Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

بررسی آثار به‌کارگیری هوش مصنوعی بر حریم خصوصی اشخاص و مسئولیت مدنی ناشی از آن

سیدمرتضی‌مرتضوی(نویسنده مسئول) دانش آموخته کارشناسی ارشد، حقوق خصوصی، دانشگاه قم، ایران

دکتر حجت خدائی فام گروه حقوق، واحد ارومیه، دانشگاه آزاد اسلامی، ارومیه، ایران

فصلنامه علمی فقه و حقوق نوین

Print ISSN: 2717- 1469
Online ISSN: 2717 – 1477

ISC.SID.NOORMAGZ.MAGIRAN
GOOGLESCHOLAR.ENSANI
www.jaml .ir

سال ۱۴۰۴، سال ششم، شماره ۲۲،
صفحات ۱۵-۱

چکیده

باتوسعه روزافزون فناوری هوش مصنوعی، ابزارهای نوین داده‌کاوی و تحلیل اطلاعات، تحول چشمگیری در شیوه‌های جمع‌آوری، پردازش و بهره‌برداری از داده‌های شخصی پدید آمده است. این تحول، در کنار فرصت‌های قابل توجه، چالش‌هایی بنیادین برای حفظ حریم خصوصی افراد ایجاد کرده است. هوش مصنوعی از طریق تحلیل کلان‌داده‌ها، ردیابی الگوهای رفتاری و پردازش اطلاعات حساس، ممکن است موجب نقض حقوق شخصی اشخاص شود. در این میان، پرسش اساسی آن است که در صورت ورود لطمه به حریم خصوصی افراد توسط سیستم‌های مبتنی بر هوش مصنوعی، چه کسی مسئول جبران خسارت خواهد بود؟ آیا مسئولیت بر عهده تولیدکننده نرم‌افزار است یا بهره‌بردار سیستم؟ مقاله حاضر با تبیین ابعاد مختلف حریم خصوصی در نظام حقوقی و بررسی مبانی مسئولیت مدنی، تلاش دارد تا چارچوبی برای تعیین مسئولیت حقوقی در این حوزه نوظهور ارائه نماید و به ضرورت اصلاح و تکمیل قوانین در مواجهه با چالش‌های حقوقی هوش مصنوعی بپردازد

واژگان کلیدی: هوش مصنوعی، حریم خصوصی، داده‌های شخصی، مسئولیت مدنی، حقوق فناوری، حفاظت اطلاعات، جبران خسارت

طبقه‌بندی JEL: فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Studying the effects of using artificial intelligence on individuals' privacy and the resulting civil liability

Scientific Journal of Modern Jurisprudence and Law

Print ISSN: 2717- 1469
Online ISSN: 2717 - 1477

Profile in ISC,SID, Noormags, Magiran, Ensani, GoogleScholar
www.jaml .ir

Year 2025، Sixth year ,Issue 22

Pages 1-15

Seyed Morteza Mortazavi (Responsible Author) — Master's degree in private law, University of Qom, Iran

Dr. Hojat Khodaifam — Department of Law, Urmia Branch, Islamic Azad University, Urmia, Iran

Abstract

With the increasing development of artificial intelligence technology, new data mining and information analysis tools, a significant change has occurred in the methods of collecting, processing and utilizing personal data. This change, along with significant opportunities, has created fundamental challenges for protecting individuals' privacy. Artificial intelligence may violate the personal rights of individuals through big data analysis, tracking behavioral patterns and processing sensitive information. In the meantime, the fundamental question is: who will be responsible for compensation if individuals' privacy is harmed by artificial intelligence-based systems? Is the responsibility the responsibility of the software producer or the system operator? By explaining the various dimensions of privacy in the legal system and examining the foundations of civil liability, this article attempts to provide a framework for determining legal liability in this emerging field and addresses the need to amend and supplement laws in the face of legal challenges of artificial intelligence.

Keywords: Artificial Intelligence, Privacy, Personal Data, Civil Liability, Technology Law, Information Protection, Compensation

JEL Classification: Jurisprudence - Law - Criminal and Criminology - International Law - Private Law

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

مقدمه

با گسترش فناوری‌های نوین، به‌ویژه هوش مصنوعی، الگوی تعامل انسان با داده‌ها و اطلاعات به‌طور بنیادین دگرگون شده است. سامانه‌های هوشمند با قابلیت تحلیل حجم وسیعی از اطلاعات، نقش پررنگی در تصمیم‌گیری‌های خودکار، نظارت، و حتی پیش‌بینی رفتارهای انسانی یافته‌اند. این تحول، در عین حال که تسهیلات فراوانی را برای افراد و نهادها فراهم کرده، موجب نگرانی‌های عمیقی در خصوص حفظ حریم خصوصی اشخاص نیز شده است. حریم خصوصی که یکی از اصول اساسی حقوق بشری به شمار می‌رود، در مواجهه با ابزارهای پیشرفته تحلیل داده و قابلیت‌های نفوذپذیر هوش مصنوعی، بیش از هر زمان دیگر در معرض تهدید قرار دارد.از سوی دیگر، هنگامی که فناوری‌های هوشمند موجب ورود آسیب به حریم خصوصی افراد می‌شوند، مسئولیت حقوقی ناشی از این لطمه، با ابهاماتی مواجه است. در چنین مواردی، شناسایی شخص یا نهادی که باید پاسخگوی خسارت باشد – چه تولیدکننده، چه بهره‌بردار و چه توسعه‌دهنده فناوری – پرسشی جدی و پیچیده در حوزه مسئولیت مدنی به شمار می‌رود. نظام‌های حقوقی در سراسر جهان در تلاش‌اند تا با بازنگری در مفاهیم سنتی مسئولیت و تطبیق آن با شرایط نوین فناورانه، پاسخی کارآمد به این چالش ارائه دهند. سعی می‌شود در این مقاله، با نگاهی تحلیلی به آثار به‌کارگیری هوش مصنوعی بر حریم خصوصی، ابعاد مختلف مسئولیت مدنی ناشی از آن بررسی گردد و چارچوبی حقوقی برای پاسخگویی مناسب به این پدیده نوظهور پیشنهاد شود.

۱-۱-تعریف و ماهیت هوش مصنوعی از منظر حقوقی

هوش مصنوعی در معنای عمومی به سیستم‌هایی اطلاق می‌شود که با بهره‌گیری از الگوریتم‌ها و داده‌ها قادرند عملکردهایی مشابه رفتار انسانی مانند یادگیری، استدلال، تصمیم‌گیری و حل مسئله را انجام دهند. از منظر حقوقی، هوش مصنوعی نه صرفاً یک ابزار تکنولوژیک، بلکه پدیده‌ای چندبعدی است که دارای آثار حقوقی در حوزه‌های مختلف از جمله مالکیت فکری، مسئولیت مدنی، داده‌های شخصی و حتی شخصیت حقوقی است. در چارچوب حقوق، شناخت ماهیت هوش مصنوعی اهمیت ویژه‌ای دارد، زیرا بر اساس همین شناخت است که می‌توان وضعیت حقوقی کنش‌های آن را تحلیل و ارزیابی کرد.[۱]

