را فراهم کرده است.

افزون بر موارد مذکور، کارآمدی نظام جبران خسارت در نقض حریم خصوصی، در گرو پذیرش هم‌زمان جبران خسارت مادی و معنوی و تلفیق آن با تدابیر تکمیلی غیرمالی است. جبران صرف مالی، به‌ویژه در موارد خسارت معنوی گسترده یا نقض سیستماتیک حریم خصوصی، کفایت نمی‌کند و باید با ضمانت اجراهایی همچون دستور

حذف داده‌ها، توقف بهره‌برداری، الزام به اصلاح رویه‌ها و انتشار رأی همراه شود. چنین رویکردی، ضمن بازگرداندن وضعیت زیان‌دیده تا حد امکان، نقش بازدارنده مهمی در پیشگیری از تکرار تعرض به حریم خصوصی ایفا می‌کند و با هدف نهایی حمایت مؤثر از کرامت انسانی هم‌راستا است.[1]

5-خلأهای حقوقی، نقد نظام موجود و پیشنهادهای اصلاحی

5-1-ابهام در توزیع مسئولیت میان طراح، بهره‌بردار و نهاد ناظر

ابهام در توزیع مسئولیت میان طراح، بهره‌بردار و نهاد ناظر در حوزه سامانه‌های هوشمند، یکی از چالش‌های اساسی حقوق نوین مسئولیت مدنی است؛ زیرا زنجیره تصمیم‌سازی و اجرا در این سامانه‌ها به‌گونه‌ای پراکنده و چندمرحله‌ای است که تعیین منشأ دقیق رفتار زیان‌بار و سهم هر بازیگر در آن دشوار می‌گردد. طراح از یک‌سو مسئول کیفیت و ایمنی ساختار سامانه و پیش‌بینی پیامدهای احتمالی عملکرد آن است، در حالی‌که بهره‌بردار مستقیماً بر نحوه استفاده، تنظیمات و داده‌های ورودی کنترل دارد و از منافع اقتصادی آن بهره‌مند می‌شود. از سوی دیگر، نهاد ناظر وظیفه دارد از طریق مقررات‌گذاری و نظارت پیش‌گیرانه، چارچوب‌های فنی و اخلاقی حاکم بر کارکرد سامانه‌ها را تضمین نماید. با این حال، در عمل مرز مسئولیت‌ها هم‌پوشانی یافته و ضعف در یکی از این سطوح، آثار زیان‌بار را به دیگران منتقل می‌کند؛ به‌ویژه زمانی‌که فرآیند تصمیم‌گیری غیرشفاف یا توزیع‌شده است. در نتیجه، بدون تعیین دقیق معیارهایی چون «قدرت کنترل»، «نفع مستقیم» و «نقش در ایجاد خطر»، انتساب مسئولیت میان این سه رکن همواره با ابهام مواجه بوده و نیازمند تدوین نظام مسئولیت اشتراکی و سازوکارهای هم‌تکمیلی جبران خسارت است.

5-2-نارسایی قواعد سنتی اثبات دعوا در دعاوی مرتبط با حریم خصوصی

نارسایی قواعد سنتی اثبات دعوا در دعاوی مرتبط با حریم خصوصی عمدتاً ناشی از آن است که این قواعد بر مبنای روابط خطی، فعل انسانی قابل مشاهده و ادله کلاسیک شکل گرفته‌اند، در حالی‌که نقض حریم خصوصی

[1] - عاشوری کیسمی، محمدعلی(1403)، همگرایی حریم خصوصی و شفافیت، محدودیت های طراحی هوش مصنوعی حکمت و فلسفه، دوره20، شماره78،ص50

