

مسئولیت مدنی هوش مصنوعی در حوزه حریم خصوصی با رویکردی بر استانداردهای نظارتی در قراردادهای تجاری

فاطمه ذوالفقارزاده^۱

* نوع مقاله: ترویجی / تاریخ دریافت: ۱۴۰۳/۰۹/۱۷ / تاریخ پذیرش: ۱۴۰۳/۱۱/۰۱

کد مقاله: ۱۲۵۷-۱-۲۵۰۱-JHVMN

چکیده

برنامه های کاربردی هوش مصنوعی در زندگی روزمره ما استفاده می شوند و مزایای قابل توجهی را برای کاربران خود به همراه دارند. با این حال، درست مانند هر چیز دیگری در زندگی، همه چیز ممکن است اشتباه پیش برود و کاربران یا اشخاص ثالث آنها ممکن است متحمل ضررهایی مرتبط با عملکرد نادرست برنامه هوش مصنوعی مربوطه شوند جهت استانداردسازی مطلوب در حوزه هوش مصنوعی و ارزیابی دقیق آن و اعتمادسازی نسبت به فرآیندها و سامانه های مبتنی بر هوش مصنوعی، بررسی استانداردهای تدوین شده در این خصوص در سطح بین المللی و ملی ضروری است. به دلیل کاربردهای وسیع و مهم هوش مصنوعی، امروزه استانداردسازی هوش مصنوعی در دستور کار اغلب سازمان های استانداردسازی قرار گرفته است. استانداردها این اطمینان را ایجاد می کنند که هوش مصنوعی در خدمت منافع عمومی خواهد بود. به بیانی دیگر بدون مقررات و استانداردهایی برای استفاده مسئولانه از هوش مصنوعی، نمی توان از پیامدهای مضر آن اجتناب کرد. همه می دانیم که زمانی که سود و قدرت تنها انگیزه باشد، هوش مصنوعی نیز برای خدمت صرف به قدرت و سرمایه مورد استفاده قرار می گیرد. در این موقعیت به پیامدهای آن برای زندگی انسان ها هرگز توجه نخواهد شد. بنابراین استانداردها تضمین می کنند که فناوری های هوش مصنوعی مطابق با اصول اخلاقی و هنجارهای اجتماعی توسعه یابد. همچنین بر اساس نتایج تحقیق قراردادهای یکی از پیچیده ترین موارد برای درک و تجزیه و تحلیل در دنیای تجارت هستند. هوش مصنوعی می تواند در تجزیه و تحلیل و مدیریت قراردادها کمک کند و بدین ترتیب در دنیای واقعی مورد استفاده قرار بگیرد. نتایج تحقیق شناسایی و مقابله با تهدیدات جدید، ربات های نبرد سایبری، پیش بینی خطر نقض، محافظت بهتر نقطه پایانی، یادگیری در طول زمان، مدیریت داده های فراوان، کاهش فرآیندهای تکراری و ایمن کردن احراز هویت. هوش مصنوعی به مانند دیگر فناوری ها، فرصت ها و تهدیدات بالقوه ای را برای جمهوری اسلامی ایران ایجاد نموده است. لیکن می توان با تعبیه سازوکارهای قانونی و اجرایی، زمینه بهره مندی حداکثری کشور از این فناوری در راستای افزایش قدرت ملی و جامه عمل پوشاندن به اهداف انقلاب اسلامی در سطح منطقه و جهان را فراهم کرد.

واژگان کلیدی: هوش مصنوعی، حریم خصوصی، نظارت، استاندارد.

^۱ کارشناس ارشد حقوق خصوصی، واحد صفاشهر، دانشگاه آزاد اسلامی، صفاشهر، ایران. (نویسنده مسئول)

Fatemezolfagharzade77@gmail.com



مقدمه

بسیاری از فناوری‌های هوش مصنوعی در نهایت تحت مالکیت و کنترل نهادهای خصوصی هستند. از جمله اسناد داخلی و بین‌المللی که در این تحقیق مورد استفاده قرار گرفته است عبارت است از: سند ملی هوش مصنوعی جمهوری اسلامی ایران مصوب ۱۴۰۳/۳/۲۹، همچنین کنوانسیون چارچوب هوش مصنوعی و حقوق بشر، دموکراسی و حاکمیت قانونی. بزهکاران با استفاده از هوش مصنوعی می‌توانند اقدام به سلب امنیت خصوصی و حقوق شهروندان نمایند، از آنجا که در کشور ما قانون خاصی برای جرائم در هوش مصنوعی وجود ندارد و بعضی می‌اندیشند جرائم رایانه ای می‌تواند پاسخگوی موضوع حاضر باشد در حالی که چنین نیست، لذا نگاره با تنقیح مناطق و بهره‌گیری از ادله شرعی به موضوع تاثیر هوش مصنوعی بر حفظ حریم خصوصی در حوزه حقوق پرداخته است. چرا که سالب امنیت و آسایش شهروندان با استفاده از ابزار هوش مصنوعی محارب و مفسد فی‌الارض است و در صورت اقدام به آن مستحق اعمال مجازات محارب خواهد بود (حکیم و ابراهیمیان، ۱۴۰۱: ۷۴). در برخی موارد، استفاده نادرست از هوش مصنوعی می‌تواند باعث ترس و نگرانی مردم شود. به عنوان مثال، در صنعت فیلم سازی، استفاده از تکنولوژی‌های گرافیکی و واقعیت مجازی برای ایجاد صحنه‌های ترسناک و وحشتناک متداول است. همچنین، در برخی موارد، استفاده از هوش مصنوعی در صنایعی مانند نظامی، امنیتی و پلیسی ممکن است باعث ترس و نگرانی مردم شود. به عنوان مثال، استفاده از ربات‌های نظامی با توانایی‌های بالا در جنگ‌ها و مأموریت‌های خطرناک می‌تواند باعث نگرانی و ترس مردم شود. همچنین، استفاده نادرست از هوش مصنوعی در حوزه‌هایی مانند تحلیل داده‌ها و ردیابی فردی نیز ممکن است باعث نگرانی و ترس مردم شود، به خصوص در صورتی که اطلاعات شخصی و حریم خصوصی افراد به نحوی توسط هوش مصنوعی نقض شود. به طور کلی، هوش مصنوعی برای خدمت به انسان طراحی شده است و در صورت استفاده صحیح، می‌تواند بهبود وضعیت اجتماعی، اقتصادی و فرهنگی جامعه را به همراه داشته باشد. اما برای جلوگیری از استفاده نادرست از هوش مصنوعی، باید قوانین و مقررات مناسبی برای استفاده از آن در نظر گرفته شود و به نحوی طراحی شود که حقوق و حریم خصوصی افراد را به حداکثر محافظت برساند. فناوری‌های نظامی هوش مصنوعی پیوسته در حال تکامل و بهبود هستند و ممکن است در مجموعه‌ای از محیط‌های عملیاتی مختلف مفید واقع شوند. این فناوری‌ها شامل تشخیص الگو، یادگیری ماشین، بینایی رایانه‌ای... درک زبان طبیعی و تشخیص گفتار است. فناوری‌ها برای افزایش توانایی‌های انسان‌ها و ماشین‌ها به کار گرفته می‌شوند و به آن‌ها کمک می‌کنند تا تصمیم‌هایی با کیفیت بالاتر



و سرعت بیشتر بگیرند. اینها سیستم‌هایی هستند که برای حل تکالیف و دستیابی به اهدافی خاص طراحی شده‌اند که از برخی جهات با فرآیندهای شناختی انسان‌ها در درک استدلال، یادگیری، برقراری ارتباط بین تصمیم‌گیری و عمل، موازی هستند. عملکرد این سیستم‌ها می‌تواند آن‌ها را برای کارهایی مانند شناسایی تانک‌های جنگی در تصاویر ماهواره‌ای، شناسایی اهداف با ارزش در میان جمعیت با استفاده از تشخیص چهره، ترجمه متن برای کسب اطلاعات از منابعی که در دسترس عموم قرار دارند و تولید متن در عملیات اطلاعاتی بسیار مفید باشد. همچنین در زمینه‌هایی مانند سیستم‌های توصیه، تشخیص ناهنجاری، سیستم‌های پیش‌بینی و بازی‌های کامپیوتری رقابتی بسیار توانمند است. یک سیستم هوش مصنوعی می‌تواند به ارتش در کشف تقلب در خدمات قراردادی خود، پیش‌بینی زمان خرابی سیستم‌های تسلیحاتی به دلیل مشکلات تعمیر و نگهداری یا توسعه استراتژی‌های برنده در شبیه‌سازی مخاصمه و همچنین تولید پهپادهای پیشرفته جهت تجسس، شناسایی، ارزیابی و از بین بردن هدف تعیین شده کمک کند. همه این برنامه‌ها و موارد دیگر، می‌توانند در عملیات‌های روزمره و مخاصمات بعدی، باعث بالا رفتن ضریب نیرو باشند. به عنوان نمونه، در سال ۲۰۲۱، پس از تسلط طالبان بر افغانستان، گزارشی در مورد اقدامات فوری ارتش کانادا، وزارت امور خارجه ایالات متحده و آژانس توسعه بین‌المللی ایالات متحده منتشر شد که بر اساس آن، این نهادها به سرعت فرآیندی را برای حذف حضور دیجیتالی حامیان افغان از وبسایت خود، از ترس انتقام توسط رژیم جدید افغانستان آغاز کردند. در واقع، هم طالبان و هم نیروهای ائتلاف تحت رهبری ایالات متحده به اسکنرهای قابل حمل مجهز به هوش مصنوعی که کار آنها جمع‌آوری داده‌های مربوط به چشم، اثر انگشت، عکس و زندگینامه افراد بود، تکیه داشته‌اند و این اطلاعات جمع‌آوری شده به کمک هوش مصنوعی نظامی در زمان تسلط ایالات متحده بر افغانستان، اکنون امنیت آن دسته از افغان‌هایی را که با آمریکایی‌ها همکاری می‌کردند، بیشتر تهدید می‌کند.

