

بررسی حریم خصوصی و حفاظت از داده ها در عصر هوش مصنوعی

شیرین فهیمی کبیر^۱

تاریخ دریافت: ۱۴۰۴/۰۲/۰۱ تاریخ چاپ: ۱۴۰۴/۰۵/۲۸

چکیده

با توجه به افزایش چشمگیر توسعه و بکارگیری سیستم‌های هوش مصنوعی و نیاز پایان‌ناپذیر این سیستم‌ها به داده‌های شخصی، روز به روز حق بر حریم خصوصی که در منشور بین‌المللی حقوق بشر به دفعات مورد تاکید قرار گرفته است و موضوع حریم خصوصی در استفاده‌ها از هوش مصنوعی 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 ذخیره سازی 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. در این پژوهش سعی شده است به شیوه توصیفی تحلیلی چالش‌هایی که فناوری هوش مصنوعی جهت حفظ حریم خصوصی ایجاد کرد است مورد بررسی قرار بگیرند و راهکارهایی که نظام بین‌المللی حقوق بشر جهت مدیریت این چالش‌ها در نظر گرفته است بیان شوند.

واژگان کلیدی

حریم خصوصی، هوش مصنوعی، حقوق بین‌الملل، قانون تجارت.

۱. کارشناس ارشد حقوق خصوصی، دانشکده حقوق، دانشگاه پیام نور، ایلام، ایران. مدرس دانشگاه.
(shirinfahimi.law1988@gmail.com)

۱- مقدمه

با توسعه و بکارگیری فزاینده سیستم های هوش مصنوعی در سال های اخیر حق بر حریم خصوصی به نحوی تحت تاثیر نامطلوب این تکنولوژی قرار گرفته است که برخی دوران کنونی را «عصر پوچگرایی حریم خصوصی» می نامند. انسان موجودی آزاد است که به موجب حقوق بشر و کرامت ذاتی انسانی حق دارد در خصوص سرنوشت خود بدون مداخله دیگران تصمیم گیری نماید و این امر ممکن نمی شود مگر در سایه حریم خصوصی. چندین دهه است که حق بر حریم خصوصی به عنوان یک حق بشری و یکی از ارزش های بنیادین جوامع دموکراتیک، به رسمیت شناخته شده است. اگرچه مفهوم و گستره این حق به روشنی مشخص نشده است اما به طور تقریبی تمامی جوامع و دولت ها این حق را پذیرفته و در قوانین ملی خود از آن حمایت می کنند مبنای حق بر حریم خصوصی حمایت از خودمختاری انسان ها و حفظ عاملیت افراد در تصمیماتی است که میگیرند. حریم خصوصی این امکان را برای افراد فراهم می آورد که دور از نظارت عموم به تفکر بپردازند، تصمیم بگیرند که چه عقاید و اندیشه هایی را با چه افرادی و در چه زمانی به اشتراک بگذارند، به چه اشخاصی جهت به اشتراک گذاشتن اطلاعاتشان اعتماد کنند و تصور عمومی از خود را شکل دهند. حق بر حریم خصوصی حقی است که زمینه تضمین بسیاری از اصول حقوق بشر از جمله آزادی بیان حق دسترسی به اطلاعات آزاد و حق بر داشتن عقیده را تضمین می نماید (لتونرو، ۱، ۲۰۱۸).

سیستم های هوش مصنوعی جهت انجام عملکردهای خود به میزان زیادی داده نیاز دارند و این امر موجب شده است که تمایل به جمع آوری و پردازش داده های افراد افزایش پیدا کند. هوش مصنوعی با توانمندسازی تکنولوژی های نظارتی نیز تا حد بسیار زیادی حریم خصوصی افراد را به چالش کشیده اند. کنترل و به حداقل رساندن تاثیرات نامطلوب حقوق بشری سیستم های هوش مصنوعی نیازمند یک چارچوب هنجاری دارای ضمانت اجرای قوی و بین المللی است. در حال حاضر چارچوب نظام حقوق بین الملل بشر به وضع قواعدی در زمینه حق بر حریم خصوصی پرداخته است اما این چارچوب از آنجا که در دوران آنالوگ تدوین شده و متناسب با نیازهای روز آن است؛ موجب شده است تا برخی این چارچوب را جهت ضابطه مند نمودن هوش مصنوعی و کاهش چالش های حریم خصوصی آن، کافی ندانند. این پژوهش به دنبال اثبات این موضوع است که توسعه و کاربرد سیستمهای هوش مصنوعی تاثیرات نامطلوبی بر حق بر حریم خصوصی داشته است و توسل به قواعد حقوق بشر تا حد زیادی می تواند در کاهش این اثرات نقش موثری داشته باشد. اما با توجه به تحولاتی نوینی که هوش مصنوعی ایجاد کرده است نیازهای جامعه نیز تغییرات اساسی نموده اند و چارچوب بین المللی حقوق بشر به تنهایی نمی تواند پاسخگوی تمام این نیازهای جدید باشد.

۲- اثرات نامطلوب کاربرد هوش مصنوعی بر حق بر حریم خصوصی

سیستم های هوش مصنوعی نیاز به جمع آوری حجم عظیمی از داده ها دارند؛ شرکتهای بخش خصوصی و دولت ها به عنوان دو بازیگر اصلی توسعه هوش مصنوعی روزانه حجم زیادی از داده های افراد را جمع آوری می نمایند. اغلب تکنولوژی های مورد استفاده بشر امروزه مانند کامپیوترهای شخصی گوشی های هوشمند، ساعت های هوشمند، سنسورهای موجود در خانه ها و شهرهای هوشمند همواره در حال جمع آوری داده های افراد هستند. این داده ها طیف وسیعی از اطلاعات ما از جمله نشانی، ایمیل شماره تلفن و داده های حساس تری مانند داده های مربوط به سلامتی، داده های بیومتریک و داده های اقتصادی را جمع آوری مینمایند.