از آنجا که هوش مصنوعی، به ویژه در شکل پیشرفته خود (مانند یادگیری ماشین و یادگیری عمیق)، قابلیت اتخاذ تصمیم بدون دخالت مستقیم انسان را دارد، پرسش‌هایی اساسی در حوزه مسئولیت، تعهد، و نظارت بر آن مطرح می‌شود. حقوق‌دانان در تلاش‌اند تا مشخص کنند آیا می‌توان برای سامانه‌های هوشمند شخصیت حقوقی قائل شد یا باید همواره مسئولیت اعمال آن‌ها را به انسان یا نهادهای بهره‌بردار منتسب کرد. بنابراین، ماهیت حقوقی هوش مصنوعی مستقیماً با مفاهیم بنیادینی چون مسئولیت، قصد، و اراده در تعامل است و شناخت آن مقدمه‌ای ضروری برای تنظیم قواعد حقوقی کارآمد در این حوزه به شمار می‌رود.[۲]

۱-۲-سیر تحول تاریخی هوش مصنوعی و تأثیر آن بر نظام‌های حقوقی

هوش مصنوعی به‌عنوان شاخه‌ای از علوم رایانه، نخستین بار در دهه ۱۹۵۰ میلادی به‌صورت رسمی مطرح شد، زمانی که پژوهشگرانی همچون آلن تورینگ و جان مک‌کارتی، امکان

[۱] - انصاری، باقر و همکاران(۱۴۰۰)، حقوق داده‌ها و هوش مصنوعی، تهران: شرکت سهامی انتشار،ص۵۶

[۲] - بیات، معصومه (۱۳۹۹)، حقوق بشر و فناوری‌های نوین: چالش‌ها و راهکارها، چاپ اول، تهران: نشر میزان،ص۲۵

شبیه‌سازی تفکر انسانی توسط ماشین‌ها را بررسی کردند. در دهه‌های بعد، به‌ویژه از دهه ۱۹۸۰ به بعد، با گسترش ظرفیت‌های پردازشی و ظهور شبکه‌های عصبی مصنوعی، زمینه برای توسعه سیستم‌های پیچیده‌تر فراهم شد. ورود الگوریتم‌های یادگیری ماشین و کلان‌داده‌ها در قرن ۲۱، موجب جهش چشمگیری در عملکرد هوش مصنوعی شد؛ به‌گونه‌ای که امروز این فناوری نه‌تنها در حوزه‌های علمی و صنعتی، بلکه در امور روزمره، قضایی، تجاری، پزشکی و امنیتی نیز نقشی فزاینده دارد.[۱]

با این تحولات، نظام‌های حقوقی نیز ناگزیر به بازنگری در ساختار و مفاهیم خود شده‌اند. سامانه‌های هوشمند با قدرت تحلیل و تصمیم‌گیری مستقل، مرزهای سنتی مسئولیت، اهلیت، قصد، و حتی علیت را به چالش کشیده‌اند. به‌عنوان مثال، تعیین مسئولیت در صورت وقوع خطا یا خسارت ناشی از تصمیم یک الگوریتم، یا حمایت از داده‌های شخصی که توسط سامانه‌های خودکار جمع‌آوری می‌شود، مستلزم تعریف‌های نو و قواعد ویژه‌ای است. این روند سبب شده تا بسیاری از نظام‌های حقوقی به‌سوی قانون‌گذاری مستقل برای هوش مصنوعی حرکت کنند و تلاش کنند تا با درک دقیق ماهیت این پدیده، چارچوب‌های حقوقی متناسبی برای مدیریت آن ارائه دهند.[۲]

۱-۳-جایگاه حق بر حریم خصوصی در نظام حقوق بشر

حق بر حریم خصوصی یکی از حقوق بنیادین بشر و از ارکان اساسی کرامت انسانی است که در اسناد معتبر بین‌المللی حقوق بشر مورد شناسایی قرار گرفته است. ماده ۱۲ اعلامیه جهانی حقوق بشر (۱۹۴۸) و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶) صراحتاً هرگونه مداخله خودسرانه در زندگی خصوصی، خانواده، اقامتگاه یا مکاتبات اشخاص را ممنوع دانسته‌اند. این حق در نظام‌های حقوقی ملی نیز به اشکال مختلف تضمین شده است و کشورها موظف‌اند از آن در برابر تعرض نهادهای عمومی و خصوصی حمایت کنند. مفهوم حریم خصوصی در این اسناد، تنها محدود به فضا یا مکان فیزیکی نیست، بلکه شامل اطلاعات شخصی، ارتباطات و تصمیمات فردی نیز می‌شود.[۳]

در حقوق بشر معاصر، حریم خصوصی به‌عنوان حقی مستقل و غیرقابل تقلیل تلقی می‌شود که با سایر حقوق از جمله آزادی بیان، آزادی اطلاعات، و امنیت فردی در تعارض یا توازن قرار می‌گیرد. با پیشرفت فناوری‌های دیجیتال، از جمله هوش مصنوعی، اهمیت این حق دوچندان شده است؛ زیرا ابزارهای نوین به‌راحتی قادرند داده‌های حساس افراد را شناسایی، ذخیره، تحلیل و منتشر کنند. از این رو، نهادهای حقوق بشری و دیوان‌های بین‌المللی بر لزوم شفافیت، کنترل انسانی، و نظارت مؤثر بر فرایندهای پردازش داده‌ها تأکید دارند تا از خدشه‌دار شدن این حق جلوگیری شود. بنابراین، حق بر حریم خصوصی در نظام حقوق بشر نه تنها جایگاهی تثبیت‌شده دارد، بلکه مستلزم تفسیر پویا و متناسب با تحولات فناورانه نیز هست.[۴]

۱-۴-نقش هوش مصنوعی در تهدید حریم خصوصی

هوش مصنوعی با توانایی‌های پیشرفته خود در پردازش داده‌ها و تحلیل رفتارهای انسانی، به یکی از ابزارهای قدرتمند در

---

[۱] - زاورنیک، آلاش(۱۴۰۰)، عدالت کیفری، سیستم‌های هوش مصنوعی و ملاحظات حقوق بشری، تهران: انتشارات میزان،ص۷۲

[۲] - عباسی، محمود (۱۳۹۹)، هوش مصنوعی و حقوق: چالش‌ها و فرصت‌ها، چاپ اول، تهران: نشر میزان،ص۵۱

[۳] - محمدی، حمیدرضا (۱۴۰۰)، فناوری‌های نوین و حقوق بشر، چاپ اول، تهران: انتشارات جنگل،ص۹۳

[۴] - ابن علی، آرش (۱۴۰۰)، جرم انگاری دیپ فیک‌ها از منظر تعهدات حقوق بشری دولت‌ها، مجله تحقیقات حقوق قضایی، دوره دوم، شماره ۳، صص ۳۷۴

جمع‌آوری و تجزیه‌وتحلیل اطلاعات شخصی تبدیل شده است. این تکنولوژی می‌تواند از طریق جمع‌آوری و ذخیره‌سازی داده‌های حساس افراد، نظیر اطلاعات مالی، بهداشتی، جغرافیایی و شخصی، حریم خصوصی افراد را تهدید کند. به‌ویژه در زمینه‌هایی چون شناسایی چهره، پیش‌بینی رفتار، و تحلیل داده‌های آنلاین، هوش مصنوعی قادر است بدون اطلاع و رضایت کامل افراد، اطلاعات شخصی آنان را استخراج کرده و در معرض خطر قرار دهد. این تهدیدات، که بیشتر در بستر اینترنت و شبکه‌های اجتماعی بروز می‌یابند، می‌توانند باعث نقض حریم خصوصی افراد شوند و آسیب‌های جدی به امنیت و آزادی‌های فردی وارد آورند.[1]

از منظر حقوقی، با توجه به قدرت تحلیل و تصمیم‌گیری خودکار این سیستم‌ها، مسئولیت‌پذیری در برابر نقض حریم خصوصی به چالشی پیچیده تبدیل شده است. در حالی که داده‌های شخصی به‌طور فزاینده‌ای در دست سامانه‌های هوشمند قرار دارند، قوانین موجود در بسیاری از کشورها هنوز قادر به پاسخگویی به پیچیدگی‌های ناشی از فناوری‌های نوین نیستند. بنابراین، ضرورت دارد که نهادهای قانونی و حقوقی قوانین مربوط به حفاظت از داده‌ها و حریم خصوصی را به‌طور خاص و متناسب با شرایط جدید، بازنگری و تکمیل کنند تا از نقض حقوق افراد و سوءاستفاده از اطلاعات شخصی جلوگیری به عمل آید.