آنچه ذکر گردید، نمونه‌ای است که در آن حریم خصوصی، حفاظت از داده‌ها، پردازش خودکار، اطلاعات بیومتریک و درگیری مسلحانه با یکدیگر تلاقی پیدا می‌کنند و این نشان می‌دهد که علاوه بر ربات‌های قاتل و حملات سایبری، اقیانوسی از مسائل حقوقی در زمینه نقض حریم خصوصی اطلاعاتی اشخاص و نهادها برای تحقیق در زمینه هوش مصنوعی وجود دارد؛ بنابراین با وجود چنین نقض‌هایی، باید چارچوبی را برای یک رژیم کنترل تسلیحات جدید برای کاهش خطرات مرتبط با انواع خاصی از برنامه‌های هوش مصنوعی ارائه نمود. با وجود این و تا زمانی که چنین چارچوبی

محقق شود، ضرورت دارد تا بررسی شود که آیا چارچوب‌های قانونی موجود، پیش از این به تحدید استفاده از هوش مصنوعی نظامی جهت حفظ حریم خصوصی اطلاعاتی در قالب یک معاهده پرداخته اند یا خیر و در صورت مثبت بودن پاسخ، چگونه این امر محقق گردیده است. تحقیقاتی که در این حوزه انجام شده است به شرح ذیل می باشد:

سلطانی عمیدآبادی، سمیرا، (۱۴۰۲)، کتابی با عنوان مردمک هوشمند: بررسی نقش هوش مصنوعی در نظارت بر جامعه، قلم مهر، چاپ اول نگاشته‌اند: هوش مصنوعی می تواند در توسعه علم حقوق و بهبود فرآیندهای قضایی نقش موثری ایفا کند. با این حال، ضرورت وجود سیاست ها و قوانین مناسب برای استفاده از هوش مصنوعی در حوزه حقوق به طور جدی احساس می شود. صادقی و همکاران (۱۴۰۲) «هوش مصنوعی و حقوق بین الملل» انتشارات حقوق یار نگاشته‌اند: چارچوب‌های قانونی موجود، مانند قوانین کپی رایت، نیاز به انطباق و شفاف‌سازی بیشتری دارند تا به‌طور مؤثر آثار تولید شده توسط هوش مصنوعی در عصر دیجیتال را نیز در برگیرد. امیری، جواد، حسینی، زکیه، (۱۴۰۲)، «نقش هوش مصنوعی در تحول علم حقوق و ملزومات آن»، چهارمین کنفرانس ملی پدافند سایبری: این مقاله به بررسی نقش هوش مصنوعی در حوزه علم حقوق می پردازد. هوش مصنوعی به عنوان یک زمینه پیشرفته در علوم رایانه، ابزارهای قدرتمندی را برای تجزیه و تحلیل داده ها، پردازش زبان طبیعی و تصمیم گیری هوشمند فراهم می کند. دروگری، ریحانه، کاوسی خسرقی، پرزاد، (۱۴۰۲)، «کاربرد هوش مصنوعی در حوزه پزشکی و چالش های حقوقی حفاظت از حریم خصوصی»، اولین کنفرانس ملی ارتقای سلامت و چالش های حقوقی و پزشکی فراروی آن: بر اساس نتایج این تحقیق ماهیت پیاده سازی هوش مصنوعی می تواند به این معنا باشد که چنین شرکت ها، کلینیک ها و نهادهای عمومی نقشی بیش از حد معمول در به دست آوردن، استفاده و حفاظت از اطلاعات سلامت بیمار خواهند داشت. این موضوع مسائل مربوط به حریم خصوصی مربوط به پیاده سازی و امنیت داده ها را ایجاد می کند. پژوهش حاضر بر آن است که برای استفاده از هوش مصنوعی چه استانداردهای نظارتی ملی و بین المللی باید رعایت گردد؟

۱- تعاریف، مفاهیم و اوصاف و مبانی هوش مصنوعی

۱-۱- هوش مصنوعی



هوش مصنوعی یکی از بحث برانگیزترین موضوعات علوم رایانه است که بر درک و اجرای فرایندهایی همچون منطق، یادگیری مهارت های جدید، تطبیق با شرایط موجود و حل مسائل استوار می باشد. کورزویل در سال ۱۹۹۰ هوش مصنوعی را اینگونه تعریف کرد: هنر ساخت ماشین ها و برنامه هایی که قادرند اعمالی را انجام دهند که اگر قرار بود توسط انسان انجام شوند، به هوشمندی بالایی نیاز داشتند. هوش مصنوعی یکی از علوم جدید است که پس از جنگ جهانی دوم مطرح شد و جان مک کارتی از دانشگاه پرینستون در سال ۱۹۵۶، نام آن را انتخاب کرد. اغلب این طور پنداشته می شود که انسان نمی تواند پدیده ای خلق کند که از مغزش کارایی بیشتری دارد؛ لیکن آدمی مانند دستگاه بزرگی است که می تواند فکر خود را صرف کارهای مختلف کند و بنابراین دستگاه هایی بسازد که هریک در حوزه معین، کارایی و بازدهی بیشتری از خود او دارند. از سوی دیگر، انسان خود را خردمند و دارای قابلیت های ذهنی بسیار می داند؛ لذا تلاش او برای آسان کردن کارها و سرعت بخشیدن به انجام امور، سبب ظهور مغزهای الکترونیکی و تحول بزرگی در این زمینه شده است.

۱-۲- استانداردهای نظارتی

استاندارد دستورالعمل هایی را برای مدیریت و مدیریت فناوری های هوش مصنوعی ارائه می دهد و در واقع یک رویکرد سیستماتیک برای پرداختن به چالش های مرتبط با پیاده سازی هوش مصنوعی در چارچوب یک سیستم مدیریت شناخته شده ارائه می دهد که حوزه هایی مانند اخلاق، مسئولیت پذیری، شفافیت و حریم خصوصی داده ها را پوشش می دهد و برای نظارت بر جنبه های مختلف هوش مصنوعی طراحی شده تا یک رویکرد یکپارچه برای مدیریت پروژه های هوش مصنوعی، از ارزیابی تا مدیریت ریسک را ارائه دهد و پایه و اساس استفاده اخلاقی، ایمن و آینده نگر از هوش مصنوعی را در فراهم می نماید. این استاندارد اولاً، تضمین می کند که ارزش هوش مصنوعی برای رشد شناخته شده است و سطح صحیح نظارت وجود دارد. ثانیاً، سیستم مدیریت سازمان را قادر می سازد تا به طور فعال رویکرد خود را در راستای توسعه تصاعدی فناوری تطبیق دهد. در نهایت، سازمان ها را تشویق می کند تا ارزیابی های ریسک هوش مصنوعی را انجام دهند و فعالیت های کاهش ریسک هوش مصنوعی را در فواصل منظم تعریف کنند (علوی شاد، ۱۴۰۳: ۱).

۱-۳- اوصاف نماینده هوش مصنوعی

در ابتدای این بحث لازم است به تمیز نماینده الکترونیکی از نماینده هوشمند بپردازیم. نماینده الکترونیکی را می توان برنامه رایانه ای ساده ای دانست که دارای دانش از پیش تعریف شده است و

برای اجرای دستورات در فضای مجازی به کار برده می شود تا به طور خودکار طبق برنامه کاربر خود عمل کند. اما نماینده هوشمند یا به تعبیر برخی فوق هوشمند، برخلاف نماینده الکترونیکی، از توانایی خودسازماندهی بالایی برخوردار بوده و با توجه به داده های اولیه از محیط، تجارب قبلی و اطلاعات فعلی خود، قادر به بروز رفتارهایی غیر قابل پیش بینی است و حتی توان تغییر یا اصلاح اطلاعات خود را نیز دارد. در واقع این نماینده تنها ابزار پردازش و ضبط اطلاعات نیست؛ بلکه دارای قدرت پردازش مستقل، ارسال اطلاعات، تفکر، تصمیم گیری و عمل به آنهاست. او همچنین قادر است اطلاعات، عقاید، تمایلات، اهداف و ارزش هایش را مدیریت کند؛ اعمالی که از نماینده الکترونیکی ساده بر نمی آید. (Francisco, ۲۰۰۷: ۳۵۸).