¹ Latonero

علاوه بر جمع آوری داده ها جهت تغذیه سیستم های هوش مصنوعی، این سیستم ها با استفاده از الگوریتم و مدل های خود از طریق پردازش و تحلیل داده ها قادر به تولید اطلاعات و داده های جدید در مورد افراد نیز هستند. سیستم های هوش مصنوعی از طریق پردازش داده های آنلاین افراد قادر به درک الگوهای رفتاری فردی و یا جمعی انسان ها می باشند. جمع آوری و پردازش داده های افراد می توانند منجر به نقض حریم خصوصی افراد شوند و همچنین اصل خود مختاری و آزادی اراده انسانی را دستمایه تغییرات قرار دهند. علاوه بر جمع آوری وسیع داده ها و اطلاعات مربوط به زندگی خصوصی افراد و پردازش داده های آنها همچنین توسعه و بکارگیری هوش مصنوعی نقش عظیمی در توسعه و پیشرفت تکنولوژی های نظارتی و رشد نظارت گسترده توسط دولت ها بر زندگی افراد داشته است که منجر به از میان رفتن مفهوم فضاهاى خصوصی شده است (برونلی، ۲، ۲۰۱۹).

۳- اثرات نامطلوب جمع آوری داده ها بر برخورداری افراد از حق بر حریم خصوصی

نخستین ویژگی چالش برانگیز هوش مصنوعی برای حریم خصوصی نیاز مبرم این سیستمها به اطلاعات و داده است. در سالهای اخیر با توجه به دیجیتال شدن فناوری اطلاعات و فراهم شدن امکان جمع آوری و ذخیره سازی داده ها در حجم گسترده، تامین داده برای سیستم های هوش مصنوعی نیز تسهیل شد و از طرفی دیگر تکنولوژی هوش مصنوعی به جمع آوری دادهها از طریق روشهایی مانند اینترنت اشیا و تصفیه داده ها کمک شایانی نموده است. با توجه به اینکه داده ها در قرن اخیر ارزش اقتصادی پیدا کرده اند و بسیاری از شرکتهای بخش خصوصی و دولتها به جمع آوری و ذخیره سازی داده ها روی آورده اند به این امر می پردازیم که جمع آوری و ذخیره سازی داده ها حتی اگر پردازش و تحلیلی بر روی آنها انجام نگیرد، چه تاثیرات نامطلوبی بر برخورداری افراد از حق بر حریم خصوصی دارند.

۱-۳- تجارت داده

بسیاری از شرکت های تجاری از جمله شرکت های شبکه های اجتماعی داده های شخصی کاربران خود را در دیتابیس های عظیم خود ذخیره و نگهداری می نمایند تا آنها را به معرض فروش بگذارند. همچنین بسیاری از شرکت های خصوصی با جمع آوری داده های شخصی و غیر شخصی کاربران خود اقدام به ساخت پروفایل برای افراد می نمایند. پروفایل مجموعه ای از داده های مرتبط با یکدیگر است که به موضوع خاص اعم از یک فرد و یا یک گروه را نمایندگی می نماید نحوه عملکرد پروفایل ها به این شکل است که یک موضوع خاص را شناسایی و نمایندگی می کنند و یا تشخیص می دهد که آیا یک فرد و یا موضوع خاص متعلق به یک گروه است یا خیر (آنسام^۳ و همکاران، ۲۰۲۰).

۲-۳- مشروعیت جمع آوری داده با تمسک به رضایت

مطابق با حق بشری حریم خصوصی یکی از مصادیق حریم خصوصی که افراد باید از آن برخوردار شوند، حریم خصوصی اطلاعاتی است به این معنا که هیچ شخصی حق بر مداخله و جست و جو در اطلاعات یک فرد را ندارد مگر اینکه مداخله از وصف مشروعیت برخوردار باشد در تفاسیر حقوق بشری از قاعده حریم خصوصی مراد از مشروعیت قانونی بودن است. بنابراین جمع آوری اطلاعاتی که در زمره حریم خصوصی افراد قرار میگیرند ممنوع است مگر به حکم قانون اما به دنبال ظهور تکنولوژی هایی مانند داده های بزرگ جمع آوری اطلاعات در سطح وسیع، سونامی نشت

² Brownlee

³ Ansam

داده و رشد بازاریابی، رفتاری آیا یک قاعده کلی که مداخله در حریم خصوصی را ممنوع دانسته است مگر به حکم قانون می تواند کافی باشد.

دان سولو محقق در زمینه حریم خصوصی و داده ها اشکال اساسی جمع آوری و ذخیره دادهها در دیتابیس را در این میدانست که کنترل دادهها از دست اشخاص موضوع داده خارج میشود. حق بر تعیین سرنوشت فردی که در گرو آزادی انسان ها در تصمیم گیری است محور اصلی مفهوم انسان در اندیشههای لیبرال است. کرامت ذاتی انسانها که مهمترین اصل انسان حقوق بشری است در گرو همین آزادی انسانها در تصمیم گیری است. حق بر حریم خصوصی نیز بر اساس کرامت ذاتی بشر به او واگذار شده است از این قاعده مستثنی نبوده و بسیاری از محققان مبنای حریم خصوصی را حق تعیین سرنوشت فردی و آزادی در تصمیم گیری می دانند که بر اساس این مبنا حریم خصوصی یعنی افراد بتوانند تصمیم بگیرند که چه اطلاعاتی از خود را منتشر کنند و بر شکل گیری تصور عمومی از شخصیت خود کنترل داشته باشند. مبتنی بر این نظریه بزرگترین چالشی که جمع آوری و ذخیره دادهها برای حریم خصوصی افراد ایجاد میکند از بین رفتن کنترل افراد بر دادههای خود است. در این زمینه سولو پیشنهاد می کند که اگر به افراد موضوع داده ها اجازه دسترسی به مجموعه داده ها از جمله امکان حذف و یا اصلاح دادهها اعطا گردد این چالش حل شده و دیگر ایجاد دیتابیس از داده های افراد مصداق نقض حریم خصوصی نیست (سولو، ۲۰۰۴).