۲- ابعاد حقوقی نقض حریم خصوصی در بستر هوش مصنوعی

نقض حریم خصوصی در بستر هوش مصنوعی از جنبه‌های مختلف حقوقی قابل بررسی است. نخستین بعد، مسئولیت مدنی است که در آن باید مشخص شود در صورت نقض حریم خصوصی افراد از سوی سامانه‌های هوش مصنوعی، چه کسی باید مسئول جبران خسارت باشد. آیا این مسئولیت متوجه توسعه‌دهندگان این فناوری‌ها است که ممکن است بدون در نظر گرفتن حقوق کاربران، داده‌های شخصی را جمع‌آوری و پردازش کنند؟ یا اینکه مسئولیت بر عهده استفاده‌کنندگان از این فناوری‌هاست که ممکن است بدون توجه به قوانین، از این داده‌ها به‌طور نادرست استفاده کنند؟ در این راستا، بسیاری از کشورها هنوز به قوانین و مقررات مشخصی برای شناسایی مسئولیت‌ها در چنین مواردی دست نیافته‌اند. دومین بعد حقوقی، حفاظت از داده‌های شخصی است. در دنیای دیجیتال و با ظهور هوش مصنوعی، داده‌های شخصی افراد به راحتی می‌تواند بدون رضایت آگاهانه و یا آگاهی کامل، جمع‌آوری و ذخیره‌سازی شود. این امر می‌تواند به نقض حریم خصوصی منجر شده و حقوق افراد را به خطر بیندازد. از این رو، بسیاری از کشورهای پیشرفته نظیر اتحادیه اروپا با مقرراتی همچون مقررات عمومی حفاظت از داده اتحادیه اروپا[2]، قوانین خاصی برای حفاظت از داده‌های شخصی وضع کرده‌اند تا از سوءاستفاده از اطلاعات افراد جلوگیری کنند. در این زمینه، کشورها موظفند که نظارت دقیقی بر نحوه استفاده از این داده‌ها داشته باشند و از امنیت اطلاعات افراد محافظت کنند.[3]

---

[1] - حکمت نیا،محمود و همکاران (۱۳۹۸)، مسئولیت مدنی ناشی از تولید ربات‌های مبتنی بر هوش مصنوعی خودمختار، نشریه حقوق اسلامی،دوره۱۶، شماره۶۰، ص۲۴۲

[2] - The General Data Protection Regulation (GDPR) (EU) 2016/679

[3] - سالاری، سپیده(۱۴۰۰)، رویکرد حقوق کیفری ایران و انگلستان به مسئولیت ناشی از هوش مصنوعی، پایان نامه جهت دریافت درجه کارشناسی ارشد، دانشگاه شهید بهشتی،ص۵۱

سومین بعد، تضاد بین حقوق فردی و منافع عمومی است. استفاده از هوش مصنوعی می‌تواند منافع عمومی مانند امنیت اجتماعی یا بهبود خدمات عمومی را تسهیل کند، اما این امر ممکن است به نقض حریم خصوصی افراد منجر شود. مثلاً استفاده از فناوری‌های نظارت هوشمند یا تجزیه‌وتحلیل رفتارهای فردی می‌تواند در جهت منافع عمومی مورد استفاده قرار گیرد، اما ممکن است موجب نقض حریم خصوصی افراد و سوءاستفاده از داده‌های شخصی شود. بنابراین، نیاز به توازن میان این حقوق و منافع وجود دارد.[1]

در نهایت، برای پاسخگویی به این چالش‌ها، نظام‌های حقوقی باید قوانین و مقررات جدیدی را تدوین کرده یا قوانین موجود را به‌روزرسانی کنند تا از یک سو از حقوق افراد در برابر نقض حریم خصوصی توسط فناوری‌های هوش مصنوعی محافظت کنند و از سوی دیگر زمینه را برای بهره‌برداری قانونی و اخلاقی از این فناوری‌ها فراهم سازند.

۲-۱-پردازش و بهره‌برداری از داده‌های شخصی توسط سامانه‌های هوشمند

پردازش و بهره‌برداری از داده‌های شخصی توسط سامانه‌های هوشمند، در بسیاری از کشورها تحت قوانین سخت‌گیرانه‌ای قرار دارد تا از نقض حریم خصوصی افراد جلوگیری شود. بر اساس ماده ۲۱ اعلامیه جهانی حقوق بشر، هر فردی حق دارد که از دخالت خودسرانه در زندگی خصوصی‌اش محافظت کند، و این حق در بسیاری از اسناد بین‌المللی مانند ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶) نیز مورد تأکید قرار گرفته است. در اروپا، قانون حفاظت از داده‌های عمومی، به‌عنوان یکی از مهم‌ترین قوانین بین‌المللی در این حوزه، شرایط و اصول دقیقی را برای جمع‌آوری، پردازش و نگهداری داده‌های شخصی افراد تعیین کرده است. این قانون، پردازش داده‌ها را تنها در صورت رضایت آگاهانه و آزادانه افراد مجاز می‌داند و برای داده‌های حساس، محدودیت‌های خاصی در نظر گرفته است. در ایران، قانون حمایت از حقوق مصرف‌کنندگان در فضای مجازی و قانون جرم‌یابی داده‌ها و اطلاعات به‌طور غیرمستقیم به حفاظت از داده‌های شخصی پرداخته‌اند، هرچند که هنوز قانونی جامع و دقیق در این زمینه وجود ندارد. به‌طور کلی، پردازش و بهره‌برداری از داده‌های شخصی باید به گونه‌ای انجام گیرد که حق حریم خصوصی افراد نقض نشود و این امر مستلزم شفافیت، رضایت آگاهانه، و نظارت دقیق بر فرآیندهای پردازش است.[2]

۲-۲-فقدان رضایت آگاهانه و تهدید به استقلال اطلاعاتی اشخاص

فقدان رضایت آگاهانه و تهدید به استقلال اطلاعاتی اشخاص یکی از چالش‌های اصلی در استفاده از سامانه‌های هوش مصنوعی و پردازش داده‌های شخصی است. طبق ماده ۲۱ اعلامیه جهانی حقوق بشر، هر فرد حق دارد که از دخالت‌های خودسرانه در زندگی خصوصی‌اش محافظت شود و برای پردازش داده‌های شخصی، باید رضایت آزادانه و آگاهانه وی جلب شود. در قانون حمایت از داده‌های شخصی اتحادیه اروپا نیز، اصل رضایت آگاهانه به‌طور خاص مورد تأکید قرار گرفته است. به موجب ماده ۷ این قانون، هر پردازش داده‌ای باید تنها با رضایت صریح و آگاهانه فرد صورت گیرد و فرد باید از تمامی اطلاعات مربوط به پردازش داده‌ها از جمله اهداف پردازش و مدت زمان نگهداری اطلاعات آگاه باشد.