مفهوم هوشمندی به درجه رفتار منطقی و یادگیرنده، توانایی قبول و بیان اهداف کاربر و انجام وظایف تفویض شده به نماینده برمی گردد. سطوح بالاتر هوشمندی، اشکال دیگر فهم و درک و دلیل آوری را در خصوص اینکه کاربر چه می خواهد بکند و چه برنامه ریزی برای رسیدن به هدف دارد، دربرمی گیرد. فراتر از آن، نظام هایی هستند که قابلیت یادگیری بالایی دارند و با توجه به اهداف کاربر و منابع در دسترس، با محیط خود منطبق می شوند. نمایندگان هوشمندی که در تجارت الکترونیک به کار برده می شوند، هدایت و اداره امور را در بازارهای اینترنتی به طرز شگرفی برعهده دارند. آنها به کار گرفته می شوند تا به مردم کمک کنند زمان های تلف شده برای خرید و فروش ها و در نتیجه هزینه های معاملات را کاهش دهند. شناسایی معاملات و احتیاجات مصرف کننده، بازیابی اطلاعات در خصوص اینکه چه چیزی خریداری شود تا نیازها برآورده گردد، ارزیابی اطلاعات به منظور تعیین اینکه کالا از چه کسی خریداری یا به چه کسی فروخته شود، روش تعیین مفاد و شروط قرارداد و ارزیابی رضایت مشتری، مجموعه فعالیت های اطلاعاتی آنها هستند. (ian, ۱۹۹۹: ۱۹۲). خصوصیات و ویژگی هایی که به نمایندگان هوشمند نسبت داده می شوند به دو بخش تقسیم می گردند: خصوصیات اساسی و مشترک که عبارتند از استقلال و خودمختاری، واکنش پذیری، تحرک و پویایی، قابلیت همکاری و هدفمندی؛ خصوصیات فرعی و تکمیلی که علاوه بر آگاهی، دانشمندی، صحت، صداقت و دارا بودن اراده و اعتقاد، عبارت از قابلیت یادگیری، عقلانیت و خلاقیت می باشند. در ادامه، به ترتیب، به هریک مختصراً خواهیم پرداخت:

۱-۳-۱ استقلال و خودمختاری

این ویژگی را هم نماینده الکترونیکی و هم نماینده هوشمند، هر دو، دارا می باشند. اما سطح و



میزان آن در هریک، متفاوت با دیگری است. استقلال بدین معناست که نماینده بدون دخالت مستقیم انسان یا سایر عوامل، می تواند فعالیت کند و بر اعمال و حالات درونی خود درجه ای از کنترل و تسلط را اعمال نماید؛ ولی میزان آن در هر نوع نماینده، به دایره عملکرد نوشته شده برای او بستگی دارد. هرچند بهتر است این وصف را در مفهوم دقیق آن فقط برای نماینده هوشمند به کار ببریم نه نماینده الکترونیکی و صفت خودکار بودن را به نماینده الکترونیکی نسبت دهیم؛ چرا که تنها نماینده هوشمند می تواند مستقلاً تصمیم گیری کند، نه اینکه صرفاً برنامه نوشته شده ای را به صورت اتوماتیک اجرا نماید.

۱-۳-۲ واکنش پذیری، تحرک و پویایی

یعنی نماینده می تواند محیط اطراف را درک کرده و نسبت به تغییرات حاصله در آن، به موقع واکنش نشان داده، به طور انتخابی و گزینشی عمل کند. نمایندگان هوشمند غالباً ساکن نیستند و در محیط های مجازی به سفر می پردازند، از رایانه ای به رایانه دیگر می روند و از صفحه ای به صفحه دیگر حرکت می کنند تا جستجوی خود را تکمیل کرده و مأموریتشان را به درستی انجام دهند. (۳: ۲۰۰۶، onostori).

۱-۳-۳ قابلیت انطباق و همکاری

نمایندگان هوشمند قادرند با عادات و خواسته های کاربر خود، با این فرض که اصلاً تعارضی بین اهدافشان وجود ندارد، هماهنگ شوند. نماینده هوشمند قادر به تعامل با انسان ها یا سایر نمایندگان به شیوه ای دوستانه و مبتنی بر همکاری می باشد. این همان ویژگی است که کنت آن را عمل اجتماعی هوشمندانه می نامد و معتقد است این خصیصه مبتنی بر اهلیت یک شخص است.

۱-۳-۴ هدفمندی و قابلیت یادگیری

نماینده هوشمند نمونه بارزی از نماینده مقصدگراست که برعکس نمایندگان انسانی، تعهدش به نتیجه می باشد. از او انتظار می رود اعمال خود را به گونه ای انجام دهد که به اهدافش برسد. وظایف نباید به نماینده ای تفویض شود که کاربر وی نمی تواند از انجام وظیفه طبق خواسته خود اطمینان حاصل کند؛ لذا نماینده در خصوص مرجحات و برنامه های رفتاری کاربرش باید تعلیم پذیر باشد. او

همچنین باید دارای قابلیت استنتاج و استدلال باشد تا بتواند آموزه های خود را به درستی به کار گیرد.

۱-۳-۵- عقلانیت و خلاقیت

منظور از عقلانیت این است که نماینده هوشمند در راستای یک هدف مشخص حرکت کند و اهداف متعارض را با هم پی گیری ننماید. همچنین در راه رسیدن به هدف خود موانع موجود را بردارد. در حقیقت رفتار نماینده هوشمند در صورتی عقلایی است که مشابه و نزدیک به رفتار نشان داده شده توسط یک انسان متخصص در موقعیتی مشابه باشد. علم هوش مصنوعی در زمینه طراحی و ساخت نمایندگان هوشمند تا آنجا پیش رفته که به خصوصیات و ویژگی های آنان قابلیت ارتقاء داده است. پس یک نماینده هوشمند بسیار سریع تر، قوی تر و مناسب تر از یک انسان معمولی می تواند تفکر، تصمیم گیری و عمل نماید. این خود به معنای حد بالای خلاقیت در نمایندگان هوشمند است. به علاوه آنان به هنگام شکست اقدامات اولیه شان می توانند به خوبی از پس شرایط برآمده و محاسبات بسیار پیچیده، سریع و هم زمان انجام دهند. (shoyama, ۲۰۰۵: ۱۲۹).

۱-۴-۱- مبنای مسئولیت مدنی هوش مصنوعی در قراردادهای تجاری

۱-۴-۱- مسئولیت مبتنی بر تقصیر

مطابق ماده ۹۵۳ قانون مدنی ایران، تقصیر به معنای تعدی و تفریط است. با این مبنا، اگر زیان دیده رابطه سببیت میان زیان و تقصیر واردکننده زیان را احرازاند، مسئولیت اثبات می شود. مبنای تقصیر در صورتی که هوش مصنوعی به صورت نادرست استفاده شود، قابل توجیه خواهد بود؛ زیرا بر اساس این تئوری می توان مالک، تولیدکننده، طراح، و سایر عوامل تجاری سازی هوش مصنوعی را مسئول دانست. به منظور اثبات مسئولیت تولیدکننده لازم است، ابتدا بی احتیاطی و تخطی وی از تعهدات قانونی مراقبت (که وجود این تعهد نیز نیازمند اثبات است) ثابت شود؛ و نیز اینکه ناشی از این نقض، آسیب هایی به زیان دیده وارد شده است. بنابراین، با وقوع ضرر و استناد آن به هوش مصنوعی، تولیدکننده مسئول است؛ مگر آنکه عدم تقصیر خود را اثبات کند، که امری قابل تأمل است. (رجبی، ۱۳۹۸: ۴۵۰).

قراردادهای هوشمند، یکی از ابزارهای کارآمد و مؤثر برای ورود به بازارهای جهانی هستند. قراردادهای هوشمند، تحت نظارت هوش مصنوعی در بستر بلاک چین منعقد می‌شوند و عوض قراردادی در آنها، دارایی‌های هوشمند یا ارزهای رمزنگاری شده دیجیتالی می‌باشد. عنصر قصد یکی از ارکان تشکیل هر قراردادی در نظامات حقوقی تلقی می‌گردد و ابراز و احراز آن شرط لازم برای تشکیل و اجرای هر قراردادی است. اعتبار این قراردادها نیز منوط به اثبات امکان احراز عنصر قصد به روشی مطمئن و اصیل است. ابراز قصد متعاملین در قراردادهای هوشمند از طریق مکانیسم‌های تخصیص مجوز استفاده از امضاهای دیجیتالی، مکانیسم‌های تخصیص مجوز استفاده از ارزهای مجازی و سازوکارهای برخورداری از سیستم‌های اطلاعاتی، انجام می‌شود. همچنین در قراردادهایی که به نمایندگی هوش مصنوعی انجام می‌گیرد، معامله از طریق نیابت که در سامانه‌های هوشمند ظهور یافته، انجام می‌گیرد. تأمین وصف محرمانگی و اصالت محتوا و امضای قرارداد هوشمند و اطمینان از اهلیت و قصد جدی طرفین و ملائت آنها، دخالت گسترده مقامات عمومی و دولتی را موجب شده است که در قراردادهای سنتی سابقه ندارد به گونه‌ای که می‌توان گفت اصل رضایی بودن کنار گذاشته شده و ابراز اراده معتبر در این قبیل معاملات رنگ و بوی خاصی به خود گرفته است. (رشوندبوکانی و مهدی، ۱۳۹۸: ۲۷۱).

الف) مسئولیت محض

بر اساس این نظریه، مسئولیت ناشی از خود فعل است. از این رو، در مسئولیت محض احراز تقصیر نیاز نیست. بنابراین، این نظر در موارد خاص اعمال می‌شود؛ آنجا که مقنن تصریح دارد و عمدتاً مسئولیت ناشی از رفتار همراه با خطر به شمار می‌رود. در بیشتر سیستم‌های حقوقی، این نظر در سه زمینه صدمه ناشی از حیوانات وحشی، مسئولیت ناشی از محصول، و فعالیت‌های خطرناک غیر متعارف کاربرد دارد و البته به نظر می‌رسد نمی‌توان صرف تولید هوش مصنوعی را محصول خطرناک دانست؛ لکن قانون‌گذار می‌تواند برای زیان دیده، با فرض تقصیر، تسهیل در اثبات قائل شود. (محمدی و موسوی، ۱۴۰۲: ۱۰).