۴- چالش های هوش مصنوعی در زمینه حریم خصوصی

۴-۱- چالش های ذخیره سازی داده ها

در گزارش شورای حقوق بشر تحت عنوان «حق بر حریم خصوصی در دوران دیجیتال ۲۰۲۱» نیز کمیساریای عالی حقوق بشر از جمع آوری و ذخیره داده های شخصی افراد به عنوان یکی از چالشهای نقض حریم خصوصی یاد کرده است که توسعه هوش مصنوعی و افزایش نیاز به داده ها نیز به وخامت اوضاع افزوده است. در گزارش عنوان شده است که جمع آوری و ذخیره داده های شخصی به مدت، نامعلوم، علاوه بر اینکه زندگی شخصی افراد را در معرض دید دولت ها و بخش خصوصی قرار می دهد همچنین آسیب پذیر شدن افراد به اشکال مختلف نیز می گردد که داده های حساس آنها را در اختیار اشخاص ثالث می گذارند به عنوان مثال مجموعه داده های ذخیره شده توسط بخش خصوصی این امکان را برای نهادهای دولتی فراهم می آورد که در هر زمانی بتوانند به این مجموعه داده ها دسترسی پیدا کنند که منجر به نقض خودسرانه و غیرقانونی حق بر حریم خصوصی شهروندان خواهد شد؛ همان گونه که بسیاری از دولتهای استبدادی جهت دستگیری فعالان سیاسی و حقوق بشری مجوز دسترسی به دیتابیس های بخش خصوصی را صادر می کنند (رایز، ۲۰۲۱).

جمع آوری داده از طرق مختلف توسعه یافته است و به میزانی رسیده است که میتوان ادعا نمود تقریباً هیچ فضای خصوصی برای افراد باقی نمانده است و حتی اطلاعات یک فرد پشت درهای بسته نیز قابل جمع آوری هستند این نکته زمانی نگرانی ها از زوال مفهوم حریم خصوصی را افزایش می دهد که جمع آوری داده ها به شکل پنهانی انجام بگیرند و یا با شفافیت و اطلاع صریح افراد داده های آنها گردآوری نشوند رفع این مشکل مستلزم آموزش به افراد است که از

⁴ Solov

⁵ Risse

روش های رایج جمع آوری داده مطلع شوند و در صورت عدم تمایل مانع آن شوند، هرچند در بسیاری از موارد امتناع از پذیرش موجب این می شود که به درستی از خدمات بهره مند نگردند.

در نهایت به طور کلی میتوان استدلال نمود که جمع آوری طبقه بندی و ذخیره سازی داده ها از آنجا که از شفافیت کافی برخوردار نیستند اغلب پنهانی صورت می گیرند در مواردی مورد استفاده قرار می گیرند که مورد انتظار شخص موضوع داده نیستند و ممکن است موجب آسیب پذیرتر شدن افراد در آینده می گردند از جمله افشای داده ها به اشخاص ثالث و تحلیلهای اشتباه قرار بگیرند در تضاد کامل با حق بر حریم خصوصی میباشد.

۲-۴- پردازش داده ها و نقض حریم خصوصی

پردازش داده به فرآیندی گفته میشود که دادههای خام را به اشکال قابل استفاده منطبق با هدف پردازشگر تبدیل می نماید. هدف نهایی پردازش داده همواره تبدیل داده به اطلاعات قابل استفاده می باشد. ویژگی منحصر به فرد این چالش حریم خصوصی توسط سیستم های هوش مصنوعی این امر است که تحلیل و پردازش توسط هوش مصنوعی منحصر به داده های شخصی نبوده و حتی از طریق پردازش داده های غیر شخصی نیز حق بر حریم خصوصی افراد در سطح گسترده ای تحت تاثیر واقع خواهد شد.

از آنجا که حق بر حریم خصوصی یک حق سایه است که منجر به تضمین بسیاری از حقوق دیگر میشود نقض آن از طریق پردازش داده ها بسیاری حقایق بشری دیگر از جمله حق دسترسی به اطلاعات آزاد، حق آزادی بیان حق بر داشتن عقیده حق بر دادرسی منصفانه و منع تبعیض را نیز تحت تاثیر قرار میدهد. مدیریت محتوا که یکی از کاربردهای هوش مصنوعی است با انتخاب محتواهای محدود متناسب با سلیقه کاربران اینترنتی حق دسترسی افراد به اطلاعات آزاد را به شدت نقض می کنند که در نتیجه آن حق بر داشتن عقیده و حق آزادی بیان را نیز محدود میسازند در خصوص حق بر منع تبعیض نیز همانگونه که بیان شد پردازش داده های غیر شخصی منجر به تسهیل شناخت گروههای خاص و اقلیت ها شده و آسیب پذیری این گروه ها را افزایش میدهد (زننگ، ۲۰۱۸).