در محیط‌های دیجیتال عموماً در بستر فرایندهای پنهان، غیرمستقیم و فنی رخ می‌دهد و آثار آن نیز ممکن است با فاصله زمانی یا از طریق بازیگران متعدد ظاهر شود. در چنین وضعیتی، زیان‌دیده معمولاً به شواهد مستقیم، دسترسی فنی یا اطلاعات لازم برای اثبات وقوع تعرض، تعیین مرتکب، یا احراز رابطه سببیت دسترسی ندارد؛ زیرا بخش عمده داده‌ها، سوابق پردازش و مسیرهای تصمیم‌سازی در اختیار بهره‌بردار یا نهادهای واسط است. قواعد سنتی مانند «اصل برائت»، «قاعده البینه علی المدعی» یا ضرورت اثبات تقصیر مشخص، قادر به پاسخ‌گویی به این پیچیدگی نیستند و در عمل به زیان‌دیده تحمیل بار اثباتی ناممکن می‌کنند. ازاین‌رو، حقوق نوین نیازمند گذار به قواعدی مانند جابه‌جایی بار اثبات، پذیرش امارات فنی، مسئولیت مبتنی بر خطر، و الزام بهره‌بردار به ارائه شفاف‌سازی فنی است تا حمایت مؤثر از حریم خصوصی و جبران واقعی خسارت امکان‌پذیر شود.

نتیجه گیری

گسترش سامانه‌های هوشمند، به‌ویژه در حوزه‌های پردازش داده و تحلیل رفتار، نظم حقوقی سنتی حریم خصوصی را با چالش‌های بنیادین مواجه ساخته است. در این ساختار جدید، حریم خصوصی نه‌تنها متأثر از افشا یا دسترسی مستقیم، بلکه در معرض آسیب از طریق پردازش‌های پنهان، استنتاج داده‌ها و کارکردهای غیرمستقیم قرار می‌گیرد؛ امری که ضرورت بازتعریف این حق را در پرتو تحولات فناوری و اصول حقوق بشر ایجاب می‌کند. در حقوق معاصر، مبنای حمایت از حریم خصوصی همچنان کرامت انسانی و استقلال شخصی است، اما ابزارهای نقض چنان پیچیده شده که قواعد سنتی کفایت پاسداری از آن را ندارند. از منظر مسئولیت مدنی، صرف اتکا به نظریه تقصیر، کارآمدی لازم را در مواجهه با مخاطرات ناشی از سامانه‌های هوشمند ندارد؛ زیرا رفتار زیان‌بار غالباً در زنجیره‌ای از مراحل پردازش شکل می‌گیرد و تعیین مرتکب، احراز تقصیر و اثبات رابطه سببیت، بار اثباتی سنگینی بر زیان‌دیده تحمیل می‌کند. ازاین‌رو، نظام مسئولیت باید به‌سوی پذیرش الگوهای منعطف‌تری چون مسئولیت مبتنی بر خطر، مسئولیت محض و جابه‌جایی بار اثبات حرکت کند تا حمایت مؤثر از افراد و جبران واقعی خسارت امکان‌پذیر گردد.

مسأله انتساب مسئولیت نیز در این عرصه پیچیده‌تر شده است. طراح، بهره‌بردار و نهاد ناظر هر یک نقش متفاوت اما مرتبطی در ایجاد یا کنترل خطر دارند و تفکیک سهم آن‌ها صرفاً بر مبنای قواعد سنتی امکان‌پذیر نیست. معیارهایی همچون «درجه کنترل»، «نفع اقتصادی»، «نقش در ایجاد زمینه خطر» و «توانایی پیشگیری» باید مبنای تعیین مسئولیت قرار گیرند. این الگو می‌تواند به شکل‌گیری نظام مسئولیت توزیعی و چندسطحی منجر شود که با ماهیت تجزیه‌پذیر سامانه‌های هوشمند هم‌خوانی بیشتری دارد.

هم‌زمان، نظام جبران خسارت باید ظرفیت پوشش‌دهی هر دو نوع خسارت مادی و معنوی ناشی از نقض حریم خصوصی را داشته باشد. خسارت معنوی، که مستقیماً کرامت، آسایش روانی و حیثیت شخص را هدف قرار می‌دهد، در دعاوی مرتبط با حریم خصوصی جایگاهی محوری دارد و نمی‌توان آن را به حاشیه راند. علاوه بر جبران مالی، تدابیر غیرمالی مانند دستور حذف داده‌ها، اصلاح رویه‌ها، توقف بهره‌برداری و تضمین شفافیت می‌تواند نقش مکمل و بازدارنده مهمی ایفا کند.نظم حقوقی لازم است با پذیرش واقعیت‌های فنی و مخاطرات ساختاری سامانه‌های هوشمند، به‌سوی تنظیم‌گری هوشمند و ترکیبی حرکت کند؛ نظمی که در آن حق حریم خصوصی به‌عنوان یکی از حقوق بنیادین شخصیت انسانی، نه قربانی کارآمدی فناوری، بلکه معیاری برای مشروعیت و مقبولیت بهره‌برداری از فناوری پیشرفته باشد. تنها با چنین رویکردی است که می‌توان تعادلی پایدار میان نوآوری فناورانه و صیانت از حقوق بنیادین اشخاص برقرار ساخت.