[1] -همان منبع،ص۵۲

[2] - انصاری، باقر و همکاران(۱۴۰۰)، حقوق داده‌ها و هوش مصنوعی، تهران: شرکت سهامی انتشار،ص۶۴

در صورتی که رضایت آگاهانه وجود نداشته باشد، پردازش داده‌های شخصی به‌طور غیرقانونی انجام می‌شود و این امر می‌تواند استقلال اطلاعاتی افراد را تهدید کند. فقدان این رضایت موجب می‌شود که افراد نتوانند کنترل کاملی بر روی اطلاعات شخصی خود داشته باشند و در نتیجه، احتمال سوءاستفاده از داده‌ها یا انتشار غیرمجاز آن‌ها افزایش یابد. در ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶) نیز به‌طور خاص به حق افراد برای حفاظت از حریم خصوصی و اطلاعات شخصی‌شان اشاره شده است. در سیستم‌های هوش مصنوعی، به‌ویژه زمانی که داده‌ها بدون آگاهی کامل و رضایت افراد پردازش می‌شوند، این حق نقض شده و تهدیدی برای استقلال اطلاعاتی و حریم خصوصی افراد ایجاد می‌شود. این تهدیدات به دلیل قابلیت‌های پیشرفته فناوری‌ها در جمع‌آوری، تحلیل و اشتراک‌گذاری داده‌ها، نیازمند تدابیر و نظارت‌های قانونی مؤثر هستند تا از حقوق بنیادین افراد در برابر سوءاستفاده‌های احتمالی محافظت شود.[۱]

۲-۳-افشای ناخواسته اطلاعات در سامانه‌های مرتبط با هوش مصنوعی

افشای ناخواسته اطلاعات در سامانه‌های هوش مصنوعی یکی از مشکلات عمده در دنیای دیجیتال است که به‌ویژه در زمینه پردازش داده‌های شخصی و حساس اهمیت ویژه‌ای دارد. سامانه‌های هوش مصنوعی که قادر به جمع‌آوری و تحلیل حجم زیادی از اطلاعات هستند، می‌توانند در فرآیند پردازش این داده‌ها به‌طور غیرمجاز یا تصادفی اطلاعات شخصی افراد را افشا کنند. این امر ممکن است به دلیل خطا در الگوریتم‌ها، نقص در تنظیمات امنیتی یا حتی اشتباهات انسانی در فرایندهای پردازش داده‌ها رخ دهد.[۲]

یک مثال از افشای ناخواسته اطلاعات در سامانه‌های هوش مصنوعی، رخ دادن اشتباه در سامانه‌های شناسایی چهره است. به‌عنوان مثال، ممکن است این سیستم‌ها بدون رضایت فرد یا در شرایطی نادرست، اطلاعات شخصی فرد را شناسایی کرده و آن‌ها را در دسترس اشخاص ثالث قرار دهند. در این خصوص، قانون حفاظت از داده‌های عمومی اتحادیه اروپا در ماده ۳۳ خود تصریح کرده است که در صورت افشای غیرمجاز داده‌ها، باید بلافاصله مقامات نظارتی و افراد مورد نظر از این موضوع مطلع شوند. این افشای ناخواسته نه تنها می‌تواند موجب نقض حریم خصوصی افراد شود، بلکه می‌تواند آسیب‌های اجتماعی و اقتصادی جبران‌ناپذیری را برای آنان به همراه داشته باشد.

در سطح بین‌المللی، ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹۶۶) نیز بر این نکته تأکید دارد که هر فرد حق دارد که از دخالت غیرمجاز در زندگی خصوصی‌اش محافظت شود و این شامل حفاظت از داده‌های شخصی او نیز می‌شود. این ماده به‌طور صریح، افشای ناخواسته و غیرقانونی اطلاعات را نقض حقوق فردی و شخصی افراد می‌داند. در ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ نیز به‌طور غیرمستقیم به موضوع افشای اطلاعات اشاره دارد و مقرر می‌دارد که هرگونه دسترسی غیرمجاز به داده‌های شخصی و انتشار آن‌ها تخلف است و فرد یا نهاد مسئول باید پاسخگو باشد.[۳]

[۱] - شیرزاد، کامران (۱۳۹۹)، مسئولیت کیفری صاحبان هوش مصنوعی در حقوق ایران و حقوق بین‌الملل، رساله دکتری تخصصی، دانشگاه عدالت،ص۸۶

[۲] - شفیعی، شیما (۱۴۰۲)، نقش هوش مصنوعی در پیشگیری از جرم، رساله دکتری تخصصی، دانشگاه شهید بهشتی،ص۴۹

[۳] - مولوی، حانیه (۱۴۰۲)، مطالعه چالش‌های حقوق بشری هوش مصنوعی، پنجمین کنفرانس بین المللی علوم انسانی، حقوق، مطالعات اجتماعی و روانشناسی، ص۱۹

در نهایت، به‌منظور جلوگیری از چنین افشاهایی، سامانه‌های هوش مصنوعی باید از تدابیر امنیتی و حفاظتی لازم برخوردار باشند تا هیچ‌گونه افشای غیرمجاز داده‌ها رخ ندهد و حقوق حریم خصوصی افراد حفظ شود.

۲-۴-تحلیل تهدیدات امنیتی: نشت، هک، سوءاستفاده از داده‌های کاربران

با توجه به گسترش استفاده از سامانه‌های هوش مصنوعی و پردازش داده‌های شخصی در دنیای دیجیتال، تهدیدات امنیتی مربوط به نشت، هک و سوءاستفاده از داده‌های کاربران، یکی از مهم‌ترین چالش‌ها در حفظ حریم خصوصی و امنیت اطلاعات افراد به شمار می‌روند. این تهدیدات می‌توانند به‌طور جدی حقوق فردی را نقض کنند و منجر به پیامدهای حقوقی، اجتماعی و اقتصادی گسترده‌ای شوند. در این زمینه، هر یک از این تهدیدات به شیوه‌های خاص خود ممکن است به افشای غیرمجاز اطلاعات حساس کاربران منجر شود و آسیب‌های جدی به اعتبار و امنیت افراد وارد کند.

یکی از مهم‌ترین تهدیدات، نشت داده‌ها است که زمانی رخ می‌دهد که اطلاعات حساس کاربران به‌طور غیرمجاز و بدون اطلاع یا رضایت آن‌ها در اختیار افراد یا نهادهای غیرمجاز قرار می‌گیرد. به‌عنوان مثال، در ایران در سال ۱۳۹۸، حمله به سامانه سایت‌های خرید آنلاین و نشت اطلاعات بیش از یک میلیون کاربر در فضای مجازی رخ داد. در این واقعه، اطلاعات خصوصی افراد از جمله نام، آدرس، شماره تماس و جزئیات خریدهای آنلاین آن‌ها به‌طور غیرمجاز در اختیار هکرها قرار گرفت. این نشت داده‌ها نه تنها حریم خصوصی افراد را نقض کرد، بلکه موجب از دست رفتن اعتماد کاربران به این نوع پلتفرم‌ها شد. در همین راستا، قانون جرایم رایانه‌ای ایران به‌طور صریح از حفاظت از داده‌های شخصی کاربران حمایت می‌کند و سازمان‌ها و نهادها را موظف به رعایت اصول امنیتی در مدیریت داده‌ها می‌سازد.[۱]

هک سیستم‌ها نیز یکی از تهدیدات عمده است که در آن هکرها می‌توانند به سامانه‌های ذخیره‌سازی داده‌ها نفوذ کنند و اطلاعات حساس مانند شماره کارت‌های اعتباری، سوابق پزشکی و اطلاعات هویتی افراد را به سرقت برند. در یکی از حملات معروف در ایران، در سال ۱۳۹۶، اطلاعات مربوط به کاربران بانک‌های دولتی در نتیجه حمله به یکی از سیستم‌های بانکداری الکترونیک کشور، به‌طور گسترده منتشر شد. این حمله به اطلاعات خصوصی میلیون‌ها ایرانی آسیب وارد کرد و به کاربران آسیب‌های مالی زیادی وارد شد.