از دیگر چالش های پردازش دادهها توسط هوش مصنوعی نیز عدم دقت و صحت نتایج حاصل از پردازش داده ها است. در بسیاری از موارد اگر دادههای ورودی به هوش مصنوعی داده هایی غلط بوده و یا تنوع و کیفیت کافی را نداشته باشند میتوانند منجر به نتایج اشتباه شوند که گاه نیز منجر به فجایع عظیمی خواهد شد. حتی اگر داده های ورودی به هوش مصنوعی نیز داده هایی صحیح و کارآمد باشند نیز همچنان احتمالی بودن پیش بینی های هوش مصنوعی از ویژگیهای جدایی ناپذیر تصمیمات این سیستمها است که موجب ایجاد دوگانگی در بکارگیری تکنیک های هوش مصنوعی در کاربردهای مربوط به سلامتی و پزشکی شده است همانگونه که در دوران پاندمی کووید ۱۹ هیچ کدام از سیستم های هوش مصنوعی بکار گرفته شده جهت تشخیص و کنترل این ویروس مفید واقع نشدند. بکارگیری هوش مصنوعی در پیش بینی و تصمیم گیری در مورد افراد میتواند تأثیرات منفی زیادی بر زندگی افراد بگذارد به عنوان مثال استفاده از هوش مصنوعی به عنوان ابزار پیش بینی احتمال ارتکاب جرم در افراد، می تواند منجر به نقض بسیاری از حقوق شهروندی افرادی خاص به اشتباه گردد. احتمالی بودن نتایج خروجی هوش مصنوعی و احتمال اشتباه بودن این اطلاعات در حالی است که فرآیند تصمیم گیری سیستمهای هوش مصنوعی پیچیده و مبهم است و از شفافیت کافی برخوردار نیست که نظام مسئولیت و پاسخگویی سیستمهای هوش مصنوعی نیز دچار اختلال میسازد و اماره ای است بر

غیرقابل جبران بودن خسارات ناشی از تصمیم گیریهای هوش مصنوعی این ابهام و پیچیدگی ناشی از تصمیمات هوش مصنوعی را اصطلاحاً چالش جعبه سیاه هوش مصنوعی مینامند.

حق بر حریم خصوصی یک ارزش است که مبنای آن حمایت از آزادیهای افراد در مسیر رشد و شکوفایی آنها است؛ این در حالی است که گسترش نظارت بر زندگی افراد و در معرض دید عموم قرار گرفتن مانع از آزادی اراده افراد و خودمختاری انسانها میشود و عاملیت انسانی را خدشه دار میسازد انسان موجودی اجتماعی است که از عدم تأیید توسط جامعه مورد تمسخر واقع شدن مورد تهاجم و انتقاد دیگران قرار گرفتن انزجار دارند. انسان به دنبال گرفتن تأیید گروه و جامعه و عضویت در گروههای انسانی است افراد در جهت مورد تأیید دیگران قرار گرفتن در بسیاری از موارد اقدام به سانسور خود مینمایند و بسیاری از اطلاعات خود و هویت خود که منجر به طرد شدن از جامعه می شود را پنهان می نمایند؛ حریم خصوصی از این جهت حائز اهمیت است که از حق انسان ها بر تنها رها شدن و تفکر و رشد عقیده و اندیشه خود در تنهایی حمایت می کند. حال در صورتی که تمامی اقدامات تصمیمات و افکار افراد در معرض دید عموم قرار گیرد این حق بر سانسور و دفاع از خود در برابر جامعه به طور جدی مورد حمله واقع میشود که امکان رشد و شکوفایی خلاقیت و ایجاد نظرات نامحبوب یک فرد و در نهایت شکوفایی کل جامعه بشری را از میان میرد و انسانها را به عروسک هایی مبدل می سازد که مطابق هنجارهای موجود جامعه تفکر میکنند و تصمیم می گیرند(موسی زاده، ۱۳۹۲).

۳-۴- نظارت بر افراد از طریق دسترسی به داده ها

بسیاری از دولت ها با استناد به حفظ امنیت ملی از طریق نظارت پنهانی بر ارتباطات و مکالمات شهروندان خود به جمع آوری، ذخیره سازی و پردازش داده های آنها که از روشهای مختلفی مانند ایمیل، آمار مشاهده وبسایت های اینترنتی تماس های تصویری و پیام های تلفنی به دست آمده اند اقدام بر نظارت گسترده بر زندگی افراد مینمایند. این در حالی است که مطابق با قواعد حقوق بشری حریم خصوصی مندرج در منشور بین المللی حقوق بشر، جمع آوری ذخیره و پردازش داده های افراد به بهانه حفظ امنیت ملی با اصل تناسب و اصل ضرورت در مقابل این کیفرخواست فیس بوک ادعا نمود که استدلالات شاکیان اعتباری ندارد و این افراد نمی توانند در دادگاه علیه فیس بوک شکایتی مطرح کنند زیرا علی رغم اینکه داده های آنها جمع آوری شده است و به موجب قانون حریم خصوصی داده های بیومتریک فیس بوک موظف به کسب رضایت اشخاص موضوع داده بوده است، اما چون این عمل فیس بوک منجر به ایجاد هیچ ضرر و آسیبی به اشخاص موضوع داده نشده است در نتیجه طرح دعوا منتفی بوده و مراجع قضایی نباید به این امر ورود کنند(معمد نژاد، ۱۳۹۳).

۴-۴- نقض حریم خصوصی از طریق نظارت توسط سیستمهای هوش مصنوعی

دستیابی به نظارت همگانی رویای هر حکمرانی در طول تاریخ بوده است تا با نظارت هر چه بیشتر بر افراد تحت سلطه خود آنها را کنترل کند و پایههای سلطه و قدرت خود را مستحکم تر بنا نهد در مقابل ترس از این نظارت و کنترل همگانی که بر تمامی اقدامات و فعالیتهای انسانی ناظر باشد وجود داشته است؛ این نگرانی به حدی بوده است که جورج اورول نویسنده معروف قرن ۲۰ میلادی کتاب خود ۱۹۸۴ را که یک کتاب علمی تخیلی، در مورد پیش بینی های نویسنده از وضعیت سال ۱۹۸۴ است را به این موضوع اختصاص داده است. سالها بعد در حداثال سالهای ۱۹۴۰ تا ۱۹۵۰ با ظهور عصر دیجیتال و رایانه ها و در سال های بعد اینترنت این نگرانی اورول به حقیقت پیوست. هم اکنون نیز با