منابع و مأخذ

- اصلانی، محسن؛ زمانی، سید قاسم؛ راعی، مسعود (1401)، ضمانت اجرای نقض تعهدات حقوق بشری دولت‌ها در حقوق بین الملل با رویکردی به فقه جزا، فصلنامه فقه جزای تطبیقی، دوره دوم، شماره چهارم
- باشی پور حقیقی،سیدامیر؛ شجاعیان،خدیجه؛ علایی،حسین(1403)، تاثیرگذاری هوش مصنوعی برحق بر حریم خصوصی بیماران با تاکید بر چالش ها و خلاها، مجله حقوق پزشکی، دوره هجدهم
- بنافی، فرشته (1402)، حفاظت از حق حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی، نشریه پژوهش حقوق خصوصی، دوره 12، شماره 45

- بهبودی، عادله (1401)، هوش مصنوعی در امنیت سایبری، پانزدهمین کنفرانس بین المللی فناوری اطلاعات، کامپیوتر و مخابرات
- حکمت نیا،محمود؛ محمدی، مرتضی؛ واثقی، محسن(1398)، مسئولیت مدنی ناشی از تولید ربات‌های مبتنی بر هوش مصنوعی خودمختار، نشریه حقوق اسلامی،دوره16، شماره60
- عاشوری کیسمی، محمدعلی(1403)، همگرایی حریم خصوصی و شفافیت، محدودیت های طراحی هوش مصنوعی حکمت و فلسفه، دوره20، شماره78
- علی پور،حسین؛ سلیمانپور،مهسا(1403)، تاثیر هوش مصنوعی بر حریم خصوصی و حقوق بشر در عصر دیجیتال، چهارمین کنفرانس بین المللی دانش و فناوری حقوق و علوم انسانی ایران
- فهیمی کبیر، شیرین(1404)، بررسی حریم خصوصی و حفاظت از داده ها در عصر هوش مصنوعی، فصلنامه علمی مطالعات حقوق و علوم قضایی، سال دوم، شماره4
- مرتضوی،سیدمرتضی؛ خدایی فام،حجت(1404)، بررسی آثار به کارگیری هوش مصنوعی بر حریم خصوصی اشخاص و مسئولیت مدنی ناشی از آن، سال ششم، شماره22
- مکی، اکرم السادات؛ مکی، زهرا السادات؛ کشکولیان، اسماعیل(1403)، بررسی مسئولیت ناشی از اعمال هوش مصنوعی در نظام حقوقی ایران، نشریه علمی فقه، حقوق و علوم جزا، سال هشتم، شماره32
- میرشکاری،عباس؛ ثابت قدم،فاطمه؛ اصغرنیا،مرتضی(1403)، درآمدی بر چالش های فناوری هوش مصنوعی در حوزه حریم خصوصی، فصلنامه علمی مطالعات حقوقی فضای مجازی، سال سوم،شماره چهارم.

Abstract

The rapid expansion of artificial intelligence technologies and their increasing application in various fields of decision-making, monitoring, and data processing have raised new legal concerns regarding the protection of privacy. By enabling the collection, analysis, and use of personal data, artificial intelligence systems significantly increase the potential for interference with individuals' privacy, thereby intensifying the need to define the scope and basis of legal responsibility borne by natural and legal persons involved in the development, deployment, or supervision of such systems. This study adopts a descriptive–analytical approach to examine the legal foundations governing the obligations and duties associated with the use of intelligent systems in relation to personal data, and to clarify the position of civil liability arising from violations of privacy rules. The findings indicate that the automated nature of these processes, the extensive scale of data collection, and the difficulties in establishing fault pose serious challenges to traditional liability regimes, making it necessary to revise existing legal rules or develop new legal frameworks in order to ensure effective protection of individuals' privacy.

Keywords: Artificial Intelligence, Privacy, Personal Data, Civil Liability, Legal Protection.