ب) استناد عرفی

استدلالی که در رد نظریه شیء و محصول بودن هوش مصنوعی آمده و قواعد مسئولیت ناشی از عیب تولید کالا را منطبق با هوش مصنوعی نمی‌داند، این است که اولاً، هوش مصنوعی سامانه یادگیری است که تجارب خود را می‌آموزد و تصمیمات مستقل می‌گیرد و فقط زمانی سازنده مسئول است که

بتوان زیان را به او منتسب کرد. دوماً، ورود زیان از ناحیه این محصول (هوش مصنوعی)، به گونه ای است که گاه رابطه سببیت را از بین می برد و زیان قابل انتساب به مالک یا متصرف و متصدیان نیست. بنابراین، تحلیل دیگر تبیین و توجیه مسئولیت هوش مصنوعی، اعم از خطرناک و غیر خطرناک، در حقوق ایران بر مبنای استناد عرفی است.

۱-۴-۲- مسئولیت مشترک

هنگام بررسی و تعیین اشخاص مسئول، حسب مورد، ممکن است هر یک از تولیدکننده، طراح، فروشنده، مالک، یا متصرف هوش مصنوعی مسوول خسارت های ناشی از آن شناخته شوند و از این رو مبنای مسئولیت نیز ممکن است به تبع و متناسب با هر یک تبیین و دگرگون شود. به طور کلی، در صورت تعدد اشخاص مسئول در فرایند تولید و توزیع و بهره گیری از هوش مصنوعی، مسئولیت ایشان در حقوق ایران، با توجه به استثنایی بودن مسئولیت تضامنی، اشتراکی است. به علاوه، با توجه به حرفه ای بودن برنامه نویسی الگوریتم های هوش مصنوعی و ملاحظات نظارتی سازمان های تأییدکننده ایمنی فناوری های نوظهور، می توان به مسئولیت های اشتراکی بین برنامه نویسان، توسعه دهندگان، نهادهای مرتبط و در مواردی دولت ها قائل شد؛ که بر پیچیدگی نظام مسئولیتی می افزاید.

۱-۴-۳- مسئولیت مبتنی بر فعل غیر (مسئولیت نیابتی)

مبنای مسئولیت مدنی هوش مصنوعی را می توان در قالب «مسئولیت مبتنی بر فعل غیر» نیز تبیین کرد. روآوران به این دیدگاه ابتدا مسئولیت را صرفاً بر مالک بار می کنند، اما با این ایراد مواجه می شوند که اعمال هوش مصنوعی از مالک مستقل است و بر اساس طرح سازنده و طراح اقدام می کند. این نظریه با تبیین مناسب، تأمین کننده مزایای هر دو «نظریه محصول» و «نظریه شخص حقوقی» و رافع چالش های هر یک به نظر می رسد؛ بدین ترتیب که با پذیرش هوش مصنوعی در مقام شخص حقوقی (غیر)، مسئولیت را حسب استناد عرفی و به نحو اشتراکی به دوش یک یا چند عامل انسانی و اشخاص حقوقی مرتبط می افکند. (ذاکری نیا، ۱۴۰۲: ۱۳۹).

۲- تأثیر الگوریتم های هوش مصنوعی بر حریم خصوصی

۲-۱- جمع آوری و پردازش داده ها

الگوریتم‌های هوش مصنوعی برای یادگیری و بهبود عملکرد خود به داده‌های وسیع و متنوعی نیاز دارند. این داده‌ها معمولاً شامل اطلاعات شخصی افراد هستند که ممکن است بدون رضایت آن‌ها جمع‌آوری شوند. به عنوان مثال:

۲-۱- داده‌های موقعیت جغرافیایی و اجتماعی

بسیاری از اپلیکیشن‌ها برای بهبود خدمات خود، موقعیت جغرافیایی کاربران را جمع‌آوری می‌کنند. شبکه‌های اجتماعی اطلاعاتی درباره علایق، رفتارها و ارتباطات کاربران جمع‌آوری می‌کنند. این جمع‌آوری داده‌ها می‌تواند به نقض حریم خصوصی منجر شود و اعتماد عمومی را کاهش دهد. همچنین، عدم آگاهی افراد از نحوه استفاده از داده‌هایشان، می‌تواند احساس ناامنی و نگرانی در مورد حریم خصوصی ایجاد کند. (کیانی، ۱۴۰۲: ۱۳).

۲-۲- تحلیل رفتارهای فردی

الگوریتم‌های هوش مصنوعی قادر به تحلیل رفتارها و الگوهای فردی هستند. این تحلیل‌ها می‌توانند به شناسایی نقاط ضعف و نیازهای افراد کمک کنند، اما در عین حال می‌توانند به سوءاستفاده‌های احتمالی از اطلاعات شخصی منجر شوند. به عنوان مثال:

۲-۱-۲- هدف‌گذاری تبلیغاتی

شرکت‌ها می‌توانند با استفاده از داده‌های جمع‌آوری شده، تبلیغات را به صورت هدفمند به افراد خاصی نمایش دهند. این موضوع ممکن است به نقض حریم خصوصی منجر شود، زیرا افراد ممکن است احساس کنند که تحت نظارت قرار دارند.

۲-۲-۲- تحلیل احساسات

برخی از الگوریتم‌ها می‌توانند احساسات افراد را از طریق تحلیل متن یا تصویر شناسایی کنند. این تحلیل‌ها می‌توانند به سوءاستفاده‌های احتمالی منجر شوند، به ویژه در زمینه‌های سیاسی یا اجتماعی.

۲-۳- تصمیم‌گیری‌های خودکار، استخدام و قضاوت قانونی

الگوریتم‌های هوش مصنوعی می‌توانند در فرآیندهای تصمیم‌گیری خودکار در زمینه‌های مختلف مانند استخدام، اعتبارسنجی و حتی قضاوت قانونی استفاده شوند. این تصمیمات می‌توانند تأثیرات عمیقی بر زندگی افراد داشته باشند. به عنوان مثال: برخی شرکت‌ها از الگوریتم‌ها برای انتخاب متقاضیان مناسب استفاده می‌کنند. اگر داده‌های ورودی به این الگوریتم‌ها شامل تبعیض‌های نژادی یا جنسیتی باشد، ممکن است به نابرابری در استخدام منجر شود. در برخی کشورها، الگوریتم‌ها برای پیش‌بینی رفتار مجرمانه و تعیین مجازات‌ها استفاده می‌شوند. این موضوع می‌تواند به تبعیض و ناعدالتی‌های جدی منجر شود.

۳- چالش‌های شفافیت و مسئولیت‌پذیری

۳-۱- عدم شفافیت الگوریتم‌ها

بسیاری از الگوریتم‌های هوش مصنوعی به عنوان «جعبه سیاه» شناخته می‌شوند، به این معنی که فرآیندهای داخلی آن‌ها برای کاربران و حتی توسعه‌دهندگان نامشخص است. این عدم شفافیت می‌تواند به عدم اعتماد منجر شود و افراد را از استفاده از خدماتی که این الگوریتم‌ها را به کار می‌برند، منصرف کند. به عنوان مثال:

۳-۱-۱- عدم قابلیت توضیح

بسیاری از الگوریتم‌ها نمی‌توانند توضیح دهند که چرا یک تصمیم خاص اتخاذ شده است، که این موضوع می‌تواند به عدم اعتماد کاربران منجر شود.

۳-۱-۲- پیچیدگی‌های فنی

بسیاری از کاربران اطلاعات کافی درباره نحوه کارکرد الگوریتم‌ها ندارند و این موضوع می‌تواند به سوءاستفاده‌های احتمالی منجر شود.

۳-۲- مسئولیت‌پذیری، مسئولیت توسعه دهندگان و شرکت‌ها

در صورت بروز خطا یا نقض حریم خصوصی، سوالات زیادی درباره مسئولیت‌پذیری وجود دارد. آیا توسعه‌دهندگان، شرکت‌ها یا خود الگوریتم‌ها مسئول هستند؟ تعیین مسئولیت در چنین مواردی پیچیده است و نیازمند قوانین و مقررات جدیدی است. به عنوان مثال: آیا توسعه‌دهندگان باید

مسئولیت تصمیمات اتخاذ شده توسط الگوریتم‌ها را بر عهده بگیرند؟ آیا شرکت‌ها باید برای سوءاستفاده‌های احتمالی از داده‌های کاربران مسئول باشند؟