سوءاستفاده از داده‌ها نیز تهدید دیگری است که در آن اطلاعات شخصی افراد برای اهداف غیرقانونی یا بدون اطلاع‌رسانی و رضایت آنها مورد استفاده قرار می‌گیرد. در یکی از نمونه‌های ایران، در برخی از شرکت‌های تبلیغاتی، اطلاعات مربوط به رفتار آنلاین و ترجیحات خرید کاربران بدون اطلاع آن‌ها جمع‌آوری می‌شود و برای تبلیغات هدفمند استفاده می‌شود. این نوع سوءاستفاده از داده‌ها می‌تواند منجر به دسترسی غیرمجاز به اطلاعات حساس و استفاده نادرست از آن‌ها گردد. قانون حمایت از حقوق مصرف‌کنندگان در فضای مجازی در ایران به‌طور غیرمستقیم به این موضوع پرداخته است و بر رعایت حقوق کاربران در جمع‌آوری و پردازش داده‌ها تأکید دارد.[۲]

---

[۱] - فراهانی، عاطفه؛ میرزاده کوهشاهی، نادر (۱۴۰۱)، هوش مصنوعی و نقض حقوق بشر و مسئولیت آن، نهمین همایش ملی مطالعات و تحقیقات نوین در حوزه علوم انسانی، مدیریت و کارافرینی ایران، ص۱۵

[۲] - بنافی، فرشته (۱۴۰۲)، حفاظت از حق حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی، نشریه پژوهش حقوق خصوصی، دوره ۱۲، شماره ۴۵، ص۱۵۲

در مجموع، نشت، هک و سوءاستفاده از داده‌های کاربران تهدیداتی جدی برای حریم خصوصی و امنیت اطلاعات افراد هستند. برای مقابله با این تهدیدات، نیاز به تقویت تدابیر امنیتی، به‌روزرسانی قوانین و نظارت دقیق بر فرآیندهای پردازش داده‌ها وجود دارد تا حقوق افراد به‌طور کامل محافظت شود.

۳-ارکان و حدود مسئولیت مدنی ناشی از نقض حریم خصوصی توسط فناوری‌های هوشمند

مسئولیت مدنی ناشی از نقض حریم خصوصی توسط فناوری‌های هوشمند شامل سه ارکان اصلی است: ضرر، فعل زیان‌بار و رابطه سببیت. برای اثبات مسئولیت مدنی، ابتدا باید ثابت شود که شخص زیان‌دیده دچار ضرر مادی یا معنوی شده است. این ضرر می‌تواند شامل از دست دادن داده‌های شخصی، افشای غیرمجاز اطلاعات یا آسیب به اعتبار فرد باشد. در گام بعدی، باید اثبات شود که فعل زیان‌بار از سوی شخص مسئول، اعم از شرکت‌های فناوری یا افراد دیگر، صورت گرفته است. این اقدام می‌تواند شامل نقض قوانین حفاظت از داده‌ها یا نفوذ به سامانه‌های ذخیره‌سازی اطلاعات شخصی باشد. در نهایت، باید ثابت شود که رابطه‌ای مستقیم میان فعل زیان‌بار و ضرر وارد شده وجود دارد، یعنی نقض حریم خصوصی به‌طور مستقیم به وقوع ضرر منجر شده است.[۱]

در حقوق ایران، ماده ۱۱۵۹ قانون مدنی، مسئولیت مدنی را بر اساس اصول عمومی مسئولیت قرار می‌دهد و مقرر می‌دارد که هر شخصی که به دیگران زیانی وارد کند، مسئول جبران آن است. در خصوص نقض حریم خصوصی، این ماده می‌تواند برای جبران خسارت‌های مادی و معنوی ناشی از افشای غیرمجاز داده‌ها یا نقض حریم خصوصی استفاده شود. همچنین، طبق ماده ۱۲ قانون جرایم رایانه‌ای، هرگونه دسترسی غیرمجاز به داده‌های شخصی و نقض حریم خصوصی افراد در فضای سایبری به‌عنوان جرم محسوب می‌شود و مرتکب آن می‌تواند تحت تعقیب قانونی قرار گیرد. این مواد قانونی تأکید می‌کنند که نهادهای مسئول در حوزه فناوری و سامانه‌های هوشمند موظف به حفاظت از داده‌های شخصی و جبران هرگونه خسارت ناشی از نقض این حقوق هستند.[۲]

۳-۱-مبانی مسئولیت مدنی در بستر فناوری: نظریه تقصیر، خطر

در بستر فناوری، مسئولیت مدنی ممکن است بر اساس دو نظریه «تقصیر» و «خطر» تحلیل شود. نظریه تقصیر بر این اساس استوار است که مسئولیت فرد تنها زمانی ایجاد می‌شود که او در انجام عملی که منجر به ورود ضرر به دیگری شده است، مرتکب تقصیر (اعمال بی‌احتیاطی یا عدم رعایت قوانین) شده باشد. به عبارت دیگر، طبق این نظریه، برای اعمال مسئولیت مدنی باید اثبات شود که شخص مسئول در انجام عمل خود کوتاهی کرده و این کوتاهی منجر به آسیب یا نقض حقوق دیگری شده است. در بستر فناوری، این نظریه می‌تواند زمانی اعمال شود که یک شرکت فناوری یا کاربر در حفظ داده‌های شخصی بی‌دقتی کرده و منجر به نشت اطلاعات یا نقض حریم خصوصی دیگران شود. در حقوق ایران، ماده ۱۲ قانون مسئولیت مدنی بر اساس نظریه تقصیر به صراحت

[۱] - مظاهری اوغاز، کیارش؛ غلامی مطلق، مجید (۱۴۰۳)، هوش مصنوعی، چاپ اول، تهران: انتشارات خیزران،ص۶۹

[۲] -ذاکری نیا، حانیه(۱۴۰۲)، ماهیت و مبنای مسئولیت مدنی ناشی از هوش مصنوعی در حقوق ایران و کشورهای اتحادیه اروپا، مجله حقوق خصوصی، دوره۲۰، شماره۱،ص ۱۳۹

بیان می‌کند که «هر کس به عمد یا به سبب بی‌احتیاطی به دیگری خسارت وارد آورد، مسئول جبران آن است.»[1]