به میان آمدن تکنولوژی هوش مصنوعی و تحول عظیمی که این تکنولوژی در توسعه تکنولوژیهای نظارتی ایجاد نمود نگرانیهای اجتماعی و حقوق بشری نسبت به گسترش نظارت همگانی بیش از هر زمان دیگری افزایش یافته اند. از طریق پیشرفت تکنولوژی امروزه بیش از زمانهای قبل هر روزه امکان نظارت بر فعالیتهای و به طور کلی زندگی انسانی فراهم شده است و هر روزه نیز در حال گسترش هستند پیشرفت تکنولوژی هوش مصنوعی از روش های گوناگون به گسترش توان دولتها در افزایش نظارت بر زندگی، افراد کمک نموده است. هوش مصنوعی با توانبخشی به تکنولوژیهای تصویری و پیشرفت تکنولوژی دید رایانه امکان نظارت بر افراد در تمامی سطوح را چندین برابر کرده است به نحوی که فضاهای خصوصی دیگر معنایی نداشته و افراد حتی در خصوصی ترین مکان زندگی خود یعنی اقامتگاه و اتاق شخصی خود از نظارت دولت ها در امان نیستند. همچنین دولت ها از طریق دسترسی به داده های ذخیره شده افراد توسط شرکت ها و کسب و کارهای بخش خصوصی نیز بیش از هر زمان دیگری نظارت خود بر زندگی شهروندان خود را افزایش داده اند (بورگس، ۶، ۲۰۲۳).

۵- رویکرد حقوق بشر نسبت به چالشهای حریم خصوصی هوش مصنوعی

رویکرد جامعه بشری نسبت به هر تکنولوژی جدیدی که خطراتی برای انسان ها ایجاد کند وضع قواعد جدید و تنظیم گری است. بازیگران اصلی توسعه و کاربرد سیستم های هوش مصنوعی بخش خصوصی هستند که خدمات آنها به طور فرامرزی در کشورهای مختلفی مورد استفاده قرار می گیرند. همچنین توسط جامعه آکادمیک، بخش خصوصی و یونسکو نیز تلاش هایی در تهیه یک چارچوب اخلاقی جهت هدایت هوش مصنوعی انجام گرفته است اما از آنجا که این تلاشها از جنس حقوق نرم بوده و ضمانت اجرای محکمی ندارند و همچنین مقبولیت بین المللی نداشتند موفق عمل نکردند.

دادهها از منظر حقوق بشر نقض حریم خصوصی افراد نیست اما عدم رعایت الزامات قاعده حریم خصوصی می تواند منجر به نقض حریم خصوصی بشود. بنابراین کاهش اثرات نامطلوب هوش مصنوعی بر حریم خصوصی مستلزم رعایت اصول بنیادین حقوق بشر و وضع قوانین و مقررات در حوزه پردازش داده توسط دولت ها است. شورای حقوق بشر علاوه بر تبیین چگونگی اعمال قاعده حریم خصوصی بر کاربرد هوش مصنوعی به چندین اصل حقوق بشری دیگری که توسعه دهندگان هوش مصنوعی در مسیر مطابقت با حق بر حریم خصوصی باید به آنها التزام داشته باشند، اشاره مینمایند و نحوه مطابقت کاربرد هوش مصنوعی با این اصول را بیان می کند.

۶-۱ اعمال اصول بنیادین حقوق بشر و قاعده حریم خصوصی بر کاربرد هوش مصنوعی

یک رویکرد حقوق بشری نسبت هوش مصنوعی مستلزم رعایت اصول بنیادین حقوق بشری همچون برابری، منع تبعیض حفظ کرامت انسانی و سایر حقوق و آزادیهای حقوق بشری از جمله حق بر حریم خصوصی است.

۶-۱-۱ اعمال قاعده حریم خصوصی بر کاربرد هوش مصنوعی

در منابع معاهداتی حقوق بشر در اسناد زیادی از جمله ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین المللی حقوق مدنی و سیاسی و چندین سند بین المللی و منطقه ای حقوق بشر به حق بر حریم خصوصی اشاره کرده اند. ۱۹۶ حق بر حریم خصوصی به عنوان یکی از حقوق بنیادین حقوق بشری مورد شناسایی قرار گرفته است. این قواعد دولت ها را به احترام و حمایت از حق بر حریم خصوصی متعهد می سازد و استثنائاتی که بر این اصل وارد هستند را تنها در

⁶ Burgess

صورتی مقبول میدانند که به موجب قانون تعیین شده باشند و خودسرانه انجام نگیرند. اگرچه در متن این مواد به دو اصل اساسی دیگر حریم خصوصی اشاره نشده است اما در تفاسیر بعدی از این مواد دو اصل دیگر قابل برداشت هستند که در هنگام جمع آوری ذخیره و پردازش داده‌ها توسط هوش مصنوعی باید مورد توجه قرار بگیرند.

۲-۶- پاسخگویی و مسئولیت سیستمهای هوش مصنوعی

مطابق با اصل پاسخگویی و مسئولیت ناشی از نقضهای حقوق بشری قربانیان نقض حریم خصوصی و یا سوء استفاده هایی که بخش خصوصی و دولتها از حریم خصوصی افراد مینمایند باید بتوانند که به یک دادرسی عادلانه دسترسی داشته و خسارتهایی که به آنها وارد شده است به نحو مقتضی جبران شوند. در این خصوص دولت ها موظف هستند که نه تنها پاسخگویی نهادهای دولتی را تضمین کنند بلکه باید قدم های موثری در جهت پاسخگویی موارد نقض حریم خصوصی توسط بخش خصوصی نیز بردارند. متناسب با ماهیت وضعیت و یا مورد نقضی که ایجاد شده است قربانیان باید به رسیدگی قضایی و یا غیر قضایی دسترسی داشته باشند. مطابق با مفاد «اصول راهنمای سازمان ملل متحد در خصوص تجارت و حقوق بشر» در مواردی که بخش خصوصی در رخ دادن یک نقض حقوق بشری مشارکت و یا معاونت داشته اند موظف هستند جهت اصلاح وضعیت بوجود آمده و جبران خسارات وارده همکاری کنند در این خصوص برخی از نهادهای غیر دولتی بین المللی و ملی اقدام به ایجاد نهادهای غیر قضایی نموده اند اقدامات نهادهای غیر قضایی در این خصوص باید، قانونی، قابل دسترس، قابل پیش بینی، منصفانه و مطابق حقوق بشر باشد.