۳-۳- تبعیض و نابرابری، تبعیض نژادی و تبعیض جنسیتی

الگوریتم‌های هوش مصنوعی می‌توانند تحت تأثیر داده‌های ورودی قرار گیرند و در نتیجه ممکن است تبعیض‌هایی را در تصمیم‌گیری‌ها ایجاد کنند. این موضوع می‌تواند به نابرابری‌های اجتماعی و اقتصادی منجر شود و حقوق بشر را تحت تأثیر قرار دهد. به عنوان مثال: اگر داده‌های آموزشی الگوریتم‌ها شامل تبعیض‌های نژادی باشند، ممکن است الگوریتم‌ها نیز به طور خودکار این تبعیض‌ها را بازتولید کنند. در حوزه استخدام، الگوریتم‌ها ممکن است به نفع یک جنس خاص عمل کنند و این موضوع به نابرابری‌های جنسیتی دامن بزند. چالش‌های حریم خصوصی در عصر هوش مصنوعی در دنیای انبوه اطلاعات، تجزیه و تحلیل‌های سریع و آنی در کنار فناوری هوش مصنوعی و کاربردهای حاصل از آن، اهمیت حفظ حریم شخصی افراد و معیارهای اخلاقی برای استفاده از این نوع اطلاعات، اهمیت حیاتی پیدا کرده است. حدود سال ۲۰۱۰ بود که شرکت تارگت، یک شرکت خرده‌فروشی زنجیره‌ای معروف در آمریکا، با استفاده از الگوریتمی که با بررسی الگوی خرید افراد، زنان باردار را شناسایی کرده و به منظور تشویق و مشتری‌مداری برای آنها کوپن ارسال می‌کرد، به دردسر افتاد. یکی از این کوپن‌ها برای خانمی ارسال شد که هنوز بارداری خودش را به پدرش اعلام نکرده بود و به واسطه این کوپن، پدر زودتر از زمان برنامه‌ریزی شده از بارداری دختر مطلع شد. (۱۹: ۲۰۲۰، teach) در مورد دیگر و البته حساس‌تر و گسترده‌تر، یک شرکت فناوری، قوانین حریم شخصی کانادا را نقض کرده بود. شرکت کلیر ویو هوش مصنوعی متهم به انتشار و به کارگیری بدون مجوز اطلاعات زیست‌سنجی (بیومتریک) افراد در کانادا شد. این شرکت آمریکایی بدون اجازه افراد، تصاویر افراد بزرگسال و حتی کودکان را برای دوربین‌های نظارتی، تشخیص چهره و حتی به منظورهای فروش و تجارت جمع‌آوری کرده بود. (۹۰: ۲۰۲۱، pearce) ادعای این شرکت مبنی بر استفاده از تصاویر افراد، در دسترس بودن آزادانه آنان در اینترنت بوده است و در پی خود یک چالش حقوقی به دنبال داشت. این موارد و سایر چالش‌های مشابه، مباحث اخلاقی زیادی را پیرامون استفاده هوش مصنوعی در تجزیه و تحلیل داده‌ها و حفظ حریم شخصی افراد به وجود آورد. سوال مهم‌تر این است که شرکت‌های کسب‌وکار هوشمند اساساً مجاز به دانستن چه چیزهایی درباره افراد هستند. در اصل، کسب‌وکارهایی که با داده‌های افراد و پردازش آنها سروکار دارند، کسب‌وکارهای هوشمند هستند و باید به طور ویژه‌ای مسائل اخلاقی پیرامون استفاده از اطلاعات شخصی افراد را در نظر بگیرند.



متأسفانه در این زمینه همچنان خلاءهای قانونی به شکل محسوسی در بسیاری از حوزه‌ها به قوت خود باقی مانده است. افراد در اقصی نقاط جهان هم ترس‌های به جا و مشترکی دارند، حدود ۹۸ درصد مردم آمریکا احساس می‌کنند که باید کنترل بیشتری بر اشتراک‌گذاری داده‌های‌شان داشته باشند، حدود ۷۹ درصد ساکنان هندوستان همچنان نسبت به ارائه داده‌های‌شان به طرف ثالث احساس ناخوشایندی دارند و به طور کلی هنوز ۷۴ درصد مردم جهان در خصوص داده‌های شخصی‌شان ابراز نگرانی می‌کنند. (۱۸: ۲۰۲۱، pearce)

با توجه به افزایش چشمگیر توسعه و بکارگیری سیستم‌های هوش مصنوعی و نیاز پایان ناپذیر این سیستم‌ها به داده‌های شخصی، روز به روز حق بر حریم خصوصی که در منشور بین‌المللی حقوق بشر به دفعات مورد تأکید قرار گرفته است بیش از هر زمان دیگری با چالش‌های فراوانی مواجه شده است. حق بر حریم خصوصی یکی از حقوق بنیادین افراد است که قدرت انتخاب سرنوشت فردی به دور از دید و مداخله دیگر افراد را فراهم می‌آورد و به افراد این اجازه را می‌دهد که در خلوت خود به دور از ترندهای اجتماع به رشد و شکوفایی فردی و گوهر وجودی خود دست یابند. در سال‌های اخیر توان محاسباتی بالای هوش مصنوعی و ظهور فناوری اطلاعات دیجیتال دست در دست هم موجب شدند تا بیش از هر زمان دیگری جمع‌آوری و ذخیره‌سازی و پردازش داده‌های شخصی افراد تسهیل شود که می‌تواند منجر به نقض خودمختاری افراد و ایجاد زمینه‌های دستکاری در افکار و عقاید عموم افراد جامعه شود (طباطبایی پور، ۱۴۰۲: ۱).

۳-۴- جمع‌آوری و پردازش داده‌های شخصی

هوش مصنوعی برای آموزش مدل‌ها و ارائه خدمات خود نیاز به حجم عظیمی از داده‌های شخصی دارد. این داده‌ها شامل اطلاعات حساس مانند مکان، تاریخچه جستجو، اطلاعات پزشکی، خریدها و حتی احساسات و رفتارهای فردی هستند. یکی از اصلی‌ترین چالش‌ها در زمینه حریم خصوصی، جمع‌آوری و پردازش این داده‌هاست. برخی از این اطلاعات می‌توانند برای شناسایی هویت افراد استفاده شوند و در صورت افشا، تهدیداتی جدی برای حریم خصوصی به همراه خواهند داشت.

۳-۵- عدم شفافیت در تصمیم‌گیری‌های هوش مصنوعی

یکی از مشکلات عمده در استفاده از هوش مصنوعی، عدم شفافیت در فرایندهای تصمیم‌گیری است. مدل‌های یادگیری ماشین، به ویژه مدل‌های پیچیده مانند شبکه‌های عصبی، به گونه‌ای عمل می‌کنند

که قابل درک برای انسان‌ها نیستند. این عدم شفافیت می‌تواند منجر به تصمیم‌گیری‌های ناعادلانه یا تبعیض‌آمیز شود که ممکن است حقوق افراد و حریم خصوصی آنها را نقض کند. همچنین، در بسیاری از موارد، افراد حتی از اینکه تحت تاثیر الگوریتم‌ها قرار دارند آگاهی ندارند، که این خود می‌تواند تهدیدی برای حقوق اولیه آنان باشد.

۳-۶- هک و سوء استفاده از داده‌ها

داده‌های جمع‌آوری شده برای آموزش و کارکرد هوش مصنوعی می‌توانند هدف حملات سایبری قرار بگیرند. در صورتی که این داده‌ها به‌طور ناخواسته یا عمدی توسط هکرها دزدیده یا افشا شوند، حریم خصوصی افراد به شدت تهدید خواهد شد. حملات به سیستم‌های هوش مصنوعی می‌توانند پیامدهای منفی زیادی داشته باشند، از جمله افشای اطلاعات حساس و هویت‌زدایی کاربران.

۳-۷- پیش‌بینی و نفوذ در رفتار فردی

با استفاده از هوش مصنوعی و تحلیل داده‌های جمع‌آوری شده، شرکت‌ها و سازمان‌ها قادر به پیش‌بینی رفتارهای فردی کاربران و حتی تاثیرگذاری بر تصمیمات آن‌ها هستند. این پیش‌بینی‌ها می‌توانند به طرق مختلف از جمله تبلیغات هدفمند، دستکاری در تصمیم‌گیری‌ها یا حتی نقض آزادی‌های فردی به خطر بیفتند.

۴- تهدیدات ناشی از هوش مصنوعی برای حریم خصوصی

۴-۱- بازنمایی نادرست و سوءاستفاده از داده‌ها، پایش دائمی و نقض آزادی‌ها

در برخی موارد، هوش مصنوعی ممکن است اطلاعات شخصی افراد را به اشتباه تجزیه و تحلیل کرده و اطلاعات نادرست یا تعمیم یافته‌ای را در اختیار سایرین قرار دهد. برای مثال، سیستم‌های تشخیص چهره ممکن است خطاهایی در شناسایی هویت افراد داشته باشند، که این موضوع می‌تواند منجر به نقض حریم خصوصی و حتی سوء استفاده‌های قانونی و اجتماعی گردد. با استفاده از ابزارهای هوش مصنوعی، برخی از سازمان‌ها ممکن است به‌طور پیوسته رفتارهای آنلاین و حتی آفلاین افراد را پایش کنند. این امر می‌تواند منجر به نقض آزادی‌های فردی و تهدید جدی برای حریم خصوصی در دنیای دیجیتال شود. به عنوان مثال، استفاده از فناوری‌های نظارتی مانند دوربین‌های تشخیص چهره در مکان‌های عمومی می‌تواند باعث شود که افراد تحت نظارت دائمی قرار گیرند.

۴-۲- استفاده از داده‌ها برای دستکاری اجتماعی

هوش مصنوعی می‌تواند برای دستکاری در افکار عمومی یا حتی تغییر نظرات و رفتارهای افراد از طریق الگوریتم‌های پیچیده و تحلیل داده‌های شخصی استفاده شود. به‌ویژه در شبکه‌های اجتماعی، هوش مصنوعی می‌تواند برای ایجاد فیلترهای اطلاعاتی یا معرفی محتوای خاص، که ممکن است منجر به انتشار اطلاعات نادرست یا تفرقه‌افکنی شود، به کار رود.