اما در برخی شرایط، نظریه خطر به کار می‌رود که در آن مسئولیت ناشی از فعالیت‌های پرخطر یا استفاده از فناوری‌های جدید به‌طور خودکار ایجاد می‌شود، حتی اگر فرد مرتکب تقصیر نشده باشد. این نظریه به ویژه در مواردی که فناوری‌ها به خودی خود خطرات ذاتی دارند و امکان آسیب به دیگران به‌طور مستقیم از سوی کاربر یا سازمان مسئول وجود دارد، اعمال می‌شود. برای مثال، سامانه‌های هوش مصنوعی یا فضای سایبری ممکن است به‌طور خودکار داده‌های شخصی را پردازش کنند و در نتیجه، احتمال نشت یا سوءاستفاده از داده‌ها افزایش یابد. طبق ماده ۹ قانون جرایم رایانه‌ای، هرگونه نفوذ غیرمجاز به سامانه‌های اطلاعاتی و نقض امنیت داده‌ها، حتی بدون وجود تقصیر مستقیم از سوی عامل، موجب مسئولیت مدنی است. این ماده به وضوح مسئولیت نهادهای مسئول در حوزه فناوری را برای حفاظت از داده‌ها و جبران خسارت‌های ناشی از نقض حریم خصوصی تأکید می‌کند، حتی در صورت نبود تقصیر از سوی آن‌ها. به این ترتیب، مسئولیت مدنی در بستر فناوری می‌تواند هم بر اساس نظریه تقصیر و هم بر اساس نظریه خطر به‌طور مستقل ایجاد شود.[2]

۳-۲-تحلیل ارکان تحقق مسئولیت: فعل زیان‌بار، ضرر، رابطه سببیت

برای تحقق مسئولیت مدنی ناشی از نقض حریم خصوصی در بستر فناوری‌های هوشمند، سه رکن اساسی وجود دارد: فعل زیان‌بار، ضرر و رابطه سببیت. ابتدا باید اثبات شود که شخص مسئول عملی زیان‌آور انجام داده است. این عمل می‌تواند شامل افشای غیرمجاز اطلاعات شخصی، نفوذ به سامانه‌های اطلاعاتی یا عدم رعایت استانداردهای امنیتی در فناوری‌های هوشمند باشد. به‌عنوان مثال، اگر یک شرکت فناوری به‌طور ناخواسته اطلاعات کاربران خود را در معرض افشا قرار دهد، این عمل به‌عنوان یک فعل زیان‌بار محسوب می‌شود. در حقوق ایران، ماده ۳۰۰ قانون مدنی، هر نوع خسارت واردشده به دیگران را بر اساس عمل زیان‌بار مسئول دانسته و آن را مستوجب جبران می‌کند.

دومین رکن، ضرر است که باید به‌طور دقیق و ملموس وجود داشته باشد. ضرر می‌تواند به‌صورت مادی (مانند هزینه‌های درمان یا جبران خسارت‌های مالی) یا معنوی (مانند آسیب به اعتبار یا حیثیت فرد) باشد. در صورت نقض حریم خصوصی، شخص زیان‌دیده ممکن است دچار اضطراب، استرس و آسیب‌های روانی شود که خود نوعی ضرر معنوی محسوب می‌شود. طبق ماده ۱۱۵۹ قانون مدنی ایران، هرگاه فردی به دلیل نقض حقوق او دچار ضرر شود، مسئولیت جبران آن بر عهده مرتکب است. در نهایت، باید رابطه مستقیم میان فعل زیان‌بار و ضرر وارد شده اثبات شود. به‌عبارت دیگر، اگر عمل زیان‌بار (افشای اطلاعات یا نقص امنیتی سامانه) باعث آسیب به فرد شده باشد، باید ثابت شود که این آسیب به‌طور مستقیم از آن عمل ناشی شده است. در حقوق ایران، ماده ۳۰۰ قانون مدنی به‌طور خاص به این موضوع اشاره دارد که در صورت اثبات رابطه سببیت میان عمل زیان‌آور و ضرر، مسئولیت جبران خسارت بر عهده مرتکب خواهد بود.[3]

---

[1] -مکی، اکرم السادات و همکاران(۱۴۰۳)، بررسی مسئولیت ناشی از اعمال هوش مصنوعی در نظام حقوقی ایران، نشریه علمی فقه، حقوق و علوم جزا، سال هشتم، شماره۳۲، ص۷۳

[2] - حکمت نیا، محمود و همکاران(۱۳۹۸)، مسئولیت مدنی ناشی از تولید ربات‌های مبتنی بر هوش مصنوعی خودمختار، فصلنامه حقوق اسلامی، شماره۶۰،ص۲۷

[3] -امین ابراهیم آبادی، محمدحسین؛ متین راد، علی محمد(۱۴۰۳)، مطالعه تطبیقی مسئولیت مدنی ناشی از استفاده از هوش مصنوعی در حقوق ایران و کشورهای اتحادیه اروپا، چاپ اول، انتشارات پژوهشگران پارسه،ص۱۲۳

۳-۳-انواع خسارات قابل مطالبه در تعرض به حریم خصوصی (مادی، معنوی، حیثیتی)

در صورت تعرض به حریم خصوصی، افراد می‌توانند خسارات مختلفی را مطالبه کنند که به‌طور کلی به سه دسته اصلی تقسیم می‌شود: خسارات مادی، معنوی و حیثیتی. خسارات مادی شامل تمام ضررهای مالی است که فرد از تعرض به حریم خصوصی متحمل می‌شود، مانند هزینه‌های پزشکی، هزینه‌های قانونی برای پیگیری شکایات، یا کاهش درآمد ناشی از از دست دادن فرصت‌های شغلی یا تجاری به دلیل افشای اطلاعات خصوصی. خسارات معنوی به آسیب‌های غیرمالی اشاره دارد که فرد به دلیل نقض حریم خصوصی دچار آن می‌شود، مانند اضطراب، افسردگی، استرس یا سایر مشکلات روانی ناشی از افشای اطلاعات حساس. در این نوع خسارت، فرد ممکن است به دلیل نقض حریم خصوصی‌اش احساس تحقیر یا بی‌احترامی کند. خسارات حیثیتی نیز شامل آسیب‌هایی است که به اعتبار و شهرت فرد وارد می‌شود. برای مثال، اگر اطلاعات خصوصی فردی در فضای عمومی افشا شود، او ممکن است با از دست دادن اعتماد عمومی یا مواجهه با طرد اجتماعی روبه‌رو شود. طبق ماده ۱۱۵۹ قانون مدنی ایران، فردی که به حریم خصوصی دیگری تعرض کرده است، موظف به جبران تمامی انواع خسارت‌های مادی، معنوی و حیثیتی وارد شده به وی است.[۱]

۳-۴-امکان انتساب فعل زیان‌بار به اشخاص حقوقی و مسئولیت‌های جمعی

در حقوق ایران، اشخاص حقوقی نیز می‌توانند مسئولیت مدنی ناشی از نقض حریم خصوصی را تحمل کنند. این بدین معناست که اگر یک شخص حقوقی مانند شرکت‌ها، مؤسسات یا سازمان‌ها، به دلیل عدم رعایت اصول امنیتی یا افشای غیرمجاز اطلاعات شخصی، مرتکب فعل زیان‌بار شوند، مسئولیت جبران خسارت‌های ناشی از آن بر عهده آن شخص حقوقی خواهد بود. طبق ماده ۵۸ قانون مدنی ایران، اشخاص حقوقی می‌توانند به‌عنوان مسئول جبران خسارت‌های مادی و معنوی شناخته شوند، زیرا فعل انجام‌شده در چهارچوب فعالیت‌های آن‌ها قرار دارد. علاوه بر این، در صورتی که مسئولیت جمعی ناشی از اقدام گروهی باشد، مانند مجموعه‌ای از کارکنان یک سازمان که موجب نقض حریم خصوصی دیگران شده‌اند، مسئولیت جمعی نیز مطرح است. این امر در ماده ۳۴ قانون مسئولیت مدنی قابل استناد است، که بر مسئولیت مشترک اعضای گروه یا سازمان در صورت انجام اعمال زیان‌آور تأکید دارد. بنابراین، اشخاص حقوقی می‌توانند به‌طور مستقیم یا به‌واسطه کارکنان خود مسئول جبران خسارات ناشی از نقض حریم خصوصی باشند.[۲]