در مواردی که نقض حریم خصوصی و یا تاثیرات نامطلوب بر آن مستقیماً توسط یک شرکت انجام نگرفته است اما توسط یک شرکت دیگر به واسطه خدمات و کالاهای شرکت نخست موارد نقض انجام شده باشند، به موجب ماده ۱۹ اصول راهنما، شرکت ارائه کننده خدمات ملزم است از هر اهرم فشاری جهت منع شریک تجاری خاطی خود استفاده کند تا شرکت مرتکب نقض فعالیت های خود را اصلاح نماید. پاسخگویی و مسئولیت توسعه دهندگان و سازمان هایی که هوش مصنوعی را بکار می برند در مقررات حقوق بشری واضح و مشخص است اما پیاده سازی این مقررات در عمل به علت شرایط خاص تکنولوژی هوش مصنوعی موانع و مشکلاتی دارد. خاصیت فرامرزی بودن برخی از کاربرهای هوش مصنوعی مانند نظارت مداخله در ارتباطات و پردازش داده ها، در بسیاری از موارد چالش های حقوقی و رویه ای فراوانی را ایجاد می نماید؛ از طرفی دیگر به علت سطح پایین اطلاعات فنی افراد نسبت به روش های نقض حریم خصوصی و یا محرمانه انجام گرفتن این نقض ها توسط سیستم های هوش مصنوعی در واقع در بسیاری از موارد نقض اصلا قربانیان از چنین نقض هایی مطلع نمی شوند؛ به عنوان مثال در مواردی که دولت ها اجازه دسترسی به داده های کاربران یک شبکه اجتماعی را می خواهند شرکتی که داده ها را در اختیار دارد از مطلع نمودن اشخاص موضوع داده ها منع می کنند. همچنین بسیاری از داده های که از طریق پردازش توسط الگوریتم های هوش مصنوعی به دست می آیند عملکرد این الگوریتم ها به سادگی قابل فهم نیست و افراد نمی توانند پیش بینی کنند سیستم های هوش مصنوعی چه پردازش هایی بر روی داده های آنها انجام می دهند و به چه نتایجی خواهند رسید.

۳-۶- ارتقای شفافیت در سیستمهای هوش مصنوعی

یکی از اصولی که در دو گزارش مربوط به حریم خصوصی در دوران دیجیتال شورای حقوق بشر و گزارش گزارشگر ویژه آزادی بیان به آن بسیار اشاره شده است اصل شفافیت فعالیت سیستم های هوش مصنوعی می باشد. مطابق این اصل نخست بکارگیری این سیستم ها به هیچ عنوان نباید مخفیانه انجام گیرد و همچنین داده هایی که جهت عملکرد این

سیستم ها جمع آوری می گردند نیز باید با شفافیت و اطلاع کامل افراد مورد جمع آوری و پردازش قرار بگیرند. دوماً نحوه عملکرد و چگونگی پردازش داده های هوش مصنوعی نیز باید کاملاً مشخص و قابل درک باشد. در خصوص تعهد دولت ها و بخش خصوصی که کاربر سیستم های هوش مصنوعی هستند، این اشخاص موظف هستند نوع سیستم های هوش مصنوعی که به کار می برند اهداف استفاده از این سیستم ها و هویت ایجاد کنندگان و توسعه دهندگان این سیستمها را به اطلاع اشخاصی که متأثر از عملکرد این سیستم ها هستند را به اطلاع افراد برسانند. علاوه بر این افرادی که زندگی آنها تحت تأثیر تصمیمات اتوماتیک ماشینهای هوش مصنوعی است.

۴-۶- اصل مراقبت مقتضی مبتنی بر حقوق بشر در کاربرد هوش مصنوعی

یکی از انتقادات وارده به نظام حقوق بشر در عرصه هوش مصنوعی دولت محور بودن این نظام هنجاری است. این در حالی است که بازیگران اصلی عرصه توسعه و بکارگیری تکنولوژی هوش مصنوعی شرکتهای بخش خصوصی هستند. اما همانطور که در مبحث اول این فصل نیز بدان اشاره شد، چارچوب هنجاری حقوق بشر تنها حاکم بر دولت ها نبوده و همچنین اشخاص بخش خصوصی نیز ملزم به رعایت قواعد حقوق بشری می باشند. سازمان ملل متحد در سند «اصول راهنمای سازمان ملل متحد راجع به تجارتهای و حقوق بشر» به روشنی وظایف و تعهدات شرکت های بخش خصوصی را در قبال رعایت حقوق بشر تعیین نموده است.

ستون دوم اصول راهنما، احترام به حقوق بشر را از تعهدات شرکت های بخش خصوصی دانسته است و این شرکت ها را متعهد به جلوگیری از مشارکت و یا سبب شدن نقض های قواعد حقوق بشر ساخته است. این تعهد شرکت های خصوصی کاملاً تعهدی مستقل از تعهدات حقوق بشری دولت های محل اقامتگاه این شرکت ها است و چه دولت ها به تعهدات حقوق بشری خود عمل کنند و چه نکنند شرکت های خصوصی مستقلاً متعهد به رعایت قواعد حقوق بشری هستند.