۴-۳- عدم امنیت داده‌ها و اطلاعات

چالش‌های مربوط به امنیت داده‌ها و حریم خصوصی در ارتباطات بین‌المللی به مسائلی مرتبط با حفاظت از اطلاعات شخصی و امنیت داده‌ها در محیط‌های بین‌المللی اشاره دارد. این چالش‌ها معمولاً به علت پیشرفت تکنولوژی ارتباطات و استفاده گسترده از این تکنولوژی‌ها در تبادل اطلاعات میان کشورها و افراد به وجود می‌آیند. در ادامه، به توضیح دو چالش اصلی در این حوزه می‌پردازیم.

در مورد چالش‌های امنیت داده‌ها در ارتباطات بین‌المللی و کاربرد هوش مصنوعی باید گفت که یکی از مهمترین نگرانی‌ها، خطر حملات سایبری و نفوذ به سامانه‌های رایانه‌ای و دزدی اطلاعات حساس و محرمانه است. با توجه به وابستگی فزاینده بسیاری از فعالیت‌های ضروری به فضای مجازی، این حملات می‌توانند باعث بروز مشکلات و اختلالاتی در سطح ملی و بین‌المللی شوند. همچنین احتمال سوءاستفاده از داده‌های شخصی افراد توسط عوامل خصوصی یا دولتی برای اهدافی چون فریب یا تهدید افراد، یکی دیگر از چالش‌های مهم است. جاسوسی دیجیتال و نظارت گسترده بر ارتباطات و فعالیت‌های آنلاین افراد نیز می‌تواند به نقض حریم خصوصی آنها منجر شود. در مجموع، بدون وجود قوانین و مقررات کافی برای حفاظت از داده‌ها، ارتباطات بین‌المللی در عصر هوش مصنوعی با چالش‌ها و تهدیدات جدی روبرو خواهد بود. (۱۸۰: ۲۰۲۱، bachelet)

یکی از مسائل مهم، تهدید حریم خصوصی افراد در اثر جمع‌آوری و تجزیه و تحلیل گسترده داده‌های شخصی آنهاست. الگوریتم‌های هوش مصنوعی قادرند الگوهای رفتاری افراد را استخراج کنند و پیش‌بینی‌هایی در مورد آنها انجام دهند که میتواند منجر به طبقه‌بندی‌ها و تصمیم‌گیری‌های ناعادلانه شود.



همچنین وجود قوانین و مقررات مشخص و یکپارچه برای حفاظت از داده ها در سطح بین المللی یک چالش مهم است. مسائل مربوط به مالکیت و کنترل داده ها در محیط های ابری و بین المللی نیز پیچیده و نیازمند توجه جدی است. در مجموع، همکاری های بین المللی و تدوین چارچوب های حقوقی مناسب برای حل این چالش ها ضروری به نظر می رسد.

کسب و کارهای هوشمند یا شرکت های فناوری که به مدد هوش مصنوعی با داده های اشخاص سروکار دارند، چه در زمان دسترسی مستقیم به انواع داده ها و چه در زمان پردازش داده ها باید حواس شان به معیارهای اخلاقی باشد. اما چرا و یا اساساً چه طور پیشرفت هوش مصنوعی می تواند بلای جان حریم شخصی افراد شود، مگر هدف اولیه بسیاری از کسب و کارها در استفاده از هوش مصنوعی، شناخت بهتر مشتری ها نیست؛ پس چه نگرانی های در این باره به وجود می آید؟

به طور کلی هوش مصنوعی به سه شکل می تواند حریم شخصی افراد را مورد چالش قرار دهد: ماندگاری داده ها: هوش مصنوعی ذخیره سازی داده ها را کم هزینه می کند، از این رو، شرکت های فناوری قادر خواهند بود که داده های ایجاد شده افراد را در بازه های زمانی طولانی تری ذخیره و نگه داری کنند.

۴-۳-۱ استفاده مجدد از داده ها

داده ها توسط افراد علاوه بر اینکه در یک زمان خاصی تولید شده اند، قطعاً هم برای خود دارای هدف خاصی بنیادین هستند، هوش مصنوعی می تواند به داده های از پیش موجود، کاربری های جدید ببخشد بی آنکه مولد اولیه داده روحش هم خبردار شود.

۴-۳-۲ سرریزی داده ها

یکی از اولین کاربردهای جذاب هوش مصنوعی، توانایی جمع آوری داده هایی انبوه در حجم بسیار بالا بوده است، گاهی این توانایی می تواند منجر به کسب بیش از حد داده های هدف مورد نیاز شود و آن شرکت فناوری به داده هایی دسترسی پیدا می کند که لزوماً نباید در دست داشته باشد (pearce, ۲۰۲۱: ۱۶). به طور کلی شرکت های فناوری که با هوش مصنوعی داده ها را جمع آوری می کنند، جمع آوری داده های شان از دو دسته منابع مستقیم و غیرمستقیم تأمین می شود. داده های مستقیم شامل اطلاعات تماس یا سابقه خرید افراد است. اما در نوع غیرمستقیم، جمع آوری

داده‌ها در اصطلاح پشت‌صحنه‌ای انجام می‌شود و از طریق استفاده موادی چون کوکی‌ها و سایر فناوری‌های ردیابی تحقق می‌یابد. (۱۰۰: ۲۰۲۲، usercentrics).

در تمامی این موارد، شاهد به خطر افتادن حفظ حریم شخصی افراد با در اختیار قرار دادن داده‌های شخصی‌شان با نیت دیگر ولی در نهایت بهره‌برداری به غیر از هدف اولیه توسط شرکت‌های فناوری مورد نظر هستیم. هوش مصنوعی در دهه‌های اخیر به طور نسبی پیشرفت چشمگیری داشته است و در حال حاضر در بسیاری از زمینه‌ها از جمله آموزش ماشینی، پردازش زبان طبیعی، مربی‌گری و رباتیک بکار می‌رود. با این وجود، همچنان چالش‌های مهمی در ارتباط با امنیت هوش مصنوعی و حفظ حریم خصوصی وجود دارد. (۱۸: ۲۰۱۵، fredrikson)

یکی از چالش‌ها امنیت اطلاعاتی است که بیانگر نیازمندی به محافظت در برابر دسترسی غیرمجاز به داده‌ها است. هوش مصنوعی به طور گسترده از داده‌های حساس مانند اطلاعات شخصی و حساب بانکی استفاده می‌کند و اگر این داده‌ها به دسترسی غیرمجاز بیافتند، ممکن است به نتایج و تصمیمات ناخواسته و ناپایداری منجر شوند. یک مسئله دیگر مربوط به حریم خصوصی است. استفاده از هوش مصنوعی ممکن است منجر به جمع‌آوری و تحلیل بزرگی از داده‌های شخصی شود. اگر این داده‌ها به شکل نادرست استفاده شوند یا بدون اجازه صاحب اطلاعات برای اهداف غیرقانونی استفاده شوند، حریم خصوصی آسیب می‌بیند. در حال حاضر، الگوریتم‌های هوش مصنوعی به طور گسترده از داده‌های آموزشی برای یادگیری استفاده می‌کنند. بدون دسترسی به داده‌های کافی و گوناگون، هوش مصنوعی نمی‌تواند یاد بگیرد و بینایی، گفتار و برداشت نکاتی شبیه به انسان نداشته باشد. اما، استفاده از داده‌های آموزشی ممکن است به انتقال تبعیض‌ها و تفاوت‌های زمینه‌ای مربوط به جنسیت، نژاد و سن منجر شود. (۹۰: ۲۰۲۱، yao) همچنین، میزان دقت و قدرت تصمیم‌گیری ماشین‌های هوش مصنوعی ممکن است بیشتر از فهم ما انسان‌ها باشد. این موضوع می‌تواند به تهدیدی برای امنیت فردی و جمعی تبدیل شود و منجر به استفاده ناصحیح از تصمیمات هوش مصنوعی گردد که باعث آسیب‌های جدی برای افراد و جوامع می‌شود.

۵- هوش مصنوعی و خطا؛ الگوریتم‌ها و مشکل نمایندگی؛ معنای «عیب»

در مورد هوش مصنوعی قبل از اینکه به جزئیات برسیم، باید سه موضوع فنی مهم را نیز مورد بحث قرار دهیم. یکی، که در زمینه مسئولیت تقصیر ایجاد می‌شود، مربوط به قواعد قانون عرفی در مورد



سهل انگاری است و تا چه حد می توان آنها را به طور مناسب در تصمیمات اتخاذ شده توسط هوش مصنوعی اعمال کرد. مورد دوم به موضوع آژانس مربوط می شود و اینکه چه کسی باید مسئولیت قانونی تصمیمات اتخاذ شده توسط هوش مصنوعی را بر عهده بگیرد. و سومین سوالی است که در رابطه با مسئولیت سخت به سبک مسئولیت محصول مطرح می شود، یعنی اینکه چه چیزی به عنوان هوش مصنوعی معیوب به حساب می آید. (soyer, tettenborn, ۲۰۲۲: ۷)

۵-۱- هوش مصنوعی و خطا

طبق قانون حاضر، مفهوم تقصیر در قانون قصور مستلزم فعل یا ترک فعل همراه با عدم انطباق وضعیت روانی انسان با معیار خاصی است (یا حداقل سهوی بودن منفی و قابل سرزنش آن). به دلیل تقصیر کارمند خود یا شخص دیگری در موقعیت مشابه، ۲۸ خرابی صرفاً توسط یک ماشین تحت کنترل آن، مانند راه اندازی رایانه برای نظارت بر ایمنی، شناسایی خطرات و یا انجام برخی از عملکرد مشابه، کافی نخواهد بود. باید خطای شخصی توسط یک شخص نشان داده شود، مانند یک کارمند، آن را کنترل یا برنامه ریزی می کند. (hagi esmaeili, ۲۰۲۴: ۹۰)