۴-سیاست‌گذاری حقوقی و پیشگیری از تعرض به حریم خصوصی در فضای هوش مصنوعی

سیاست‌گذاری حقوقی برای حفاظت از حریم خصوصی در فضای هوش مصنوعی به‌منظور جلوگیری از نقض حقوق افراد، نیازمند وضع قوانین جامع و مؤثر است. در این راستا، ضروری است که قوانین، به‌ویژه در زمینه پردازش داده‌های شخصی، شفافیت ایجاد کنند و مسئولیت‌های قانونی را برای شرکت‌ها و سازمان‌ها تعریف کنند. در سطح بین‌المللی، قانون حفاظت از داده‌های شخصی اتحادیه اروپا نمونه‌ای برجسته است که بر ضرورت اخذ رضایت آگاهانه از کاربران، شفافیت در جمع‌آوری و پردازش داده‌ها، و تضمین امنیت داده‌ها تأکید دارد. در ایران نیز قانون حمایت از حقوق مصرف‌کنندگان در فضای مجازی با هدف تضمین حفاظت

[۱] -همان منبع،ص۱۵۰

[۲] -ابوذری، مهرنوش(۱۴۰۲)، حقوق و هوش مصنوعی، چاپ سوم، انتشارات میزان،ص۶۸

از داده‌های شخصی کاربران در فضای سایبر و ایجاد مسئولیت‌پذیری در برابر نقض این حقوق، وضع شده است.

پیشگیری از تعرض به حریم خصوصی در بستر فناوری‌های هوش مصنوعی نیازمند ایجاد نهادهای نظارتی کارآمد و سازوکارهای اجرایی است. در این خصوص، ماده ۱۲ قانون جرایم رایانه‌ای ایران، به‌طور خاص بر لزوم رعایت تدابیر امنیتی مناسب توسط سازمان‌ها و شرکت‌ها برای حفاظت از داده‌های شخصی و جلوگیری از دسترسی غیرمجاز تأکید می‌کند. علاوه بر این، تقویت همکاری‌های بین‌المللی برای هماهنگی استانداردهای جهانی امنیت داده‌ها و حفاظت از حریم خصوصی، به ایجاد چارچوب‌های حقوقی جامع‌تر و ایمن‌تر برای کاربران در فضای هوش مصنوعی کمک خواهد کرد.[1]

۵-ضرورت تدوین سیاست‌های پیشگیرانه در حوزه حقوق فناوری

ضرورت تدوین سیاست‌های پیشگیرانه در حوزه حقوق فناوری به‌ویژه در زمینه حفاظت از حریم خصوصی، به دلیل توسعه سریع و پیچیدگی‌های فناوری‌های نوین همچون هوش مصنوعی، بیش از پیش احساس می‌شود. بدون وجود چارچوب‌های حقوقی روشن و مؤثر، امکان سوءاستفاده از داده‌های شخصی، نقض حریم خصوصی و تهدید حقوق افراد در فضای دیجیتال افزایش می‌یابد. تدوین سیاست‌های پیشگیرانه می‌تواند با تعیین مسئولیت‌های قانونی برای فعالان حوزه فناوری، تضمین امنیت داده‌ها، و ایجاد مکانیسم‌های نظارتی مؤثر، از بروز تخلفات و نقض حقوق افراد جلوگیری کند. در این راستا، قانون‌گذاران باید قوانینی را تصویب کنند که حفاظت از داده‌ها را در برابر تهدیدات جدید، همچون نفوذ به سیستم‌ها و افشای غیرمجاز اطلاعات، تأمین کرده و در عین حال فضای نوآوری را محدود نکنند.

نتیجه گیری

با توجه به مطالب مطرح‌شده در این مقاله، می‌توان نتیجه گرفت که توسعه روزافزون فناوری‌های هوش مصنوعی تأثیرات زیادی بر حریم خصوصی اشخاص دارد. استفاده از داده‌های شخصی به‌ویژه در سامانه‌های مبتنی بر هوش مصنوعی می‌تواند موجب تهدیدات جدی برای حقوق فردی و اجتماعی افراد شود. از یک سو، پردازش‌های خودکار داده‌ها بدون رضایت آگاهانه کاربران، افشای ناخواسته اطلاعات شخصی، و تهدیدات امنیتی مانند هک و نفوذ به داده‌ها، حریم خصوصی افراد را به‌طور قابل توجهی نقض می‌کند. از سوی دیگر، مسئولیت‌های قانونی ناشی از این نقض‌ها باید با دقت و شفافیت بیشتر مشخص شود تا حقوق افراد در دنیای دیجیتال به‌طور مؤثر حفظ گردد.

در خصوص مسئولیت مدنی ناشی از نقض حریم خصوصی توسط فناوری‌های هوش مصنوعی، مسئولیت در درجه اول بر عهده سازمان‌ها و شرکت‌های فناوری است که داده‌های شخصی کاربران را جمع‌آوری و پردازش می‌کنند. طبق قوانین موجود مانند ماده ۱۲ قانون جرایم رایانه‌ای ایران و قانون حمایت از حقوق مصرف‌کنندگان در فضای مجازی، نهادهای مسئول باید تدابیر امنیتی لازم را برای حفاظت از داده‌ها اتخاذ کرده و از هرگونه افشای غیرمجاز اطلاعات جلوگیری کنند. این مسئولیت شامل اقدامات پیشگیرانه و واکنش سریع در مواجهه با تهدیدات امنیتی می‌شود. همچنین، طبق ماده ۱۱۵۹ قانون مدنی ایران، هر شخص یا نهادی که موجب ورود خسارت به دیگری شود، موظف به جبران آن است.در صورتی که

[1] - عباسی، محمود (۱۳۹۹)، هوش مصنوعی و حقوق: چالش‌ها و فرصت‌ها، چاپ اول، تهران: نشر میزان،ص۶۹

نقض حریم خصوصی ناشی از اقدام عمدی یا بی‌احتیاطی باشد، مسئولیت مدنی فرد یا سازمان به‌طور واضح مشخص است. این مسئولیت می‌تواند شامل خسارات مادی و معنوی، از جمله آسیب به اعتبار و حیثیت فرد، و خسارات روانی ناشی از افشای اطلاعات خصوصی باشد. به علاوه، طبق ماده ۳۰۰ قانون مدنی ایران، در صورتی که فرد یا سازمان مسئول نتواند از داده‌های شخصی به‌طور مؤثر حفاظت کند و این امر به آسیب به دیگران منجر شود، مسئولیت جبران خسارات به‌عهده آن‌ها خواهد بود.