این سند به دنبال ظهور شرکت های فراملی که محصولات و خدمات آنها و رای مرزهای محل اقامت گاه شان نیز گسترش می یابد، تهیه و تدوین شد. از جمله لوازم تعهد شرکت های بخش خصوصی به احترام به حقوق بشر تعهد به مانع شدن در بروز پیامدهای منفی حقوق بشری ناشی از خدمات محصولات و فعالیت های شرکت امتناع از مشارکت در نقض های شدید حقوق بشری توسط دولت ها و شرکت های دیگر ارزیابی حقوق بشری خدمات محصولات خود و ارائه راه حل جهت جلوگیری از نقض های حقوق بشری توسط فعالیت هایشان و همچنین انجام رعایت مقتضی مبتنی بر حقوق بشر هستند در حالت تعارض میان قواعد ملی و تعهدات حقوق بشری شرکت های حقوق بشری، تعهدات حقوق بشری این شرکتها در ارجحیت قرار میگیرند؛ به عنوان مثال در صورت تقاضای دولت از بخش خصوصی جهت دسترسی به داده های مشتریان شرکت جهت ردیابی مخالفان سیاسی به نحو غیرقانونی در تعارض با حقوق بشر است و شرکت ها ملزم به رعایت حقوق بشر افراد هستند و باید تمامی تلاش خود جهت تفسیر مضیق قوانین ملی را به عمل آورند.

۷- قوانین حریم خصوصی و اصول پردازش داده در ایران

در نظام حقوقی ایران هیچ قانون یکپارچه و جامعی که به مختص به حریم خصوصی و یا حفاظت از داده های شخصی باشد، تصویب نشده است. این در حالی است که در برخی از قوانین به صورت پراکنده و اجمالی به لزوم حمایت از حریم خصوصی اشاره شده است که در این زمینه میتوان به قانون اساسی قانون جرائم رایانه ای و قانون انتشار و دسترسی

آزاد به اطلاعات اشاره نمود. همچنین به لزوم حفاظت از داده های شخصی نیز در برخی از مواد قانون تجارت الکترونیک مصوب ۱۳۸۲ و فصل یک قانون جرائم رایانه ای پرداخته شده است. در قانون تجارت الکترونیک بخش تعاریف به تعریف داده پیام های شخصی پرداخته است و داده پیام شخصی داده هایی دانسته است که مربوط به یک شخص حقیقی خاص و معین باشند. در ادامه نیز فصل سوم مفاد این قانون به حمایت از داده پیام های شخصی اختصاص داده شده است. ماده ۵۸ این قانون به اصل اساسی مشروعیت پردازش داده های شخصی پرداخته است که کلید آن کسب رضایت شخص موضوع داده ها می باشد. نکته ای که در خصوص این ماده شایان ذکر است این است که این ماده شامل تمامی داده های شخصی نبوده و به طور حصری تنها داده های مبین ریشه های قومی یا نژادی، دیدگاه های عقیدتی مذهبی، خصوصیات اخلاقی و داده های راجع به وضعیت جسمانی روانی و یا جنسی افراد را که اصطلاحاً داده های شخصی حساس می نامند شامل می شود و پردازش داده های شخصی غیر حساس را دیگر مقید کسب رضایت شخص موضوع داده ها ننموده است (قناد، ۱۴۰۰).

ماده ۵۹ این قانون نیز به برخی دیگر از اصول رایج پردازش داده اشاره نموده است از جمله اصل محدود بودن پردازش داده های شخصی به اهداف بیان شده اصل حداقلی بودن پردازش داده ها و اصل صحت داده ها؛ همچنین حقوقی را نیز برای اشخاص موضوع داده جهت داشتن کنترل بر داده های شخصی خود برای آنها در نظر گرفته است از جمله حق دسترسی به داده های شخصی امحای داده ها و یا اصلاح آنها ضمانت اجرای نقض مفاد مواد ۵۸ و ۵۹ قانون تجارت الکترونیک نیز در باب چهارم همین قانون مشخص شده؛ نقض این دو ماده مصداق جرم بوده و برای مجازات آن جزای نقدی و حبس از یک تا سه سال تعیین شده است.

با وجود اینکه در حال حاضر قانون تجارت الکترونیک کامل ترین قانونی است که در خصوص پردازش داده های شخصی به تنظیم گری پرداخته است؛ اما با این وجود نیز همچنان نظام حقوقی ایران در این مورد دارای نواقص جدی می باشد. اگرچه قانون تجارت الکترونیک به برخی از اصول اصلی پردازش داده های شخصی پرداخته است اما بسیاری از این موارد را نادیده گرفته از جمله اصل انتخاب، اصل امنیت، اصل شفاف سازی، اصل ممنوعیت افشاء، اصل پردازش مرتبط و اصل عدم انتقال. در نتیجه در حال حاضر با توجه به توسعه روزافزون فعالیت های داده محور از جمله تکنولوژی هوش مصنوعی بیش از هر زمان دیگر نیاز به تصویب مقررات پردازش داده های شخصی احساس می شود و تعلق در تصویب این مقررات می تواند هر روزه جامعه را با پیچیدگی های قانونی بیشتری روبه رو کرده و موجب سوء استفاده افراد از سکوت قانون شود.

۸- نتیجه گیری

در پژوهش حاضر تاثیرات نامطلوبی که توسعه و کاربرد سیستم های هوش مصنوعی بر برخورداری افراد از حق بر حریم خصوصی داشته است مورد بررسی قرار گرفتند و بیان شد که تکنولوژی هوش مصنوعی به علت نیاز به جمع آوری داده ها تا حد زیادی موجب نفوذ در زندگی خصوصی افراد می شود. همچنین عدم شفافیت عملکرد این سیستم ها، تاثیرات نامطلوب بر حریم خصوصی را تشدید نموده و اصل پاسخگویی را نیز با چالش های جدی مواجه می کند.