۵-۲- الگوریتم ها و نمایندگی

برای قابل اجرا کردن مفهوم ماشین سهل انگار که در بالا به آن اشاره شد، و همچنین پیشنهادی که بعداً ظاهر شد مبنی بر اینکه حداقل در برخی موارد باید بدون تقصیر در قبال آسیب ناشی از یک فرآیند هوش مصنوعی وجود داشته باشد، باید یک قاعده قانونی ایجاد کنیم. نمایندگی، یا انتساب، با فرض اینکه یک ماشین مقصر دیده شود، یا تصمیمی که توسط هوش مصنوعی گرفته می شود باید منجر به مسئولیت شدید شود، چه کسی پرداخت می کند؟ همانطور که در بالا ذکر شد، این نمی تواند خود ماشین باشد، نهادی که نه تمایل به مالکیت دارایی هایی برای جبران خسارت دارد و نه توانایی بیمه کردن خود به خود در برابر امکان پرداخت آنها. (برخلاف یک شرکت انسانی یا شرکتی، نمی تواند قرارداد کار یا نمایندگی را منعقد کند که کارفرما را مسئول اعمال یا ترک کارهای انجام شده در حین کار کند) (منصوری، ۱۴۰۰: ۱۵).

۵-۲-۱- هوش مصنوعی معیوب

همانطور که مسئولیت سختگیرانه محصول تحت قسمت اول قانون حمایت از مصرف کننده ۱۹۸۷۳۷ تعریف محصول معیوب را ضروری می کند، هر گونه مسئولیت موازی در قبال آسیب وارد شده توسط هوش مصنوعی حداقل نیاز به تعریفی از AI معیوب دارد .

۵-۲-۲- مسئولیت صدمات شخصی و مرگ

هوش مصنوعی در حال حاضر تعداد شگفت انگیزی از مسائل مربوط به ایمنی شخصی را کنترل می کند و این تأثیر احتمالاً با جهش و مرز افزایش می یابد. به غیر از وسایل نقلیه (موضوع قوانین جداگانه ای که در اینجا به تفصیل آن را بررسی نمی کنیم) می توان به کاربرد آن در درمان و تشخیص پزشکی اشاره کرد. در کنترل دسترسی و جهت دهی در محیط های خطرناک مانند معادن یا کارخانه ها. در کنترل هواپیماها، شناورها و هواپیماهای بدون سرنشین؛ در کنترل ترافیک؛ در تولید؛ و در طراحی ساختمانهای تجاری و مسکونی بزرگ.

۵-۲-۳- صدمات حیثیتی یا اعتباری

ما در اینجا با مداخله در تعدادی از منافع سنتی محافظت شده قانونی اشخاص حقیقی روبرو هستیم که از تمامیت بدنی کوتاهی برخوردارند، اما با وجود این، بر اساس قانون جرم قابل اثبات هستند: به ویژه حریم خصوصی، شهرت و حیثیت. تحت تأثیر استفاده از هوش مصنوعی قرار گیرد. برای مثال، تشخیص نادرست سرطان یا زوال عقل با استفاده از هوش مصنوعی، می تواند کاملاً جدا از هر آسیب واقعی، بر حیثیت و سلامتی تأثیر بگذارد. نرم افزار کنترل عملکرد قلب یا سایر عملکردهای بدن. علاوه بر این، داده کاوی و دستکاری داده های شخصی توسط الگوریتم آشکارا پیامدهای نگران کننده ای برای حریم خصوصی شخصی دارد. به مواردی فکر کنید که اطلاعات شخصی استخراج شده و سپس مورد سوء استفاده قرار گرفته یا توسط یک پردازشگر داده ذخیره شده و سپس به اشتباه به دلیل نقص در عملکرد رایانه پردازنده یا حتی سوء استفاده از هکرها یا خارجی منتشر شده است (تخشید، ۱۴۰۰: ۲۳۹).

۵-۲-۴- خسارت به اموال

در ماهیت چیزها، آسیب فیزیکی به اموال ممکن است کمتر از سایر انواع آسیب در نتیجه مشکلات هوش مصنوعی رخ دهد. اما کاملاً امکان پذیر است. جدا از وسایل نقلیه خودران، که تابع رژیم



سفارشی خود هستند، مواردی را در نظر بگیرید که هوش مصنوعی مورد استفاده در یک پروژه ساخت و ساز اشتباه می‌کند، یا فرآیندی که توسط هوش مصنوعی کنترل می‌شود، خراب می‌شود و باعث انفجار می‌شود که به ساختمان‌ها و وسایل نقلیه مجاور آسیب می‌رساند. (پناهی و همکاران، ۱۴۰۳: ۳۴).



نتیجه گیری

با افزایش سرعت اطلاعات و ارتباطات، به تبع آن حملات سایبری نیز پیشرفته تر می شود و ابزار مورد نیاز برای حفظ اطلاعات در مقابل آنان هم پیچیده تر می شود. در برخورد با تهدید امنیت سایبری و بهره گیری از تجزیه و تحلیل داده ها به کمک هوش مصنوعی و یادگیری ماشینی میزان دقت و سرعت عمل به طور چشمگیری افزایش می یابد. پیش بینی براساس تحلیل داده ها می تواند ناهنجاری های اینترنتی و بدافزارها را شناسایی کند و به منظور یافتن تهدیدهای داخلی و شناسایی کاربران درون سازمان ها و خنثی سازی عملیات آنها الگوهای رفتار کاربران را نیز تجزیه و تحلیل می کند. در قرن حاضر ارتباطات اینترنتی به بالاترین حد خود رسیده و همگان از تمامی امکانات و قابلیت های تجهیزات رایانه ای و ابزارهای ارتباطی برای انجام کارهای روزانه و پیشبرد اهداف خود بهره می گیرند. اکنون که شاهد وابستگی دولت ها، شرکت ها و شهروندان به ابزارهای اینترنتی هستیم و با توجه به حملات سایبری، مسئله امنیت سایبری به ویژه برای دولت ها به جهت محافظت از زیرساخت های حیاتی، نظامی یا دولتی بسیار ضروری است. هوش مصنوعی را می توان در سطح جهان برای پیشگیری و تشخیص جرائم هک های سایبری و تشخیص اخبار فیک استفاده کرد. بنابراین استفاده از سیستم های مبتنی بر هوش مصنوعی با قابلیت پیش بینی می تواند قبل از حملات سایبری آنها را تشخیص دهد. وابستگی امنیت ملی به فضای سایبر در زمینه تکنولوژی اطلاعات و ارتباطات سبب شده تا آسیب رساندن و مخدوش کردن این فضا تهدید جدی برای امنیت ملی محسوب شود. ورود به دنیای سیستم های مبتنی بر هوش مصنوعی به معنای تغییرات در حوزه های گوناگون و نیازمند وضع قوانین و مقررات اخلاقی و حقوقی است. نویسندگان قاطعانه بر این باورند که قوانین مسئولیت مدنی نباید به عنوان یک نماینده نظارتی ضمنی استفاده شود. بدون شک، تنظیم کننده ها باید مداخله کنند (و این موضوع در حال حاضر در حوزه های قضایی متعدد مورد بحث است) تا استانداردهای تولیدی و عملیاتی را با توجه به برنامه های هوش مصنوعی برای اطمینان از ایمنی این محصولات و همچنین محافظت از افراد اعمال کنند. با این حال، نباید فراموش کرد که نقش اساسی قانون تعهدات، ارائه مکانیزم رضایت بخش جبران خسارت است. نویسندگان ارزش های اساسی را که یک رژیم جرم باید از آنها محافظت کند و مشکلات فنی مختلف در رابطه با ایجاد مسئولیت برای استفاده از هوش مصنوعی را در نظر می گیرند که باید مورد توجه قرار گیرند، در این مقاله حمایت می کنند که نیاز به یک طرح جدید مسئولیت برای هوش مصنوعی وجود دارد که به خوبی با طرح موجود قانون تعهدات مطابقت دارد. پیشنهاد ما این است که هر مسئولیتی در قبال آسیبی که توسط هوش مصنوعی ایجاد

می‌شود، باید به موازات سایر مسئولیت‌ها باشد، با تغییراتی که فقط در مواردی ایجاد می‌شوند که ناهنجاری‌های قابل توجهی وجود دارد که باید با آنها برخورد کرد. باید دید که آیا این طرح در آزمون زمان مقاومت خواهد کرد یا خیر، اما شاید بهتر است در این مرحله به آرامی پیش برویم مگر اینکه و تا زمانی که نیاز محسوسی به اصلاحات اساسی‌تر وجود داشته باشد. هوش مصنوعی همیشه در مسیر پذیرش خود در شرکت‌ها موفق نبوده‌است و دلیل این عدم پذیرش این است که هوش مصنوعی به دلایل زیادی نتوانست اصول وعده داده شده را عملی کند. امروزه زمینه‌های زیادی وجود دارد که هوش مصنوعی می‌تواند با موفقیت به آنها وارد شود. چالش حباب فعلی به وجود آمده در مسیر پیشرفت هوش مصنوعی، حباب نبودن آن است. اینکه هوش مصنوعی وعده‌های بیش از حد داده است، یکی از دلایل به وجود آمدن این حباب است. تاکید بر هوش مصنوعی به عنوان یک ابزار حیاتی که باید در سیستم‌ها ادغام شود، راهی برای بهبود پذیرش هوش مصنوعی در شرکت فرصت‌های بزرگتر برای تمایز هر شرکت‌ها است.