در نهایت، برای پیشگیری از نقض حریم خصوصی در فضای هوش مصنوعی، نیاز به تدوین سیاست‌های حقوقی جامع و کارآمد احساس می‌شود. این سیاست‌ها باید شامل تدوین قوانینی برای حفاظت از داده‌های شخصی، تقویت نهادهای نظارتی، و اعمال مسئولیت‌های قانونی بر نهادهای پردازش‌کننده داده‌ها باشد. در این راستا، می‌توان از تجربیات بین‌المللی مانند قانون اتحادیه اروپا استفاده کرده و آن‌ها را با شرایط حقوقی ایران سازگار نمود تا هم حقوق کاربران حفظ شود و هم فضای نوآوری در حوزه فناوری‌های هوش مصنوعی محدود نگردد.

پیشنهادات

اجرایی:

۱.ایجاد نهاد ناظر مستقل تحت نظارت قوه قضائیه یا وزارت دادگستری برای نظارت بر رعایت حقوق حریم خصوصی در سامانه‌های هوش مصنوعی.

۲.الزام قانونی شرکت‌ها و نهادهای دولتی به ثبت و گزارش نحوه جمع‌آوری، پردازش و ذخیره داده‌های شخصی.

۳.تعیین سازوکار دادرسی تخصصی در مراجع قضایی برای رسیدگی سریع به دعاوی مرتبط با نقض حریم خصوصی در بستر هوش مصنوعی.

عملی:

۱.اصلاح و الحاق مواد قانونی به قانون مسئولیت مدنی به‌منظور شمول صریح موارد ناشی از آسیب‌های ناشی از فناوری‌های هوشمند.

۲.پیش‌بینی مسئولیت تضامنی شرکت، مدیر و توسعه‌دهنده سامانه در صورت افشای غیرمجاز داده‌های اشخاص.

۳.تدوین مقررات مشخص برای تعریف و احراز "رضایت آگاهانه" در فرآیند استفاده از خدمات مبتنی بر هوش مصنوعی.

کاربردی:

۱.تصویب آیین‌نامه‌های اجرایی برای ماده ۱۲ قانون جرایم رایانه‌ای درباره حفاظت از داده‌های شخصی در سامانه‌های هوش مصنوعی.

۲.تدوین منشور حقوق شهروندی در فضای دیجیتال با تأکید بر حفظ حریم خصوصی و امنیت اطلاعات در بسترهای هوشمند.

۳.ایجاد بانک ملی داده‌های شخصی با ضمانت اجرای قانونی برای کنترل، مدیریت و حفظ اطلاعات کاربران توسط دولت.

سپاسگزاری

از معاونت محترم پژوهشی به خاطر حمایت معنوی در اجرای پژوهش حاضر سپاسگزاری می‌شود.

از آقای دکتر عبدالله علیزاده به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.

از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.

نگارندگان بر خود لازم می‌دانند از آقای دکتر محمد رسول آهنگران به خاطر مطالعه متن مقاله حاضر و ارائه نظرهای ارزشمند سپاسگزاری نمایند.

منابع

کتاب‌ها

۱-ابوذری، مهرنوش(۱۴۰۲)، حقوق و هوش مصنوعی، چاپ سوم، انتشارات میزان

۲-امین ابراهیم آبادی، محمدحسین؛ متین راد، علی محمد(۱۴۰۳)، مطالعه تطبیقی مسئولیت مدنی ناشی از استفاده از هوش مصنوعی در حقوق ایران و کشورهای اتحادیه اروپا، چاپ اول، انتشارات پژوهشگران پارسه

۳-انصاری، باقر؛عطار، شیما؛ صالحی، امیرحسین(۱۴۰۰)، حقوق داده‌ها و هوش مصنوعی، تهران: شرکت سهامی انتشار

۴-بیات، معصومه (۱۳۹۹)، حقوق بشر و فناوری‌های نوین: چالش‌ها و راهکارها، چاپ اول، تهران: نشر میزان،ص۲۵

۵-زاورنیک، آلاش(۱۴۰۰)، عدالت کیفری، سیستم‌های هوش مصنوعی و ملاحظات حقوق بشری، تهران: انتشارات میزان،ص۷۲

۶-عباسی، محمود (۱۳۹۹)، هوش مصنوعی و حقوق: چالش‌ها و فرصت‌ها، چاپ اول، تهران: نشر میزان

۷-مظاهری اوغاز، کیارش؛ غلامی مطلق، مجید (۱۴۰۳)، هوش مصنوعی، چاپ اول، تهران: انتشارات خیزران

مقالات

۱-ابن علی، آرش (۱۴۰۰)، جرم انگاری دیپ فیک‌ها از منظر تعهدات حقوق بشری دولت‌ها، مجله تحقیقات حقوق قضایی، دوره دوم، شماره ۳، صص ۳۸۴-۳۵۵

۲-بنافی، فرشته (۱۴۰۲)، حفاظت از حق حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی، نشریه پژوهش حقوق خصوصی، دوره ۱۲، شماره ۴۵، صص ۱۷۶-۱۴۹

۳-حکمت نیا، محمود؛ محمدی، مرتضی؛ واثقی، محسن(۱۳۹۸)، مسئولیت مدنی ناشی از تولید ربات‌های مبتنی بر هوش مصنوعی خودمختار، فصلنامه حقوق اسلامی، شماره۶۰،صص۲۹-۱

۴-حکمت نیا،محمود؛ محمدی، مرتضی؛ واثقی، محسن(۱۳۹۸)، مسئولیت مدنی ناشی از تولید ربات‌های مبتنی بر هوش مصنوعی خودمختار، نشریه حقوق اسلامی،دوره۱۶، شماره۶۰، صص۲۵۸-۲۳۱

۵-ذاکری نیا، حانیه(۱۴۰۲)، ماهیت و مبنای مسئولیت مدنی ناشی از هوش مصنوعی در حقوق ایران و کشورهای اتحادیه اروپا، مجله حقوق خصوصی، دوره۲۰، شماره۱،صص۱۵۲-۱۳۵

۶-فراهانی، عاطفه؛ میرزاده کوهشاهی، نادر (۱۴۰۱)، هوش مصنوعی و نقض حقوق بشر و مسئولیت آن، نهمین همایش ملی مطالعات و تحقیقات نوین در حوزه علوم انسانی، مدیریت و کارافرینی ایران، صص ۲۲-۱

۷-مکی، اکرم السادات؛ مکی، زهرا السادات؛ کشکولیان، اسماعیل(۱۴۰۳)، بررسی مسئولیت ناشی از اعمال هوش مصنوعی در نظام حقوقی ایران، نشریه علمی فقه، حقوق و علوم جزا، سال هشتم، شماره۳۲،صص۷۹-۷۱

۸-مولوی، حانیه (۱۴۰۲)، مطالعه چالش‌های حقوق بشری هوش مصنوعی، پنجمین کنفرانس بین المللی علوم انسانی، حقوق، مطالعات اجتماعی و روانشناسی، صص ۲۷-۱

پایان نامه‌ها و رساله‌ها

۱-سالاری، سپیده(۱۴۰۰)، رویکرد حقوق کیفری ایران و انگلستان به مسئولیت ناشی از هوش مصنوعی، پایان نامه جهت دریافت درجه کارشناسی ارشد، دانشگاه شهید بهشتی

۲-شفیعی، شیما (۱۴۰۲)، نقش هوش مصنوعی در پیشگیری از جرم، رساله دکتری تخصصی، دانشگاه شهید بهشتی

۳-شیرزاد، کامران (۱۳۹۹)، مسئولیت کیفری صاحبان هوش مصنوعی در حقوق ایران و حقوق بین‌الملل، رساله دکتری تخصصی، دانشگاه عدالت