چارچوب حقوق بین الملل بشر میتواند نقش موثری بر کاهش اثرات نامطلوب هوش مصنوعی بر حق بر حریم خصوصی ایفا کند. زیرا چارچوب حقوق بشری مجموعه ای از قواعد بین المللی مورد قبول دولت های جامعه بین المللی هستند حق بر حریم خصوصی نیز در چارچوب منشور بین المللی حقوق بشر تدوین شده است. مبتنی بر قاعده حریم خصوصی

هیچ شخصی حق مداخله در حریم خصوصی افراد را ندارد مگر به حکم قانون به موجب این قاعده اصل ضرورت اصل تناسب و اصل قانونی بودن سه اصل سازنده حق بر حریم خصوصی هستند. رعایت این سه اصل در پردازش داده ها و همچنین در کاربرد سیستمهای نظارتی موجب میشود که حق بر حریم خصوصی تا میزان قابل توجهی تضمین شود متناسب با اصل تناسب و اصل ضرورت کاربرد بسیاری از سیستم های هوش مصنوعی که حق بر حریم خصوصی را به چالش کشیده اند؛ باید محدودتر و یا حتی ممنوع شود؛ مواردی مانند سیستمهای تشخیص بیولوژیک و ذخیره داده های شخصی به مدت نامعلوم. چارچوب حقوق بین الملل حقوق بشر همچنین دولتها را ملزم میکند که اقدام به وضع قوانین و مقررات مربوطه در زمینه پردازش داده ها نمایند.

با وجود اینکه منشور بین المللی حقوق بشر در زمینه تنظیم گری در مورد برخی از چالش های حریم خصوصی ایجاد شده توسط هوش مصنوعی به تنهایی کافی نیست. اما جامعه بین المللی و نهادهای حقوق بشری در سالهای اخیر در پی افزایش نگرانی ها راجع به تضمین حق بر حریم خصوصی در دوران هوش مصنوعی، اقدامات مثبتی انجام داده اند. به عنوان مثال شورای حقوق بشر سازمان ملل متحد در پی قطعنامه های سازمان، اقدام به ارائه گزارشهای سالانه تحت عنوان حق بر حریم خصوصی در دوران دیجیتال نموده است. در این گزارشها پایبندی بخش دولتی و بخش خصوصی بر اصول تناسب ضرورت اصل پاسخگویی و اصل شفافیت مورد تاکید قرار گرفته است. شورا همچنین دولت ها را موظف به وضع قوانین در زمینه پردازش داده ها نموده و بخش خصوصی را نیز ملزم دانسته است که لوازم مراقبت مقتضی مبتنی بر حقوق بشر را کاملاً رعایت نمایند.

منابع و مآخذ

قناد، فاطمه، شریف الهام. "مطالعه اجمالی حمایت از داده های شخصی در نظام حقوقی ایران". دو فصلنامه تخصصی حقوق فناوری های نوین، شماره ۴، صفحه ۱-۲۲. (۱۴۰۰).

<https://www.noormags.ir/view/fa/articlepage/1904400/>

معمد نژاد، رویا. "هوش مصنوعی و ضرورت قانونمند کردن آن: اولین اقدامات جامعه بین المللی"، نشریه حقوق روزنامه نگاری و ارتباطات ۲، شماره ۳. (۱۳۹۳). .. 5. magiran.com/p2178761

موسی زاده، ابراهیم، مصطفی زاده، فهیم. "نگاهی به مفهوم و مبانی حق بر حریم خصوصی در نظام حقوقی عرفی". فصلنامه دانش حقوق عمومی شماره دوم: ۴۵-۶۷. (۱۳۹۲). [http://mag.shora-](http://mag.shora-rc.ir/article_10.html?lang=fa)

[rc.ir/article_10.html?lang=fa](http://mag.shora-rc.ir/article_10.html?lang=fa) *

Abdulhussein, Ansam A., Hasanien Kariem Kuba, and Alaa Neamah Azeez Alanssari. "Computer vision to improve security surveillance through the identification of digital patterns." In 2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), pp. 1-5

Brownlee, Jason. "a gentle introduction to computer vision". Machine Learning Mastery. (2019). <https://machinelearningmastery.com/what-is-computer-vision/5>

Burgess, Matt. "ChatGPT Has a Big Privacy Problem". WIRED. April 4 (2023). <https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr>

Latonero, Mark. "Governing artificial intelligence: Upholding human rights & dignity." (2018). https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.

Pant, Ayush. "Introduction to Machine Learning for Beginners". Towarddatascience.com. (2019). <https://towardsdatascience.com/introduction-to-machine-learning-db7c668822c418>

Penney, Jonathon, Sarah McKune, Lex Gill, and Ronald J. Deibert. "Advancing human-rights-by-design in the dual-use technology industry." *Journal of International Affairs* 71, no. 2 (2018): 103-110.

Raso, Filippo A., Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz, and Levin Kim. "Artificial intelligence & human rights: Opportunities & risks." *Berkman Klein Center Research Publication* 2018-6 (2018).

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=32593443

Risse, Mathias. "The fourth generation of human rights: Epistemic rights in digital lifeworlds." *Moral Philosophy and Politics* 8, no. 2 (2021): 351-378. <https://www.degruyter.com/document/doi/10.1515/mopp-2020-0039/html31>

Solove, Daniel J. "Conceptualizing privacy." *California law review* (2002): 1087-1155. <https://www.jstor.org/stable/348132637>

Zeng, Meg Jing. "China's social credit system puts its people under pressure to be model citizens." *The Conversation* 23 (2018). <https://theconversation.com/chinas-social-credit-system-puts-its-people-under-pressure-to-be-model-citizens-89963>