لزوم تدوین چارچوب‌های قانونی و نظارتی بین‌المللی برای جلوگیری از سوءاستفاده از هوش مصنوعی علیه حقوق بشر.

سازمان بین‌المللی استانداردسازی دارای بیشترین فعالیت در زمینه استانداردسازی هوش مصنوعی در بین سطوح ملی و بین‌المللی می‌باشد، لذا کشورهایی که تمایل ورود به حوزه استانداردسازی هوش مصنوعی دارند، بهتر است سازمان بین‌المللی استانداردسازی را سر لوحه کار خود قرار دهند.

بیشتر کشورهای مطرح در استانداردسازی هوش مصنوعی، فعالیت خود را در سطح بین‌المللی انجام داده و از اسناد بین‌المللی در کشور خود استفاده نموده‌اند، لذا لازم است کشورها و یا حتی سازمان‌هایی که تمایل ورود به استانداردسازی حوزه هوش مصنوعی دارند با سازمان‌های بین‌المللی همکاری نموده و از اسناد تدوین شده توسط این سازمان‌ها که دارای اجماع جهانی و منطقه‌ای می‌باشد استفاده نمایند. توسعه قوانین و مقررات: نیاز به تدوین قوانین جدید برای حفاظت از حریم خصوصی و حقوق بشر در عصر هوش مصنوعی وجود دارد.

منابع

۱. امیری، جواد، حسینی، زکیه، (۱۴۰۲)، نقش هوش مصنوعی در تحول علم حقوق و ملزومات آن، چهارمین کنفرانس ملی پدافند سایبری.
۲. حکیم، مجتبی، ابراهیمیان، حسین، (۱۴۰۱)، بررسی فقهی و حقوقی سلب امنیت شهروندی در هوش مصنوعی، پژوهش های فقه و حقوق اسلامی.
۳. دروگری، ریحانه، کاوسی خسرقی، پریراد، (۱۴۰۲)، کاربرد هوش مصنوعی در حوزه پزشکی و چالش های حقوقی حفاظت از حریم خصوصی، اولین کنفرانس ملی ارتقای سلامت و چالش های حقوقی و پزشکی فراروی آن.
۴. ذاکری نیا، حانیه، (۱۴۰۲)، ماهیت و مبنای مسئولیت مدنی ناشی از هوش مصنوعی در حقوق ایران و کشورهای اتحادیه اروپا، گروه حقوق خصوصی و اسلامی، دانشکده حقوق و علوم سیاسی، دانشگاه شیراز، دوره بیستم، شماره اول.
۵. رجبی، عبدالله، (۱۳۹۸)، ضمان در هوش مصنوعی، مطالعات حقوق تطبیقی، دوره ۱۰، شماره ۲.
۶. سلطانی عمیدآبادی، سمیرا، (۱۴۰۲)، مردمک هوشمند: بررسی نقش هوش مصنوعی در نظارت بر جامعه، قلم مهر، چاپ اول.
۷. طباطبایی پور، فاطمه، (۱۴۰۲)، حفاظت از حق بر حریم خصوصی در کاربرد سیستم های هوش مصنوعی، دانشگاه شهید بهشتی، استاد راهنما: محمدحسین رضائی قوام آبادی.
۸. کیانی، رامین، (۱۴۰۲)، ابر چالش هموساپینس ها؛ لزوم تاسیس آژانس بین المللی هوش مصنوعی، تالار گفتگوی تخصصی حقوقی و سیاسی بین المللی انجمن ایرانی مطالعات سازمان ملل متحد.
۹. محمدی، فرهاد، موسوی، فرانک، (۱۴۰۲)، بررسی مسائل اخلاقی و حریم خصوصی هوش مصنوعی در آموزش، سومین کنفرانس بین المللی مهندسی برق، کامپیوتر، مکانیک و هوش مصنوعی.
۱۰. منصوری، عماد، (۱۴۰۰)، مسئولیت مدنی ناشی از هوش مصنوعی در حقوق ایران با نگاهی بر حقوق انگلیس، نهمین کنفرانس بین المللی مطالعات حقوقی و قضایی.



۱۱. تخشید، زهرا، (۱۴۰۰)، مقدمه ای بر چالش های هوش مصنوعی در حوزه مسئولیت مدنی، حقوق خصوصی، دوره ۱۸، شماره ۱.
۱۲. پناهی، مریم علی، نصیران نجف آبادی، داوود، شیرانی، مسعود، (۱۴۰۳)، مسئولیت مدنی ناشی از استفاده هوش مصنوعی در اتحادیه اروپا، مطالعات فقه اقتصادی، سال ۶، شماره ۵.
۱۳. رشوندبوکانی، مهدی، ناصر، مهدی، (۱۳۹۸).
۱۴. قصد متعاملین در قراردادهای هوشمند: شرایط اعتبار و شیوه احراز آن، پژوهشنامه حقوق اسلامی، دوره ۲۰، شماره ۱.
۱۵. Baris Soyer, Andrew Tettenborn, (۲۰۲۲) Artificial intelligence and civil liability—do we need a new regime, International Journal of Law and Information Technology, Volume ۳۰, Issue ۴, Winter, Pages ۳۸۵–۳۹۷, <https://doi.org/10.1093/ijlit/eaad۰۰۱>.
۱۶. Francisco Andrade, et.al., (۲۰۰۷) “Contracting Agents: Legal Personality and Representation,” Artif.Intell.Law ۱۵ ۳۶۱.
۱۷. Fredrikson, Matt & Li, Tom & Jagannathan, Sharan & Busch, Christoph. (۲۰۱۵). Privacy in Machine Learning: Federated Learning vs. Split Learning. CoRR. abs/۱۸۱۲.۰۰۵۶۴.
۱۸. Milad Haji Esmaeili, The Civil Liability Challenges of Artificial Intelligence (AI) in Iran's Legal System and a Comparative Look at Regulations in the European Union, Quarterly Journal of Government and Law, Vol. ۵, No. ۱ (Serial ۱۵), Spring ۲۰۲۴.
۱۹. Monostori, et.al., “Agent-based Systems for Manufacturing,” Annals of The CIRP (ParkUniversity) ۵۵ (۲۰۰۶): ۳.
۲۰. Pearce, G. (۲۰۲۱, May ۲۸). Beware the Privacy Violations in Artificial Intelligence Applications. Retrieved from ISACA: <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/۲۰۲۱/beware-the-privacy-violations-in-artificial-intelligence-applications>.
۲۱. R.M. Shoyama, “Intelligent Agents: Authors, Makers and Owners of Computer-Generated.



۲۲. Usercentrics. (۲۰۲۲, April ۱۲). Artificial intelligence (AI) and data privacy. Retrieved from usercentrics: <https://usercentrics.com/knowledge-hub/data-privacy-artificial-intelligence>.

۲۳. Yao, Hongyang & Shen, Jun & Shi, Yi & Li, Yaoli & Gao, Xiaohui & Wu, Jiamin. (۲۰۲۱). Deep Learning for Cyber Security Attacks Detection in Fog Computing. ۱-۷. ۱۰, ۱۱۰۹/ICACT. ۲۰۲۱, ۹۴۱۶۲۰۷.



Civil liability of artificial intelligence in the field of privacy with an approach to regulatory standards in commercial contracts

Fatemeh Zolfagharzadeh^۱

Article Number: JHVMN-۲۵۰۱-۱۲۵۷

Abstract

Artificial intelligence applications are used in our daily lives and bring significant benefits to their users. However, just like anything else in life, things can go wrong and users or their third parties may suffer losses related to the malfunctioning of the relevant AI program. Building trust in processes and systems based on artificial intelligence, it is necessary to review the standards developed in this regard at the international and national level. Due to the wide and important applications of artificial intelligence, today artificial intelligence standardization is on the agenda of most standardization organizations. Standards ensure that AI will serve the public good. In other words, without regulations and standards for the responsible use of artificial intelligence, its harmful consequences cannot be avoided. We all know that when profit and power are the only motivations, artificial intelligence is also used to serve power and capital. In this situation, its consequences for human life will never be considered. Standards therefore ensure that AI technologies are developed in accordance with ethical principles and social norms. These standards also guarantee that artificial intelligence is used to protect civil liberties and equal access to technologies, and ultimately lead to the advancement of humanity. The digitalization of today's world is inextricably linked with the development of artificial intelligence. Based on research findings, identify and counter new threats, cyber warfare bots, predict breach risk, better endpoint protection, learn over time, manage abundant data, reduce repetitive processes, and secure authentication. Artificial intelligence, like other technologies, has created potential opportunities and threats for the Islamic Republic of Iran. However, by implementing legal and executive mechanisms, it is possible to provide the country with the maximum benefit from this technology in order to increase national power and fulfill the goals of the Islamic Revolution at the regional and global level.

Keywords: artificial intelligence, privacy, monitoring, standard.

^۱. Master of Science, Islamic Azad University, Safashar Branch, Law Department, Private Law Orientation. (Corresponding Author) Fatemezolfagharzade^{۷۷}@gmail.com

